Rapid Recovery 6.2

ユーザーガイド

目次

Rapid Recovery への概要 14
Core Console 15
Rapid Recovery Core Console へのアクセス 15
クイックスタートガイドについて 15
クイックスタートガイドの非表示設定 17
Rapid Recovery Core Console での移動 17
左側のナビゲーションエリアについて 19
Rapid Recovery Core Console の ホーム ページの表示 19
ホーム ページ (サマリテーブルビュー) について 19
Core ダッシュボードレポートについて 22
保護対象マシン メニューの表示 23
保護対象マシンのサマリ情報の表示 23
「サマリ」ペインの表示 24
保護対象マシンでのボリュームの表示 24
レプリケーション情報の表示 24
Exchange Server 情報 ペインの表示 24
SQL Server 情報 ペインの表示 25
ホストのサマリ情報の表示 25
マシンのリカバリポイントの表示 25
保護対象マシンのイベントの表示 26
保護対象マシンのレポートの表示 28
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 28
「リカバリポイントのみ」メニューの表示 29
カスタムグループ メニューの表示 29
エラー ダイアログボックスの使用 29
Core 設定 30
Core 設定の主な機能 30
Core 設定のバックアップとリストア 31
Core サービスの再起動またはシャットダウン 32
Rapid Recovery Core の設定 33
Core 一般設定の構成 37
アップデート設定の構成 39
夜間ジョブについて 40
Core の夜間ジョブの設定 43
転送キュー設定の変更 44
クライアントタイムアウト設定の調整 44

重複排除キャッシュと保存場所について 46
重複排除キャッシュ設定の構成 47
Replay エンジン設定の構成 48
導入設定の構成 49
データベース接続の設定の構成 50
ローカルデータベースの接続設定の変更 52
SMTP サーバ設定の管理 53
クラウドアカウント接続設定の構成 53
Core に関連付けられた Azure 管理証明書の操作 54
Azure アカウントの公開設定ファイルの取得 54
Azure 管理証明書のロード 55
Azure 管理証明書の更新または削除 55
レポート設定の管理 56
Core の SQL アタッチ可否設定の管理 57
Core ジョブについて 59
Core ジョブの設定 63
Core ジョブの設定への追加 63
Core ジョブ設定の編集 64
ライセンスの管理 65
ライセンスのアップデートまたは変更 67
ライセンスの追加 68
Rapid Recovery ライセンスポータル サーバへの接続 69
SNMP 設定について 69
SNMP の設定 70
SNMP MIB ファイルのダウンロード 71
vSphere 設定の構成 72
VMware のプロキシ設定の管理 72
vFoglight 設定の構成 73
Core レベルのツール 74
Core のシステム情報について 74
Core のシステム情報の表示 75
Core ログへのアクセス 76
Core ログファイルのダウンロードと表示 76
リポジトリ 78
リポジトリについて 78
Rapid Recovery での重複排除 81
DVM リポジトリの管理 82
DVM レポジトリの作成 82

既存 DVM リポジトリへのストレージ場所の追加 85
DVM リポジトリの整合性チェックについて 88
DVM リポジトリでの整合性チェックの実行 89
DVM リポジトリの最適化について 89
DVM リポジトリの最適化 90
DVM リポジトリ最適化の中断または再開 91
階層化リポジトリの管理 91
階層化リポジトリの作成 92
リポジトリのチェック 94
リポジトリ設定の変更 94
既存のリポジトリへの接続 95
リポジトリの詳細の表示または変更 97
リポジトリの切断 99
リポジトリの削除 100
プライバシーの管理 101
一般データ保護規則の遵守 101
Rapid Recovery が個人情報を使用する方法 102
Phone Home 以外のライセンスの制限 103
Phone Home 以外のライセンスの取得と使用 104
暗号化 106
暗号化キーについて 106
ネットワーク経由の転送でデータを暗号化する 107
暗号化キーの適用または削除 107
暗号化キーの保護対象マシンとの関連付け 108
保護対象マシンページからの暗号化キーの適用 108
暗号化キーの関連付けを保護対象マシンから解除 110
暗号化キーの管理 110
暗号化キーの追加 112
暗号化キーのインポート 113
暗号化キーのアンロック 114
暗号化キーのロック 115
暗号化キーの編集 115
暗号化キーのパスフレーズの変更 116
暗号化キーのエクスポート 116
暗号化キーの削除 117
暗号化キーのタイプを変更 117
マシンの保護 119
Rapid Recovery によるマシンの保護について 119

エージェントベースの保護またはエージェントレス保護を選択するときの要因 120
Rapid Recoveryを使用した Linux マシンの保護について 122
Oracle データベースサーバの保護について 122
Oracle データベースの認証情報の入力または編集 124
保護対象 Oracle データベースのアーカイブログモードの有効化と VSS ライターの追加 126
Oracle ログの切り捨てについて 126
Oracle データベースログの手動による切り捨て 127
Rapid Recovery Core での保護対象アプリケーションサーバの管理について 128
サーバクラスタの保護について 128
Rapid Snap for Virtual について 129
エージェントレス保護のためにハイパーバイザツールをインストールする利点 133
クラッシュ整合性バックアップとアプリケーション整合性バックアップについて 134
Rapid Recovery Agent ソフトウェアのインストーラについて 134
Rapid Recovery Agent インストーラのダウンロード 135
Core Console からの複数マシンへの Agent の同時展開 135
Agent ソフトウェアの展開 ウィザードを使用した 1 台または複数のマシンへの展開 136
Active Directory ドメイン上のマシンへの導入 137
VMware vCenter/ESXi 仮想ホスト上のマシンへの展開 138
Rapid Recovery Agent 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 139
手動によるマシンへの導入 140
複数マシンへの導入の確認 140
導入設定の変更 141
保護スケジュールについて 141
マシンの保護 142
クラスタの保護 148
クラスタ内のノードの保護 153
シンプルモードでのカスタム保護スケジュールの作成 154
詳細設定モードでの複数の保護スケジュール期間の作成 155
保護の一時停止と再開 156
複数のマシンの保護について 158
Active Directory ドメインでの複数マシンの保護 159
VMware vCenter/ESXi 仮想ホスト上での複数のマシンの保護 163
エージェントレスの保護を使用した vCenter/ESXi 仮想マシンの保護 168
Hyper-V 仮想ホスト上の複数のマシンの保護 173
エージェントレス保護を使用した Hyper-V 仮想マシンの保護 177
手動での複数マシンの保護 182
複数マシンの保護の監視 186
アプリケーションサポートの有効化 186

保護対象 Exchange Server の設定と機能 187
Exchange Server マシンの認証情報の設定 188
Exchange マシンのログの切り捨ての強制実行 189
Exchange データベースのマウント可否チェックについて 189
Exchange データベースのマウント可否チェックの強制実行 190
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 190
保護対象 SQL Server の設定と機能 191
SQL Server マシンの資格情報の設定 192
SQL マシンのログの切り捨ての強制実行 192
SQL アタッチ可否について 193
SQL Server のアタッチ可否チェックの強制実行 193
保護対象マシンの管理 195
保護対象マシンの管理について 195
保護対象マシンの表示 195
クラスタのサマリ情報の表示 196
マシン設定の構成 196
保護対象マシンの設定の表示と変更 197
Hyper-V ホストまたはノードの設定変更 201
Hyper-V の保護対象仮想マシンの設定変更 202
VMware 保護対象仮想マシンの vSphere 設定の変更 203
転送設定の変更について 204
転送速度のスロットル 204
保護対象マシンの夜間ジョブのカスタマイズ 205
保護対象マシンのシステム情報の表示 206
マシンの管理 207
マシンの削除 207
保護からのクラスタの削除 207
保護からのクラスタノードの削除 208
クラスタ内のすべてのノードの保護からの削除 208
マシンのライセンス情報の表示 208
保護対象マシンのログファイルのダウンロードと表示 209
保護対象クラスタノードの保護対象マシンへの変換 209
カスタムグループについて 209
カスタムグループの作成 210
カスタムグループ名の変更 211
カスタムグループの削除 211
グループアクションの実行 212
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 213

スナップショットとリカバリポイント....214
スナップショットとリカバリポイントの管理....214
保護対象マシンのリカバリポイントページの表示....214
リカバリポイントステータスインジケータについて....216
リカバリポイントのマウント....217
リカバリポイントのマウント解除....218
Linux リカバリポイントの操作....219
Linux マシンでのリカバリポイントボリュームのマウント....219
Linux マシン上でのリカバリポイントのアンマウント....220
スナップショット作成の強制実行....221
リカバリポイントの削除....222
孤立したリカバリポイントチェーンの削除....222
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....223
レプリケーション....225
Rapid Recovery でのレプリケーション....225
リカバリポイントチェーンとオーファン....229
レプリケーション開始のタイミング....230
シーディングの要件と戦略の決定....230
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....232
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....233
レプリケーションの保持ポリシーについて....234
入力方向および出力方向のレプリケーションの表示....234
レプリケーションの設定....236
自己管理ターゲット Core へのレプリケーション....237
サードパーティのターゲット Core へのレプリケート....241
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....241
カスタマからのレプリケーションリクエストの確認....244
レプリケーションリクエストの承認....244
レプリケーションリクエストの拒否....245
カスタマからのレプリケーションリクエストの無視....245
既存のレプリケーションへのマシンの追加....246
ターゲット Core 上のシードドライブの消費....248
シードドライブの破棄....249
レプリケーション設定の管理....250
レプリケーションのスケジュール....251
Copy 機能を使用したシードドライブの作成....251
レプリケーションのモニタリング....254
レプリケーションの一時停止と再開....255

レプリケーションの強制実行 256
出力方向のレプリケーションの設定の管理 257
ターゲット Core の設定の変更 258
保護対象マシンのレプリケーション優先度の設定 258
ソース Core からの出力方向のレプリケーションの削除 259
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 259
レプリケートされたデータのリカバリ 260
イベント 262
タスク、アラート、およびジャーナルページを使用したイベントの表示 262
タスクの表示 263
任意の Core コンソールページからの実行中タスクの表示 264
スケジュールされたタスクの一時停止または再開 265
アラートの表示 266
ログ記録されたすべてのイベントのジャーナルを表示 267
タスク、アラート、およびイベントのジャーナル間の移動 268
Rapid Recovery のイベント通知について 269
通知グループの設定 270
電子メール通知について 273
電子メールサーバの設定 274
電子メール通知テンプレートの設定 275
イベント設定の構成 278
繰り返し回数の削減について 278
繰り返し回数の削減の設定 278
イベントの保持の設定 279
レポート 280
Rapid Recovery レポートについて 280
Core Console からのレポートの生成 281
オンデマンドでの Core レポートの生成 282
オンデマンドでの保護対象マシンのレポートの生成 284
Core Console からのスケジュールされたレポートの管理 286
レポートのスケジュール設定 286
レポートスケジュールの変更 289
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 290
レポート メニューの使い方 290
レポート ツールバーの使い方 291
ジョブレポートについて 293
ジョブサマリレポートについて 293
失敗レポートについて 294

サマリレポートについて 294
リポジトリレポートについて 296
従来のサマリレポートについて 296
VM のエクスポート 297
Rapid Recovery を使用した仮想マシンへのエクスポート 297
ESXi 仮想マシンへのデータのエクスポート 299
1 回限りの ESXi エクスポートの実行 299
ESXi への連続エクスポートのセットアップ 300
VMware Workstation 仮想マシンへのデータのエクスポート 302
1 回限りの VMware Workstation エクスポートの実行 303
Vmware Workstation への連続エクスポートのセットアップ 304
Hyper-V 仮想マシンへのデータのエクスポート 306
1 回限りの Hyper-V エクスポートの実行 307
Hyper-V への連続エクスポートのセットアップ 308
VirtualBox 仮想マシンへのデータのエクスポート 310
1 回限りの VirtualBox エクスポートの実行 310
VirtualBox への連続エクスポートのセットアップ 312
Azure 仮想マシンへのデータのエクスポート 313
Microsoft Azure での操作 314
Azure インタフェースの免責事項 314
Azure ストレージアカウントでのコンテナの作成 314
Microsoft Azure のマニュアル 315
Azure へ仮想エクスポートする前に 316
Azure への VM のエクスポートと展開 316
1 回限りの Azure エクスポートの実行 317
Azure への連続エクスポートの設定 321
Azure での仮想マシンの展開 322
エクスポートの管理 324
データのリストア 328
Rapid Recovery を使用したデータのリストアについて 328
Live Recovery について 328
リカバリポイントからのデータのリストア 329
ファイルの検索と復元の機能について 330
ファイルの検索および復元 331
データリカバリポイントからのボリュームのリストア 333
リカバリポイントからのボリュームのリストア 333
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 336
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 336

クラスタとクラスタノードの復元 337
接続されているアーカイブからの復元 337
Rapid Recovery によるメールのリストア 338
メールのリストアの前提条件 339
Rapid Recovery で Exchange データベースを開く 339
Rapid Recovery によるメールアイテムのリストア 340
ベアメタル復元 344
Windows マシンのベアメタル復元について 344
Windows マシンでのベアメタル復元の実行 345
Windows マシンに対してベアメタル復元を実行するための前提条件 346
マシンのリストアウィザードを使用したベアメタル復元の実行 346
Windows マシンのブート CD の作成について 350
ブート CD へのドライバの導入について 351
ブート CD の ISO イメージの作成 351
ブート CD の ISO イメージのメディアへの転送 353
ブート CD のロードおよびターゲットマシンの起動 353
BMR への Universal Recovery Console の使用 354
Universal Recovery Console ツールについて 354
Universal Recovery Console を使用したドライバのロード 355
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 355
Chromium を使用した URC でのドライバのロード 356
リカバリポイントの選択と BMR の開始 357
ベアメタル復元のためのディスクのマップについて 357
BMR のディスクの自動マッピング 358
BMR のディスクの手動でのマッピング 359
アーカイブからの BMR の実行 359
オペレーティングシステムへのドライバのロード 362
Linux マシンでのベアメタル復元の実行 362
Linux マシンに対してベアメタル復元を実行するための前提条件 364
Linux ブートイメージの管理 364
Linux 用のブート ISO イメージについて 365
メディアへの Live DVD の ISO イメージの保存 365
Live DVD のロードおよびターゲットマシンの起動 366
Rapid Recovery Core から BMR ターゲットへの接続 366
Linux パーティションの管理 366
宛先ドライブでのパーティションの作成 367
宛先ドライブでのパーティションのフォーマット 368
コマンドラインからのパーティションのマウント 368

Linux 用のベアメタル復元の開始 ... 369
Screen ユーティリティの開始 ... 369
コマンドラインを使用して Linux マシンに対してベアメタル復元を起動する ... 370
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 ... 372
ベアメタル復元の確認 ... 373
リカバリの進捗状況の表示 ... 373
リストアされたターゲットサーバの起動 ... 373
Universal Recovery Console への接続に関するトラブルシューティング ... 374
起動の問題の修復 ... 374
コマンドラインからのベアメタル復元の確認 ... 374
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 ... 375
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 ... 375
過去のデータ管理 ... 378
データの保持、セカンダリストレージの階層化、およびアーカイブ ... 378
保持ポリシーの管理 ... 379
Core のデフォルト保持ポリシー設定の指定 ... 379
保護対象マシンの保持ポリシー設定のカスタマイズ ... 381
保護対象マシンのロールアップの強制実行 ... 384
アーカイブあーかいぶ ... 385
アーカイブについて ... 385
アーカイブの作成およびストレージオプション ... 385
Amazon のストレージオプションとアーカイブ ... 386
アーカイブ用のリカバリポイントチェーンのオプション ... 387
アーカイブにアクセスする方法 ... 387
アーカイブの使用 ... 388
アーカイブの作成 ... 388
クラウドへのアーカイブ ... 392
スケジュール設定されたアーカイブの編集 ... 392
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 ... 395
アーカイブジョブの強制実行 ... 395
アーカイブのチェック ... 395
アーカイブのアタッチ ... 397
アーカイブのインポート ... 398
クラウドアカウント ... 401
クラウドアカウントについて ... 401
クラウドストレージオプションの検討 ... 402
クラウドアカウントの追加 ... 403
クラウドアカウントの編集 ... 406

クラウドアカウントの削除 406
Local Mount Utility 407
Local Mount Utility について 407
Local Mount Utility での Rapid Recovery Core マシンの操作 407
Local Mount Utility への Core マシンの追加 408
Local Mount Utility オプションの変更 409
Local Mount Utility での Core の接続設定の編集 410
Core への再接続 411
Local Mount Utility からの Rapid Recovery Core マシンの削除 411
Local Mount Utility での保護対象マシンの操作 411
Local Mount Utility を使用したリカバリポイントのマウント 411
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 412
リカバリポイントの更新 413
Local Mount Utility でのリカバリポイントのマウント解除 413
Core Console リファレンス 414
Core Console ユーザーインタフェースの表示 414
保護対象マシンの表示 422
保護対象マシンのイベントの表示 423
保護対象マシンの 詳細 タブの表示 425
Third-party contributions 426
Apache 2.0 432
Chromium BSD License N/A 434
Code Project Open License (CPOL) 1.02 435
Far Manager BSD License N/A 438
GNU AFFERO GENERAL PUBLIC LICENSE 438
GPL (GNU General Public License) 2.0 446
LGPL (GNU Lesser General Public License) 2.1 450
OpenSSL 1.0 455
Quest について 458
用語集 459

Copyright © 2018 Quest Software Inc.

無断転載を禁じます。

本書には、著作権によって保護されている機密情報が記載されています。本書で説明されているソフトウェアは、ソフトウェアライセンスまたは秘密保持契約の下で提供されています。本ソフトウェアは、適用契約の条件に従ってのみ使用またはコピーできます。本書のいかなる部分も Quest Software Inc. の書面による許可なしに、購入者の個人的な使用以外の目的で、複写や記録などの電子的または機械的ないかなる形式や手段によっても複製または転送できません。

本書には、Quest Software 製品に関連する情報が記載されています。明示的、黙示的、または禁反言などを問わず、本書または Quest Software 製品の販売に関連して、いかなる知的所有権のライセンスも付与されません。本製品の使用許諾契約の契約条件に規定されている場合を除き、QUEST SOFTWARE はいかなる責任も負わず、製品に関連する明示的、黙示的または法律上の保証（商品性、特定の目的に対する適合性、権利を侵害しないことに関する黙示的保証を含む）を放棄します。いかなる場合も、本書の使用または使用できないことから生じる直接的、間接的、結果的、懲罰的、特殊的、偶発的損害（利益損失、事業中断、または情報損失の損害を含む）について、かかる損害の可能性を DELL が報告を受けたとしても、QUEST SOFTWARE は一切の責任を負わないものとします。Quest Software は、本書の内容の正確性または完全性について、いかなる表明または保証も行わず、通知なしにいつでも仕様および製品説明を改変する権利を有します。Quest Software は、本書の情報を更新する一切の義務を負いません。

本書の使用について質問がある場合は、下記までお問い合わせください。

Quest Software Inc., Attn: LEGAL Dept., 4 Polaris Way, Alisa Viejo, CA 92656.

支社および国際オフィスについては、弊社の Web サイト（https://www.quest.com/jp-ja）を参照してください。

特許

Quest Software は、自社の先進技術に誇りを持っています。特許および出願中の特許が本製品に適用される場合があります。本製品に適用される特許の最新の詳細については、弊社の Web サイト（https://www.quest.com/legal）を参照してください。

商標

Quest、Quest ロゴ、および Join the Innovation は、Quest Software Inc. の商標および登録商標です。Quest マークの完全なリストについては、https://www.quest.com/legal/trademark-information.aspx を参照してください。その他の商標および登録商標は、それぞれの所有者に帰属します。

凡例

WARNING: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

CAUTION: 注意アイコンは、指示に従わなかった場合に、ハードウェアの損傷やデータ損失につながる可能性があることを示します。

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: 情報アイコンは、サポート情報を示します。

Rapid Recovery への概要

Rapid Recovery は、ほぼゼロに近いリカバリ時間目標とリカバリポイント目標を提供するバックアップ、レプリケーション、およびリカバリソリューションです。Rapid Recovery では、データ保護、ディザスタリカバリ、データ移行および管理の機能が提供されます。Rapid Recovery には、ベアメタルリストアを（類似または異種のハードウェアに対して）実行する柔軟性があり、元のマシンの形態に関わらず、バックアップを物理マシンまたは仮想マシンにリストアすることができます。Rapid Recovery では、クラウド、DL シリーズのバックアップおよびリカバリアプライアンス、または希望の対応システムへのアーカイブも可能です。Rapid Recovery を使用して、冗長性とセキュリティを強化するために 1 つ以上のターゲットにレプリケートできます。

Rapid Recovery では次の機能を提供します。

- **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など、複数のプラットフォームに対して Universal Recovery を実行できます。
- **クラウドの統合**。VM をエクスポートし、クラウドにアーカイブおよびレプリケートして、クラウド内のアーカイブからベアメタル復元を実行できます。互換性のあるクラウドサービスには、Microsoft Azure、Amazon Web Services（AWS）、OpenStack ベースのプロバイダ（Rackspace を含む）、Google Cloud などがあります。米国政府固有のプラットフォームには、AWS GovCloud（US）および Azure Government などがあります。
- **高度な重複排除**。データを 1 度格納し、それ以降はそのデータを参照することで、ストレージ要件を削減できます（リポジトリまたは暗号化ドメインごとに 1 度）。
- **即時リカバリ**。Live Recovery 機能では、重要なデータに最初にアクセスし、残りの復元操作を並行して実行します。
- **ファイルレベルのリカバリ**。オンプレミスのファイルレベルで、リモートの場所またはクラウドからデータをリカバリできます。
- **ファイルレベルの検索**。指定された条件を使用して、1 つまたは複数のファイルについて一定範囲のリカバリポイントを検索できます。検索結果で、Core Console から直接希望するファイルを選択して、ローカル Core マシンに復元できます。
- **仮想サポート**。Rapid Recovery では 1 回限りの仮想エクスポートがサポートされ、リカバリポイントから起動可能な VM を生成できます。また、生成した起動可能な VM が各バックアップ後に継続的に更新される、仮想スタンバイもサポートされます。Microsoft Hyper-V クラスタの共有ボリュームに仮想エクスポートを実行することもできます。
- **Rapid Snap for Virtual のサポート**。仮想化のサポート強化には、vCenter/ESXi VM および Hyper-V VM のエージェントレス保護が含まれます。Rapid Snap for Virtual には、エージェントのソフトウェアがインストールされていない VMware ESXi 5.5 以上に対応する保護と自動検出が含まれています。ホストベースの保護は、Microsoft Hyper-V ホストでのみ Rapid Recovery Agent のインストールをサポートし、そのすべてのゲスト VM をエージェントレスで保護できます。
- **アプリケーションサポート**。Rapid Recovery Agent は、Microsoft Exchange、SQL Server、および Oracle に対するアプリケーションサポートにより構築されています。Core でこれらのアプリケーションサーバを保護するとき、バックアップスナップショットは自動的にアプリケーションアウェアになります。この場合、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、キャッシュがディスクに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。SQL アタッチ可否（SQL Server の場合）およびデータベース整合性 DBVERIFY チェック（Oracle の場合）を含む、特定のアプリケーション機能がサポートされます。アプリケーションアウェアネスは、SQL Server と Exchange Server のエージェントレス保護にも有効です。

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

- Rapid Recovery 製品サポートウェブサイト（https://support.quest.com/rapid-recovery/）。
- マニュアルウェブサイト（https://support.quest.com/rapid-recovery/technical-documents/）。

Core Console

本項では、Rapid Recovery Core Console ユーザーインタ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。
    1. 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。
    2. 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/

NOTE: 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。

NOTE: 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。

NOTE: 「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 1.「クイックスタートガイド」の設定タスク

関数	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 **クラスタの保護** を選択し、クラスタに接続 ダイアログボックスを開きます。クラスタの保護の詳細については、「クラスタの保護」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仮想スタンバイ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」を参照してください。
管理と設定	Rapid Recovery Core の追加設定をセットアップできます。	管理または設定することができるその他の機能を参照するには、**その他** をクリックします。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。
暗号化の設定	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」のトピックで説明されています。
通知の設定	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

関数	簡単な説明	タスクの選択結果、手順へのリンク
		トピック、さらに「通知グループの設定」と「電子メールサーバの設定」のトピックも参照してください。
保持の管理	Core のデフォルト保持ポリシーを表示または変更します。	**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、データリカバリポイントからのボリュームのリストア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。

    NOTE: 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。

    NOTE: 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 アイコンをクリックすると、 ページが表示されます。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 ダッシュボードレポートについて」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。アイコンバーからアクセスできるオプションには、レプリケート、仮想スタンバイ、イベント、設定、および その他 が含まれます。
- アイコンバーの (その他) 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。ボタンには、保護、復元、アーカイブ、および レプリケート が含まれます。

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 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。例:

- 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。

各ページで使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、「「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。

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。

See also: 保護対象マシンのサマリ情報の表示
See also: ホストのサマリ情報の表示
See also: レプリケーション
See also: カスタムグループについて

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  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。**ホーム** ページでは、**ダッシュボード ホーム** が導入され、使い慣れた **サマリ表** ビューを表示できます。サマリ表はデフォルトのビューです。

ホーム ページの右上にあるダッシュボード切り替えアイコン  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、次のトピックをお読みください。

- 左側のナビゲーションエリアについて
- Core ダッシュボードレポートについて
- ホーム ページ (サマリテーブルビュー) について
- Core Console ユーザーインタフェースの表示

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 2. ホーム ページのオプション

UI エレメント	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。

UI エレメント	説明
	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、重複排除ボリュームマネージャ（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。

UI エレメント	説明
	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が示されます。 • **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、「リポジトリについて」を参照してください。
警告	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。 • **日付**。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、およびジャーナルページを使用したイベントの表示」を参照してください。

Core ダッシュボードレポートについて

Core ダッシュボードには、Core、保護対象マシン、およびリポジトリに保存したスナップショット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。ダッシュボードレポートには次のものがあります。

- Core システムレポート
  - **障害モニタ**。このレポートには、ジョブのアクティビティ、ライセンスポータルとの接続、および転送アクティビティが表示され、システム上の問題が初期検出されます。クロックウィジェットをクリックすると、追跡されたすべてのアクティビティがクリアされ、新しいイベントが監視されます。
  - **リポジトリ**。このレポートには、Core に関連付けられたリポジトリが表示されます。リポジトリの数、各リポジ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。
- マシンレポート
  - **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。
- スナップショットレポート
  - **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。

ダッシュボード ペインの上部で （展開）ウィジェットをクリックすると、ダッシュボードに表示されるレポートのリストが上記の 3 つカテゴリで表示されます。各レポートカテゴリとレポートにはチェックボックスがあります。このチェックボックスを選択すると、レポートまたはカテゴリがダッシュボードに表示されます。オプションを選択解除すると、レポートは表示されません。このようにして、ダッシュボードに表示するレポートを簡単に変更できます。 （縮小）をクリックすると、メニューが非表示になります。

レポートのヘッダーで上下矢印をクリックして、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こともできます。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列できます。

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して、メニューを表示します。

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。

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。任意のクラスタのドロップダウンメニューからも、選択したクラスタの **保護対象ノード** ページに移動できます。

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、「」を参照してください。

NOTE: **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。

See also: 「サマリ」ペインの表示
See also: 保護対象マシンでのボリュームの表示
See also: レプリケーション情報の表示
See also: Exchange Server 情報 ペインの表示
See also: SQL Server 情報 ペインの表示
c_Viewing_summary_information_for_a_host.xml

「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。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、「シンプルモードでのカスタム保護スケジュールの作成」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、「スナップショット作成の強制実行」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 icrosoft 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。

ホストのサマリ情報の表示

Core Console でハイパーバイザホストまたはクラスタホスト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。このページには、少なくとも、機能のアクションバー、サマリ ペイン、および プロセッサ ペインがあります。アクションバーは、ホストの全ページの上部に表示されます。サマリ ペインには、ホスト名および仮想化ソフトウェアなどの情報が表示されます。プロセッサ ペインには、各プロセッサのアーキテクチャ、Core の数、スレッドの数、クロックスピード、および説明を一覧した表が表示されます。

マシンのホストタイプに応じて、次のような他のペインも表示されます。

- **SMB サーバ**。Hyper-V ホストで 1 つ以上の SMB サーバを使用している場合、このセクションに各 SMB サーバのホスト名がリストされます。
- **ノード**。クラスタホストの **サマリ** ページには、各ノードのホスト名および Rapid Recovery のバージョン番号をリストするセクションがあります。
- **ボリューム**。エージェントレス保護を使用している場合、Hyper-V ホストの **サマリ** ページには、各保護対象ボリュームの名前、ファイルシステム、使用容量、現在のスケジュール、および次回のスナップショットをリストするセクションがあります。
- **共有ディスク**。エージェントレス保護を使用している Hyper-V ホストに 1 つ以上の共有 VHDX がある場合、このセクションに各仮想ハードディスクの名前とパスがリストされます。

CSV クラスタの詳細については、『*Rapid Recovery #########*』の「Support for Cluster Shared Volumes」（クラスタ共有ボリュームのサポート）を参照してください。その他の関連トピックについては、次のリンクを参照してください。

- 保護対象マシンのサマリ情報の表示
- Rapid Snap for Virtual について

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 3. リカバリポイントのサマリ ペインのデータ

UI エレメント	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。

UI エレメント	説明
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、「」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 で実行する必要のあるジョブ。
- **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 4. イベント ページの要素

UI エレメント	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。
リストア元	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。

UI エレメント	説明
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
 (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 5. イベントのサマリ表の詳細情報

UI エレメント	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(N)	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。
終了時間	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。
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。失敗したジョブの場合、失敗レポートで詳細を表示することができます。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、「ソース Core からの出力方向のレプリケーションの削除」または「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。

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。

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
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

「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の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。

CAUTION: 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 Recovery Core Console ユーザーインタフェー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。

ユーザーインタフェースエラーが原因で 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 ページ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 Core AppRecovery.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、Rapid Recovery Core の設定の管理および変更方法について説明し、Core Console から使用可能な主な機能ボタンとツールについて説明します。

Rapid Recovery Core の調整可能な設定は、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、Core Console で表示される情報や、Rapid Recovery Core のパフォーマンスに影響します。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。

主要な一連の機能が、ボタンとしてページの上部に水平に表示されます。これらの機能のいずれかにアクセスするには、対応するボタンをクリックします。これらのボタンの詳細については、「Core 設定の主な機能」を参照してください。

主要な機能ボタンの下には、変更可能な Core 設定があります。いずれかの設定のすべての設定オプションを表示するには、設定 ペインの左側にあるショートカットリンクをクリックするか、ページの右側をスクロールダウンします。すべての Core 設定の詳細については、「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。

Core 設定の主な機能

主要な一連の機能が水平に並んだボタンとして、（設定）ページの上部に表示されます。これらの機能のいずれかにアクセスするには、対応するボタンをクリックします。

設定 ページでアクセスできる機能ボタンの説明を、次の表に示しています。

表 6. Core 設定の主な機能

主な機能ボタン	説明
バックアップ設定	Core 構成の設定を、指定した XML ファイルにバックアップします。Core サーバのローカルの完全修飾パスを指定します。
リストア設定	Core 設定のバックアップ XML ファイルがある場合、このオプションでそのファイル名とローカルパスを指定して、Core 設定のリストア元として使用できます。この機能を使用して Core 設定をリストアしたり、別の Core から移行したりすることができます。必要に応じて、リポジトリをリストアすることもできます。
Core サービスを再起動	このオプションは、Core サービスを正常にシャットダウンして再起動します。
Core サービスをシャットダウン	このオプションは、Core サービスを正常にシャットダウンします。

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。

Core サービスのシャットダウンと再起動の詳細については、「Core サービスの再起動またはシャットダウン」を参照してください。

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。

NOTE: 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** または **リストア設定** オプションが表示されます。
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\RRCoreSettings` と入力し、**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。

   NOTE: 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** ページの一番上で **リストア設定** 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\RRCoreSettings` と入力します。

   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、およびジャーナルページ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、「暗号化キーのアンロック」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仮想スタンバイが設定されている場合、正常な同期を実現するには、仮想スタンバイ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 のエクスポート」を参照してください。
- クラウド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 サービスの再起動またはシャットダウン

通常、Rapid Recovery Core が実行されているマシンはシャットダウンします。または再起動する必要があります。リリース 6.2.1 では、Rapid Recovery Core が強化され、Core サービスを正常にシャットダウンして再起動する機能が向上しました。

Core の UI には、ワンクリックで Core サービスを再起動またはシャットダウンするための UI 機能が追加されました。この機能は、Core サーバの計画されたメンテナンス（リブートまたは再起動を含む）が必要な場合に便利です。ユーザーは、対応するサービスのシャットダウンが完了したときに通知を受け取ります。これらの機能は、Core 設定 ページの上部からアクセスできます。

NOTE: 正常なシャットダウンがサポートされるもう 1 つの便利な機能は、Core で将来のタスクのスケジュールを一時停止する機能です。詳細については、「スケジュールされたタスクの一時停止または再開」のトピックを参照してください。

次の手順を使用して、Core サービスを再起動またはシャットダウンします。

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。

   設定 ページが表示されます。設定 ペインの上部にある設定のカテゴリの上に、**Core サービスを再起動** または **Core サービスをシャットダウン** のオプションが表示されます。

3. Core サービスを再起動する場合は、設定 ペインの上部にある **Core サービスを再起動** をクリックします。

再起動前に完了する必要がある各タスクのリストが表示されます。タスクの進行状況も表示されます。

4. 必要に応じて、以下のいずれかの作業を行うことができます。
    a. 再起動を強制するには (タスクが完了する前に明示的に停止される正常ではないプロセス) 、**再起動を強制** をクリックします。
    b. Core サービスの再起動をキャンセルするには、**キャンセル** をクリックします。
5. Core サービスを、すぐに再起動せずにシャットダウンする場合は、設定 ペインの上部にある **Core サービスをシャットダウン** をクリックします。
6. 必要に応じて、以下のいずれかの作業を行うことができます。
    a. シャットダウンを強制するには (タスクが完了する前に明示的に停止される正常ではないプロセス) 、**シャットダウンを強制** をクリックします。
    b. Core サービスの再起動をキャンセルするには、**キャンセル** をクリックします。

関連タスク

See also: スケジュールされたタスクの一時停止または再開

Rapid Recovery Core の設定

設定 ペインの左側には、各 Core 設定が表示されたナビゲーション列があります。このリストの任意のリンクをクリックするか、ページの右側で下へスクロールして、各 Core 設定のすべての設定オプションを確認することができます。

変更する設定をクリックすると、その設定が編集可能なコントロールになります。次のいずれかを実行します。

- コントロールがドロップダウンメニューである場合、下向き矢印をクリックしてオプションを表示し、メニューから目的のオプションを選択します。
- コントロールがテキストフィールドである場合は、値を入力します。
- オプションに はい または いいえ が表示されたときは、値をクリックすると、チェックボックスに置き換えられます。はい の設定には、チェックボックスを選択します。いいえ の値には、チェックボックスをクリアします。
- オプションに日時の値 (たとえば、時、分、秒を表示している場合) 、それぞれのコンポーネントをクリックして、新しい値を入力するか上下の矢印を使用して新しい値を選択します。

各設定の変更が完了したら、✔ をクリックして変更内容を確認して保存し、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。

構成可能な Rapid Recovery Core 設定については、次の表で説明します。それぞれの設定に対し、詳しい情報が含まれている関連トピックへのリンクが示されています。

表 7. Rapid Recovery Core の構成可能な設定

構成設定	説明
全般	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。
更新	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。

構成設定	説明
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。通常の業務時間外にジョブのスケジュールを設定して、リソースの需要が高いとき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、「夜間ジョブについて」、「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。
展開	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の設定	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の設定 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

構成設定	説明
	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	Core の Simple Mail Transfer Protocol (SMTP) サーバ設定を構成して、Core のイベント情報を電子メールで送信します。 SMTP 電子メールサーバの設定の詳細については、「電子メールサーバの設定」を参照してください。 **NOTE:** 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。
クラウドアカウント	クラウドアカウント 設定では、サポート対象のクラウド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、既存の外部クラウドストレージまたはクラウドサービスプロバイダアカウントを 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。クラウドアカウントのタイムアウト設定を設定する方法の詳細については、「クラウドアカウント接続設定の構成」を参照してください。 Rapid Recovery Core Console でのクラウドアカウントの管理の詳細については、「クラウドアカウント」を参照してください。
Azure 管理証明書	Core Console で Azure サブスクリプションの情報を利用できるようにするには、Azure 管理証明書をロードして Core に関連付ける必要があります。Core Console では、新しい証明書のロード、現在 Core に関連付けられている証明書の表示の更新、現在 Core に関連付けられている Azure 証明書の削除を行うことができます。 Core で Azure 管理証明書を使用する方法の詳細については、「Core に関連付けられた Azure 管理証明書の操作」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設定パラメーターがあります。レポートの用紙サイズとページの向きを設定することもできます。 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。
アタッチの可否	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。試行回数 を使用して、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、1 日あたり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。

構成設定	説明
	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、「*Rapid Recovery ################*」を参照してください。 **NOTE:** 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、Quest Technical Documentation ウェブサイトを参照してください。
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 を使用する方法については、「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。
VMware プロキシ	ユーザーは、Core とともにインストールされた VMware プロキシサービスを使用して、VMware ディスクストレージに関連付けられたサービスタイムアウトを設定できます。これらの設定の詳細については、VMware のプロキシ設定の管理を参照してください。
Data Protection ポータル	2 つ以上の Core を管理している場合は、Core サーバを Quest Data Protection ポータルと統合することができます。 この機能は特にマネージドサービスプロバイダに有用で、単一のウェブベースのユーザーインタフェースから、複数の Core の管理、タスクとイベントを監視できるダッシュボードへのアクセス、リポジトリステータスの表示、システムの正常性のチェック、および増加するその他の機能の実行が可能です。 ポータルへのアクセスを有効または無効にするには、この設定を使用します。
vFoglight	Quest の Foglight for Virtualization (vFoglight) は、管理者が VMware、Hyper-V、および OpenStack 環境のハイパーバイザを監視、分析、および最適化する際に役立ちます。vFoglight を使用して VM を管理し、Rapid Recovery Console で VM を保護するユーザーは、この Core 設定を使用して 2 つの製品のナビゲーションを統合できます。vFoglight 設定を正常に入力した後、Core Console の VM の **サマリ** ページで vFoglight URL をクリックすると、ユーザーは、vFoglight でその仮想マシンの対応するページに移動します。 vFoglight Core 設定の詳細については、「vFoglight 設定の構成」を参照してください。vFoglight の詳細については、Quest ウェブサイトの vFoglight 製品ページ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。

Core 一般設定の構成

Rapid Recovery Core の一般設定には、Core ID、表示名、Web サーバポート、サービスポート、およびロケール（Core Console 表示言語）およびディスプレイのカラーテーマがあります。

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、**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。
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
Core ID	Core ごとに固有の Core ID があります。この ID は、Core と Data Protection ポータルを統合して、2 つ以上の Core のレポートまたは管理機能を提供する場合などに使用されます。Core ID は 一般 設定に表示されます。 **NOTE:** このフィールドを設定することはできません。
表示名	Core の新しい表示名を入力します。これは、Rapid Recovery Core Console および（有効な場合）Data Protection ポータル に表示される名前です。64 文字まで入力できます。
Web サーバポート	Web サーバのポート番号を入力します。デフォルトのポートは8006です。 **NOTE:** Quest では、デフォルトポートの使用をお勧めします。
サービスポート	Rapid Recovery Core サービスに使用するポート番号を入力します。デフォルトのポートは8006です。 **NOTE:** Quest では、デフォルトポートの使用をお勧めします。
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。 **NOTE:** 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。このサービスは、Core 設定ページの上部から **Core サービスを再起動** ボタンを使用して再起動できます。
主題	**テーマ** ドロップダウンリストで、Core Console に適用するスタイルを選択します。次のカラーテーマが使用できます。 • **暗色**。このテーマでは、インタフェース全体（左側ナビゲーションメニュー、上部ボタンバー、およびプライマリペイン）に無地の濃いグレーの背景を使用しま

テキストボックス	説明
	す。フォーカスされていないテキスト要素とテキストボタンは、オフホワイトで表示され、フォーカスされると白で表示されます。クリック可能なリンクは中濃度の青色で表示されます。状況に応じて表示されるボタンの背景は中濃度の青色でテキストは白色です。 • **混合**。このテーマでは、Core Console の左側ナビゲーションメニューと上部のボタンバーに見やすいグレーの背景を使用します。これらの領域のテキスト要素は白色です。プライマリペインの背景は白色でハイライトはオフホワイトです。テキスト要素とテキストボタンは黒色です。クリック可能なリンクは濃い青で表示されます。状況に応じて表示されるボタンの背景は青色でテキストは白色です。 • **明色**。このテーマでは、インターフェイス全体（左側ナビゲーションメニュー、上部ボタンバー、およびプライマリペイン）に白い背景を使用します。Quest 口ゴおよび一部のデザイン要素はオレンジ色です。テキスト要素は濃いグレーで、タイトルは黒で表示されます。マウスオーバーするとクリック可能なリンクが青で表示されます。状況に応じて表示されるボタンの背景は中濃度の青色でテキストは白色です。
個人データの使用に同意する	アプリケーションに個人情報の使用を許可する設定を変更するには、**個人データの使用に同意する** ドロップダウンリストから、必要に応じて、**はい** または **いいえ** を選択します。表示されるダイアログボックスで、適切なライセンスファイルを選択し、登録します。 Rapid Recovery Core をアップグレードまたはインストールするときは、個人情報の共有を設定するオプションがあります。Quest と情報を共有することに同意した場合は、自動アップデートや Data Protection ポータル（以後はデフォルトで有効になります）などの機能を利用できます。 インストール時に Quest と情報を共有することを拒否した場合は、Phone Home 以外のライセンスを登録するように求められます。変更を確認して保存するには、Phone Home 以外のライセンスへのアクセス権を持っている必要があります。 インストール時に選択したオプションに関係なく、Core 一般設定で **個人データの使用に同意する** 設定を変更できます。この操作では、Phone Home 以外のライセンスをアップロードするように求められるため、Phone Home 以外のライセンスへのアクセス権を持っていることを確認します。 リリース 6.2.1 で、この設定を はい から いいえ に変更するとき、以下が適用されます。: a. Phone Home 以外のライセンスファイルをアップロードするように求められます。 b. Phone Home 以外のライセンスを確認した後、Core のアップデートをチェックまたはインストールしないように Core の アップデート 設定が自動的に調整します。 c. Data Protection ポータル設定 Data Protection ポータルへの接続の有効化 が いいえ に設定されます。 ただし、その反対は同じようになりません。この設定を いいえ から はい に変更するとき、Core に自分の情報を共有する許可を与えますが、ライセンスを明示的に Phone Home モードに変更し、該当する Core 設定をアップデートするまで情報は共有されません。例: a. Phone Home 以外のキーは、標準の Phone Homeキー（ライセンスポータルから入手できます）を明示的にアップロードするまで、登録されています。 b. 自動アップデートを使用するには、新規アップデートのチェック を 無期限 から 毎日、毎週、または 毎月 に変更します。必要に応じて、アップデートをインス

テキストボックス	説明
	トール をユーザーに通知するように、またはアップデートを自動的にインストールするように変更します。
	c. Data Protection ポータル と情報を共有するには、データプロテクションポータルへの接続の有効化 を はい に設定します。

> **NOTE:** 最初にこれを設定した場合は、Phone Home ライセンスをアップロードするように求められます。

個人情報の共有による影響を理解するには、「プライバシーの管理」、さらに「Rapid Recovery が個人情報を使用する方法」のトピックを参照してください。

Phone Home 以外のモードを使用しているときに使用できない機能の詳細については、「Phone Home 以外のライセンスの制限」のトピックを参照してください。

Phone Home 以外のモードのライセンスを要求するには、「Phone Home 以外のライセンスの取得と使用」を参照してください。

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。

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するかどうか、およびアップデートのチェック頻度を選択できます。

> **NOTE:** 自動アップデート機能には、標準の Phone Home モードを使用するライセンスが必要です。Phone Home 以外のモードでソフトウェアライセンスを使用する場合、Core には Rapid Recovery ライセンスポータル と通信する権限がなく、Core をアップデートすること、または利用可能なアップデートについてユーザーに通知することはできません。詳細については、「プライバシーの管理」を参照してください。

通常、Rapid Recovery リリース番号は、メジャーリリース番号、マイナリリース番号、リビジョン、およびビルド番号の 4 つの固有情報が、それぞれ小数点で区切られて構成されています。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。

> **NOTE:** Rapid Recovery Core ソフトウェアのインストール方法については、『*Rapid Recovery ########## ##########*』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。

> **CAUTION:** **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、Quest では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。
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ます。次のいずれかのオプションを選択できます。 • 無期限 • 毎日 • 毎週 • 毎月 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、自動的には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。

夜間ジョブについて

夜間ジョブは、通常の営業時間外の事前に設定された時間に毎日実行される自動化タスクです。これらのジョブはメモリ集中型で、Rapid Recovery Core の負荷が低いときに最適に動作するさまざまな整合性チェックおよびデータ統合タスクが含まれます。

すべての夜間ジョブ、およびジョブを適用できる範囲を次の表に示します。夜間ジョブは、Core レベルで管理できます (Core 上のすべての保護対象マシンに適用されます) 。特定の保護対象マシンにも適用できる夜間ジョブでは、範囲に「保護対象マシン」と記載しています。

表 10. 夜間ジョブの情報

ジョブ名(J)	スコープ	説明
変更	該当なし	このコントロールにより、**夜間ジョブ** ダイアログボックスを表示します。ここで夜間ジョブごとの設定を有効 / 無効にしたり、変更したりすることができます。
夜間ジョブの時間	すべて	この設定は、夜間ジョブを開始するようにスケジュールされている時刻を表しています。Quest では、アクティビティの少ない時間に夜間ジョブを実行するよう Core を設定することをお勧めします。 デフォルトの時刻は午前 0 時です。
SQL データベースのアタッチ可否チェック	保護対象マシン	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。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。
Exchange データベースのチェックサムチェック	保護対象マシン	EDB データベース (EDB) ファイルを含むリカバリポイントの整合性をチェックします。 **NOTE:** Core で Exchange 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。
Oracle データベースの整合性をチェック	Core または保護対象マシン	DBVERIFY ユーティリティを使用して、Oracle データベースの整合性を確認します。 プロセス : • すべての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検査して、データファイルが有効で、データブロックが破損していないことを確認します。 • リカバリポイントをマウント解除します。
リカバリポイントの整合性チェック	Core または保護対象マシン	各保護対象マシンのリカバリポイントの整合性をチェックします。デフォルトでは、`Check integrity of recovery points` オプションが無効になっています。 プロセス : • すべての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て、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。
Hyper-V エージェントで孤		Rapid Recovery リリース 6.1.x エージェントレス保護を使用した Hyper-V ホストの場合、この夜間ジョブでは、アタッチおよびデタッチ操作ごとに Windows レジストリで作成された孤立キーを消去します。レジストリエン

ジョブ名(J)	スコープ	説明
立レジストリキーを消去		トリは無害ですが、時間の経過とともに累積するためパフォーマンスの低下につながります。 **NOTE:** リリース 6.2.1Rapid Recovery 以降では、Hyper-V エージェントレス保護のストレージメタデータを取得する方法が改善されており、レジストリエントリが作成されないようにします。
保護対象仮想マシンの VMware スナップショットの統合	Core または保護対象マシン	この夜間ジョブは、ネイティブ VMware API を使用して Rapid Recovery Agent ソフトウェアなしでマシンを保護している場合に関連します。 定期的に VMware スナップショットを統合する必要があります。この夜間ジョブを有効にすることで、これらの統合を日単位で実行できます。この夜間ジョブは、1 つのパラメータ (最大同時統合数) を含んでいます。このパラメータは 1 〜 100 の範囲の数値に設定する必要があります。
据え置き削除	Core	この設定により、夜間ジョブを実行するよう Core で指定された時間まで、リポジトリからのリカバリポイントの削除を保留できます。この設定を有効にすると、他の夜間ジョブの実行後、Core では「事前に削除フラグが付けられたレコードの削除」ジョブを実行する処理のみが行われます。このジョブでは、マークの付いたリカバリポイントがリポジトリからなくなるまで、または夜間ジョブの実行時間から 4 時間経過するまで、それらのリカバリポイントを削除する処理を行います。夜間ジョブを終了すると、その他のキューに登録されたジョブが再開されます。残った削除処理がある場合は、その削除処理は、次の日の夜間ジョブの実行まで他のタスクと並行してバックグラウンドで実行されます。 デフォルトでは、`Deferred Delete` オプションが無効になっています。 Quest では、バックアップのリカバリポイントの削除に関連する、転送処理におけるパフォーマンスの不具合が発生していない限り、この夜間ジョブは無効のままにすることを推奨します。 Quest では、このオプションを有効にする場合は、Core のジョブを見直して、削除対象としてマークされたリカバリポイントの大多数が 1 週間以内にリポジトリから削除されていることを確認することを推奨します。このアプローチは、最大転送パフォーマンスとリポジトリ容量の最大利用のバランスを取るのに役立ちます。
古いイベントおよびジョブの削除	Core	古いイベントを削除して、イベントデータベースのサイズを維持します。日数を設定可能で、デフォルト値は 30 日です。
Exchange のログの切り捨て	保護対象マシン	最新のリカバリポイントに合わせて Exchange データベーストランザクションログを切り捨てて、Exchange ログのサイズを維持します。 **NOTE:** Core で Exchange 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。
Oracle のログの切り捨て	保護対象マシン	Oracle のログの切り捨てを制御します。無効にしないかぎり、夜間ジョブを実行するたびに 1 日に 1 回切り捨てが発生します。 • 夜間ジョブの実行時に、Core の **自動** 削除ポリシー (デフォルトで有効) に従ってローカルに保存されたすべての Oracle ログを切り捨てることができます。現在の日付のログは、夜間ジョブが実行される前のバックアップスナップショットにも保持されます。 • 特定の保護対象 Oracle サーバにカスタムの削除ポリシーを選択できます。**最新を保持** ポリシーでは、Oracle ログが切り捨てられるまでの時間を指定できます。**指定された数を保持** ポリシーでは、指定し

ジョブ名(J)	スコープ	説明
		た数のログファイルを保持できます。ログファイルが増えた場合、古い Oracle ログから順に切り捨てられます。 • 夜間ジョブを無効にすると、相当量のログファイルが累積されます。この場合、「Oracle データベースログの手動による切り捨て」で説明しているようにユーザーは手動でもログファイルを切り捨てることができます。
SQL のログの切り捨て	保護対象マシン	最新のリカバリポイントに合わせてデータベーストランザクションログを切り捨てて、SQL Server ログのサイズを維持します。 **NOTE:** 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。
ロールアップ	Core または保護対象マシン	ポリシーで指定された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」することにより、バックアップデータの保持ポリシーを適用します。すべての保護対象マシンにデフォルトで適用される Core のポリシーをカスタマイズできます。デフォルトでは、ロールアップジョブが Core 全体に実行されます。または (展開) をクリックして保護対象マシンのビューを展開します。次に、Core ポリシーを使用してロールアップする一連の保護対象マシンを定義できます。 Core で設定されているデフォルトのポリシーとは異なる保持ポリシーを保護対象マシンで使用する方法については、「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。

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。

NOTE: 夜間ジョブのスコープ (「夜間ジョブについて」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、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 設定のリストで **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。
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、**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。
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。
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. 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。

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。

NOTE: ご使用の環境で特定の問題が発生している場合や、Quest 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。
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。 **NOTE:** 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。 **NOTE:** 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。 **NOTE:** 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。 **NOTE:** 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。

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。したがって、キャッシュのサイズは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 のデフォルト設定では、DVM リポジトリ用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を AppRecovery ディレクトリ内に配置します。このフォルダは Core マシンにインストールされます。

NOTE: 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\RepositoryMetaData\PrimaryCache
セカンダリキャッシュの場所	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache

設定	デフォルトの保存先
メタデータキャッシュの場所	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

これらのキャッシュの保存先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。

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 での重複排除」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、**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。
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

設定	説明
	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. 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。

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、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、Quest サポートから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。
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。

テキストボックス	説明
	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。デフォルトのポートは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 ポートの自動割り当てを行う場合は、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。
送信バッファのサイズ	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、Quest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。

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、**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。
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. 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。

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、このトランザクション情報をデフォルトで Core マシンのローカルにインストールされている 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。

NOTE: 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、およびジャーナルページ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。
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リストアします。
     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

Rapid Recovery Core の 設定 ページで利用できる接続設定の説明です。

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。 **NOTE:** 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(O)	データベース接続のポート番号を入力します。 **NOTE:** 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。 **NOTE:** 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(A)	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。

テキストボックス	説明
	NOTE: 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。
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。 **NOTE:** 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。 **NOTE:** 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。

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。

NOTE: Rapid Recovery Core から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、およびジャーナルページ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、**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。
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(A)	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. 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。

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、「電子メールサーバの設定」のトピックに記載されています。

NOTE: 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。

クラウドアカウント接続設定の構成

クラウドアカウント接続設定を指定すると、Rapid Recovery がクラウドアカウントに接続を試みてから操作が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 に移動します。
2. 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。

3. 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。
4. 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、次のいずれかのアクションを実行します。
   - カスタム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** 8,388,608 (バイト)
     - **読み取りバッファサイズ** 8,388,608 (バイト)
   - クラウドアカウント接続設定を変更するには、**編集** をクリックし、**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。

Core に関連付けられた Azure 管理証明書の操作

Rapid Recovery Core の設定で、Azure 管理証明書を Core に関連付けることができます。このプロセスにより、Core は Azure サブスクリプションに関する情報にアクセスし、その情報を Core Console から利用できるようになります。

たとえば、Azure への仮想エクスポートを実行する場合、証明書情報をロードした後に、適切な Azure サブスクリプションをドロップダウンボックスから選択できます。その後、そのサブスクリプションに関連付けられたオブジェクトは Core Console UI の他のコントロールからアクセスできるようになります (ストレージアカウント、コンテナなど) 。

Azure 管理証明書の情報は、Microsoft Azure 内で生成される公開設定ファイルに保存されています。1 つ以上の管理証明書を Core に追加できます。Core により資格情報は安全にキャッシュされます。

Core 設定から行う Azure 管理証明書の操作には、次のタスクが含まれます。

- Azure アカウントの公開設定ファイルの取得
- Azure 管理証明書のロード
- Azure 管理証明書の更新または削除

Azure アカウントの公開設定ファイルの取得

このタスクを実行するには、PowerShell が有効になっている Windows マシンを使用する必要があります。また、サービス管理者またはサービス共同管理者の役割が与えられた Azure アカウントにアクセスできることも必要です。

公開設定ファイルは、Azure で生成される XML ドキュメントです。このファイルには AzureServiceManagement API 定義と、Azure サブスクリプションに関する情報 (エンコードされた安全な資格情報、サブスクリプションのタイプ、および Azure 管理証明書) が含まれています。このファイルの拡張子は `.publishsettings` であり、ファイルの内容を示しています。公開設定ファイルがないと、Core を Azure アカウントに接続することはできません。

公開設定ファイルのコピーは、Azure アカウントにログインしている Windows マシンから取得できます。

CAUTION: **公開設定ファイルには、Azure アカウントの資格情報などの情報が含まれているため、Microsoft ではこのファイルを安全な場所に保管することを推奨しています。証明書をロードしたら、このファイルはローカルシステムから削除して構いません。**

Microsoft では、サブスクリプションごとの管理証明書の数を 100 個に制限しています。また、特定のサービス管理者のユーザー ID 下にあるすべてのサブスクリプションでも、管理証明書の数を 100 個までに制限しています。複数の Core から同じ Azure アカウントにアクセスする必要がある場合、公開設定ファイルを 1 回生成し、同じファイルを再利用して管理証明書を複数の Core にロードできます。このようにすると、証明書生成の制限数を超過しないようにできます。

NOTE: この制限の詳細については、Microsoft KB 文書「Azure Cloud Services の証明書の概要」（https://docs.microsoft.com/ja-jp/azure/cloud-services/cloud-services-certs-create）の「制限事項」セクションを参照してください。

次の手順を実行して、公開設定ファイルを取得します。

1. Windows マシンで Azure ダッシュボードにログインします。
2. Azure にログインした状態で、別のブラウザウィンドウを開きます。
3. ブラウザの URL に次のアドレスを入力し、PowerShell スクリプトを実行してファイルをダウンロードします。`https://manage.windowsazure.com/publishsettings/index?client=powershell`

   正常に実行されると、公開設定ファイルがデフォルトのダウンロードディレクトリに保存されます。
4. このファイルを Core Console にアクセス可能なマシンに移動します。

Azure サブスクリプション情報を Rapid Recovery Core に関連付けるには、『*Rapid Recovery #######*』のトピック「Loading an Azure management certificate」（Azure 管理証明書のロード）を参照してください。

Azure 管理証明書のロード

このタスクを実行するには、適切な Azure アカウントの公開設定ファイルが必要です。このファイルにアクセスする方法については、「Azure アカウントの公開設定ファイルの取得」を参照してください。

Azure 管理証明書を Core にロードすると、Core Console は Azure アカウントのサブスクリプション情報にアクセスできます。Core Console に、Azure サブスクリプションに関連付けられたオブジェクトが表示されます。

次の手順を実行して、Azure 管理証明書を Core にロードします。

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、**Azure 管理証明書** をクリックします。
   - 設定 ページの右側で、Azure 管理証明書 の見出しが表示されるまで下にスクロールします。
3. Azure 管理証明書 の見出しの下にある、**証明書のロード** をクリックします。

   証明書のロード ダイアログボックスが表示されます。
4. **証明書のロード** ダイアログボックスで、**参照** をクリックします。

   ファイルアップロード ウィンドウが表示されます。
5. 公開設定ファイルが存在する場所に移動し、ファイルを選択し、**開く** をクリックします。

   ファイルアップロード ウィンドウが閉じ、Azure 管理証明書が、Core Console にロードされます。

Azure 管理証明書の更新または削除

Azure 管理証明書を Core Console から削除するには、証明書が Core にロードされ、その Core と関連付けられている必要があります。証明書を Core に関連付ける方法については、「Azure 管理証明書のロード」を参照してください。.

次の手順を実行して、Core に関連付けられた Azure 管理証明書の表示を更新するか、Core から証明書を削除します。

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、**Azure 管理証明書** をクリックします。
   - 設定 ページの右側で、Azure 管理証明書 の見出しが表示されるまで下にスクロールします。
3. Core Console 内の証明書の表示を更新するには、Azure 管理証明書 の見出しの下にある、**更新** をクリックします。

   Core 設定 ページが更新され、Core に関連付けられている証明書に関する情報が更新されます。
4. Core から証明書を削除するには、該当する証明書の をクリックし、**削除** を選択します。
5. 確認のダイアログボックスでクリックして証明書の削除を確認します。

   ダイアログボックスが閉じ、選択した Azure 管理証明書が Core から削除されます。

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」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、**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
デフォルトにリストア	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(F)	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。デフォルトの書体は Trebuchet MS 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。デフォルトは

オプション	説明
	レターです。次のいずれかの用紙サイズを選択できます。 • A3 • A4 • B4 • エグゼクティブ • Ledger • Legal • Letter • Tabloid
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 横です。次のいずれかのレイアウトオプションを選択できます。 • 横方向 • 縦方向

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. 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。

   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動している場合は、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。

保護対象マシンの SQL Server インスタンスを使用してアタッチ可否を実行する機能は、Rapid Recovery Agent ソフトウェアの機能です。SQL Server が、エージェントレスで保護されている場合、この機能は動作しません。したがって、SQL マシンでエージェントレス保護を使用している場合は、この手順の手順 3 に示すように、この Core 設定を **Core で SQL Server を使用** に構成します。

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。

  NOTE: 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。

NOTE: 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

SQL Server への接続を認証するために必要な情報についての説明です。

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(W) • SQL
ユーザー名(A)	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(A)	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. **Test Connection** (テスト接続) をクリックします。

NOTE: 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 のジョブ設定を表示または編集する場合、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(J)	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： • 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	1	0	デフォルト

ジョブ名(J)	説明	最大同時実行ジョブ数	試行回数	設定
	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
リモートリ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、出力方向の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

ジョブ名(J)	説明	最大同時実行ジョブ数	試行回数	設定
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(A)
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(A)
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(A)
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(A)
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(A)
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(A)
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(A)
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(A)
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(A)

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

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 ー 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 ー 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、**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 ー 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 ー 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。

  NOTE: 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。

  NOTE: 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、**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

Rapid Recovery ソフトウェアライセンスには次の 3 つのタイプがあります。

- **試用版**は、14 日が経過するとスナップショットの作成を停止します。
- **サブスクリプション版**には有効期限がありますが、
- **永久版**には有効期限がありません。

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。14 日が経過した後、必要に応じ、グループ管理者は試用版ライセンスを 28 日間に延長できます。あるいは、サブスクリプション版または永久版のライセンスを購入して登録できます。

NOTE: 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。

Rapid Recovery では、ライセンスをファイルで提供します。Rapid Recovery ライセンスファイルには、保護するマシンに配布できるライセンスのプールが含まれています。このプールは Rapid Recovery ライセンスポータル に反映されます。上に挙げたライセンスのタイプごとに、2 つのタイプのライセンスプールがあります。

- **エンタープライズ**。このプールに含まれる各ライセンスは、使用されている容量にかかわらず、インストールされた Rapid Recovery Agent ごと、またはエージェントレス保護を使用しているハイパーバイザホスト上のソケットごとに適用されます。
- **容量**。これらのライセンスは、インストールされた Rapid Recovery Agent や保持しているソケットの数にかかわらず、保護する予定のデータ量（テラバイト（TB）単位）に対して適用されます。購入したライセンスに割り当てられた容量を超過したら、別のライセンスを購入する必要があります。容量ライセンスの場合：
  - DL Appliance では、ライセンスで指定されている容量がアプライアンスで使用できるリポジトリのサイズ（TB 単位）を制限する、バックエンド容量ライセンスモデルを使用します。
  - ソフトウェアのインストールでは、ライセンスで指定されている容量が、保護対象のマシンからリポジトリに保存できるデータ量（TB 単位）の制限を指定する、フロントエンド容量ライセンスモデルを使用します。フロントエンド容量は、圧縮と重複排除の前に測定されます。

リリース 6.2.1 では、1 つの Core で使用できるライセンスプールタイプは 1 つのみです。たとえば、Core で容量ベースのライセンスプールを使用している場合、エンタープライズライセンスプールを併用することはできません。この逆についても同じです。

1 つのライセンスファイルに複数のタイプのライセンスプールを組み合わせて含めることはできません。たとえば、エンタープライズライセンスプールと容量ライセンスプールを同じ永久版ライセンスに含めることはできません。

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。以下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。
- DL シリーズアプ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 <アプ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。

Rapid Recovery は、標準の Phone Home モードと、複数の制限のある Phone Home 以外のモードの 2 つのモードでこれらのライセンスタイプをサポートします。サブスクリプションライセンスは、Phone Home モードでのみ動作します。永久版ライセンスと試用版ライセンスは、Phone Home ライセンスまたは Phone Home 以外のライセンスを使用できます。このモードが Rapid Recovery での個人データの使用にどのように影響するかを確認するには、「プライバシーの管理」のトピックを参照してください。Phone Home 以外のライセンスにおける

制限、またはこのモードを使用してライセンスを取得する方法に関する情報を確認するには、「Phone Home 以外のライセンスの取得と使用」を参照してください。これらのトピックは、『*Rapid Recovery #######*』に記載されています。

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 に関連付けられた**ライセンスを変更**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、DL シリーズのバックアップアプ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、『*Rapid Recovery ##################*』の「Understanding software license types」（ソフトウェアライセンスタイプについて）の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されているか期限切れの場合、または Core が猶予期間を過ぎた 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。
- **ライセンスキーの期限切れ時期**。このオプションは、サブスクリプションライセンスを使用していて、サブスクリプションの有効期限が切れる前の期間（日数）が表示されるときにのみ使用できます。

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、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試用版ではない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、『*Rapid Recovery ##################*』の「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 によって使用**。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。
- **グループ内の合計使用**。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。
- **Phone home が無効になりました**。表示されている場合、このステータスは Core が Rapid Recovery ライセンスポータル または Data Protection ポータル と通信しないことを示しています。自動アップデートは無効にされ、GDPR ポリシーに従い、個人情報が Core と Quest Software Inc. またはその他の企業体との間で通信されることはありません。

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回の接続**：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にこのオプションを使用すると、スケジュールされた次回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、『*Rapid Recovery ################*』を参照してください。

ライセンスキーまたはファイルのアップデート / 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。

DL シリーズの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。

ライセンスポータルサーバへのアクセスの詳細については、「Rapid Recovery ライセンスポータル サーバへの接続」を参照してください。

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。

NOTE: DL シリーズの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。

NOTE: 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、『*Rapid Recovery ################*』を参照してください。

新しい Core のインストールが完了し、Core Console でライセンスファイルまたはキーの選択を要求するメッセージが表示されている場合は、手順 5 に進みます。

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。
3. **設定** ページの右側で、**ライセンスサーバ**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. Core に関連付けられている既存のライセンスをアップデートまたは変更するには、ライセンスの詳細の一番上にある Core 設定領域で **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. ライセンスキーを手動で入力する場合は、手順 6 に進みます。ライセンスファイルをアップロードする場合は、次の手順を実行します。
   a. ライセンスファイルをアップロードするには、**ライセンスファイルを選択するか、ライセンスキーを入力します** フィールドで、**ファイルの選択** 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。

b. 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。選択したライセンスファイルが、ライセンステキストフィールドに表示されます。

c. **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。

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 Core に関連付けられます。

d. 手順 7 に進みます。

6. ライセンスキーを手動入力するには、**ライセンスファイルを選択するか、ライセンスキーを入力します** テキストフィールドにライセンスキーを正確に入力し、**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 Core に関連付けられます。

7. **クイックスタートガイド** のようこそページが表示されたら、ガイドを開始するか、このツールを閉じることができます。これは、この手順に必要な最後の手順です。

   NOTE: 『クイックスタートガイド』の詳細については、『*Rapid Recovery #######*』の「クイックスタートガイドについて」を参照してください。

8. Core **設定** ページでこれらの手順を実行する場合は、**設定** ページの右側で、ライセンスサーバ の見出しが表示されるまで下にスクロールします。
9. 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。

Rapid Recovery Core Console の上部にエラーメッセージ (特定のサービスが起動していないなど) が表示された場合は、エラーメッセージのガイダンスに従ってこれらのエラーを解決してください。

ライセンスの追加

DL シリーズ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。

NOTE: アプライアンスの追加 ボタンが表示されるのは、DL シリーズバックアップアプライアンスのユーザーだけです。

NOTE: ライセンスキーの取得については、「*Rapid Recovery ##################*」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。表示される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。

   a. ライセンスキーを手動入力する場合は、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、**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。選択したライセンスファイルは、現在のダイアログボックスに表示されます。

d. ダイアログボックスで、**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。

5. **設定** ページの右側で、ライセンスサーバ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。

Rapid Recovery ライセンスポータル サーバへの接続

Rapid Recovery Core Console は頻繁に Rapid Recovery ライセンスポータルサーバにアクセスし、ライセンスポータルに加えられた変更を最新の状態に維持します。

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 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 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。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。

NOTE: 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、 Rapid Recovery Core と SNMP ブラウザ間の通信 (アラートなど) を制御します。使用可能な設定には、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の名前が含まれています。

NOTE: Rapid Recovery リリース 6.1 以前のビルドには、**コミュニティ文字列** 設定を変更できる機能は含まれていません。

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、**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 の各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
入力リクエストを処理	Core が入力 SNMP プロトコルを認識できるようにするには、このオプションを選択します。入力 SNMP プロトコルをブロックするには、このオプションを選択解除します。 **NOTE:** このオプションを選択して入力リクエストの処理を有効にすると、コミュニティ文字列の設定を編集できます。
コミュニティ文字列	コミュニティの名前を入力します。 **NOTE:** **入力リクエストを処理** 設定が **はい** に設定されている場合、この設定のみを変更できます。
着信ポート	SNMP 接続のポート番号を入力します。 **NOTE:** デフォルト設定は 8161 です。

テキストボックス	説明
トラップを送信	SNMP プロトコルを使用したアラート（トラップ）の送信を許可するには、このオプションを使用します。アラートをブロックするには、このオプションを選択解除します。
トラップ受信ポート	アラートの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。 **NOTE:** デフォルトのホスト名は localhost です。

4. 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。

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 quest-rapid-recovery-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、 （その他）をクリックして、 を選択します。
   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. **Opening quest-rapid-recovery-core.mib 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、**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。
     MIB 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。
     quest-rapid-recovery-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。
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 エレメント	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。 **NOTE:** 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。 **NOTE:** 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。 **NOTE:** 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。 **NOTE:** デフォルト設定は いいえ（オフ）です。

4. 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。

VMware のプロキシ設定の管理

VMware のプロキシ設定は、Virtual Disk Development Kit（VDDK）API を必要とする保護対象の VMware ESXi マシンが Vmware のディスクストレージにアクセスすることを目的としています。Rapid Recovery は VMware プロキシと呼ばれるプロセスを使用して、このアクセスと、それに関連する可能なタイムアウトを実現します。

このサービスは、Rapid Recovery Core と一緒に自動的にインストールされ、必要時にのみ実行されます。Core の設定 ページでは、サービスのタイムアウト設定を適切と考えられる値に調整できます。

1. Rapid Recovery Core Console のアイコンバーで、（設定）をクリックして、以下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、**VMware プロキシ** をクリックします。
   - 設定 ページの右側で、**VMware プロキシ** の見出しが表示されるまで下にスクロールします。
2. **VMware プロキシ** では、次の表に記載されたタイムアウト設定を変更します。

表 23. Vmware プロキシの設定情報

UI エレメント	説明
接続タイムアウト	VMware プロキシが VMware ディスクストレージへの接続の試行を中止するまでに経過しなければならない最大時間です。hh:mm:ss 形式で指定します。 **NOTE:** デフォルト設定は 5 分（00:05:00）です。
読み取り / 書き込みタイムアウト	VMware プロキシが VMware ディスクストレージからの読み取り、または VMware ディスクストレージへの書き込みを中止するまでに経過しなければならない最大時間です。hh:mm:ss 形式で指定します。 **NOTE:** デフォルト設定は 5 分（00:05:00）です。
サービス開始のタイムアウト	Rapid Recovery が VMware プロキシ開始の試行を中止するまでに経過しなければならない最大時間です。hh:mm:ss 形式で指定します。 **NOTE:** デフォルト設定は 5 分（00:05:00）です。
サービス停止のタイムアウト	Rapid Recovery が VMware プロキシ停止の試行を中止するまでに経過しなければならない最大時間です。hh:mm:ss 形式で指定します。 **NOTE:** デフォルト設定は 1 分（00:01:00）です。

3. 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。

vFoglight 設定の構成

Core 設定に vFoglight の情報を入力すると、Core Console では各保護対象 VM の サマリ ページに各 VM の vFoglight URL が表示されます。この URL をクリックすると、vFoglight で VM に関する情報が表示されます。

次の手順を実行して、vFoglight サーバと Rapid Recovery Core サーバを統合します。

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、**vFoglight 設定** をクリックします。
   - 設定 ページの右側で、vFoglight の見出しが表示されるまでスクロールダウンします。

   vFoglight 設定 の各設定が表示されます。
3. 次の表の説明に従って、vFoglight 設定を変更します。

表 24. vFoglight 接続の設定情報

テキストボックス	説明
https の使用	セキュアなハイパーテキスト転送プロトコルを有効または無効にします。セキュアな HTTPS がデフォルトです。
ホスト	vFoglight サーバのホスト名または IP アドレスを入力します。詳細については、vFoglight サーバ管理者に問い合わせてください。
ポート(O)	適切なポートを指定します。デフォルトのポートは32896です。詳細については、vFoglight サーバ管理者に問い合わせてください。
認証トークン	適切な認証を指定して、Core と vFoglight サーバが通信できるようにします。詳細については、vFoglight サーバ管理者に問い合わせてください。

4. 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。

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 25. 他のCore レベルのツール

UI エレメント	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、「夜間ジョブについて」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 26. システム情報

UI エレメント	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次の情報が表示されます。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。

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。

NOTE: 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、 (その他) 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。

NOTE: 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。

NOTE: 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。

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、Quest 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。

See also: Core ログファイルのダウンロードと表示
See also: 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 ログをダウンロードして表示するか、Quest 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、 (その他) 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. `Core AppRecovery.log` ファイルを開く、または保存するように求められた場合、**保存** をクリックします。
4. **Core AppRecovery.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。

     Core AppRecovery.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。

     Core AppRecovery.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。

See also: Core ログファイルのダウンロードと表示
See also: 保護対象マシンのログファイルのダウンロードと表示

リポジトリ

本項では、Rapid Recovery によってサポートされるリポジトリの操作方法について説明します。プライマリリポジトリタイプ（重複排除ボリュームマネージャまたは DVM）、およびセカンダリタイプ（階層化リポジトリ）の機能と属性について説明しています。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 リポジトリおよび階層化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も学習できます。

次のトピックで構成されています。

- リポジトリについて
- Rapid Recovery での重複排除
- DVM リポジトリの管理
- 階層化リポジトリの管理
- リポジトリのチェック
- リポジトリ設定の変更
- 既存のリポジトリへの接続
- リポジトリの詳細の表示または変更
- リポジトリの削除

リポジトリについて

リポジトリは Rapid Recovery データを保存して管理するために使用されるデータ構造です。バックアップスナップショットは、リカバリポイントの形式でフォーム内のリポジトリに保存されます。Rapid Recovery でマシンを保護し、データをレプリケート、または復元する前に、少なくとも 1 つのリポジトリが必要です。

Rapid Recovery 管理者は、特定の Core に関連付けられたストレージ場所（ディスクボリューム）内で明示的にリポジトリを作成します。リポジトリは、UI またはコマンドラインから作成できます。Rapid Recovery Core Console から、新しいプライマリ DVM リポジトリ、またはセカンダリ階層化リポジトリを作成できます。マシンを保護する場合、ウィザードワークフローの高度な手順を実行して DVM リポジトリを定義することもできます

Rapid Recovery Core Console の **リポジトリ** ページから、新しいリポジトリを作成するか、現在別の Core で使用されている既存のリポジトリに Core を接続できます。通常、リポジトリの詳細とリポジトリ設定の表示、リポジトリのチェック、またはリポジトリの削除を実行できます。 DVM リポジトリを使用すると、ストレージの場所を追加したり、リポジトリを最適化したりできます。 階層化リポジトリを使用すると、リポジトリをホストしているマシンから切断できます。特定のリポジトリタイプの管理方法の詳細については、それぞれ「DVM リポジトリの管理」、または「階層化リポジトリの管理」を参照してください。

リポジトリは、ダイレクト接続ストレージ（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）など異なるストレージテクノロジ上に存在できます。

NOTE: Rapid Recovery リポジトリは、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 のようなアーカイブ用のストレージデバイスは、パフォーマンスの制限のためサポートされていません。同様に、クラウドに階層化する NAS ファイラにリポジトリを保存しないようにします。これらのデバイスには、プライマリストレージとして使用したときにパフォーマンスが制限される傾向があるためです。

DAS は、最高のデータ帯域幅と最高速アクセスレートを提供しており、実装が簡単です。最適な結果を得るには、RAID (Redundant Array of Independent Disks) 6 ストレージとともに DAS を使用します。詳細については、次を参照してください。Quest ナレッジベース記事 118153、リポジトリオプション：ダイレクト接続ストレージ、ストレージエリアネットワークストレージ、またはネットワーク接続ストレージ。

プライマリ DVM リポジトリの格納場所は常に、指定したサブディレクトリ (`E:\Repository` など) である必要があります。ボリュームのルート (`E:\` など) は、リポジトリの場所にしないでください。 階層化リポジトリを作成する場合、ディレクトリは指定できませんが、コンテナは指定できます。デフォルトのコンテナを指定するか新しいコンテナを作成します。

DVM リポジトリは、プライマリストレージに使用されます。プライマリストレージでは、Core によって指定されたストレージデバイスにリカバリポイントが直接保存されます。

階層化リポジトリはセカンダリストレージとして使用されます。このモデルでは、リカバリポイントがプライマリ DVM リポジトリから指定したセカンダリストレージボリュームに再配置されます。コピーされ検証されると、リカバリポイントはプライマリリポジトリから削除され、より多くのバックアップデータを保存できるようになります。

NOTE: リリース 6.2.1 では、階層化リポジトリは Quest DR シリーズバックアップおよび重複排除アプライアンスでのみサポートされます。

1 つの Core に DVM リポジトリおよび階層化リポジトリの任意の組み合わせを定義できます。両方の リポジトリタイプが Core に追加されている場合、**リポジトリ** ページに個別のペインが表示され各リポジトリタイプがリストされます。プライマリリポジトリ が最初にリストされ、次に階層化 (セカンダリ) リポジトリがリストされます。

次のセクションで Rapid Recovery でサポートされる各リポジトリタイプの機能を説明します。

DVM リポジトリ。この リポジトリフォーマットでは、重複排除ボリュームマネージャ（DVM）を使用します。

- DVM はリカバリポイントを保存するために使用するプライマリリポジトリテクノロジです。
- DVM リポジトリは Rapid Recovery Core Console で作成および管理されます。
- DVM リポジトリは複数のボリュームに対応し、1 つの Core で最大 255 リポジトリをサポートしています。
- 作成時に DVM リポジトリのサイズを指定したり、エクステントを後で追加したりできます。
- DVM リポジトリは、Windows オペレーティングシステムが搭載されたマシンでのみ作成することができます。
- DVM 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）、または CIFS（Common Internet File System）共有上のストレージ場所に配置できます。
- このリポジトリタイプは、既存の AppAssure インストールのアップグレード時や、Rapid Recovery の新規インストール時に使用することができます。
- DVM リポジトリには、さまざまなストレージテクノロジを使用することができます。
- 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）、ダイレクト接続ストレージ（DAS）、ネットワーク接続ストレージ（NAS）があります。
- 8 GB RAM（できれば、エラーチェックおよび修正（ECC）メモリ）が必要です。
- Core マシンにはクアッドコアプロセッサが必要です。
- ホストごとに複数の DVM リポジトリをサポートします。
- 追加サービスは不要です。DVM リポジトリは、ネイティブ Core サービスを使用して、Core との通信とイベントの追跡を行います。
- 各 DVM リポジトリは、最大で 4096 のリポジトリエクステント（ストレージロケーションとも呼ばれます）をサポートします。
- 固定サイズです。DVM リポジトリでは、ボリューム上のリポジトリの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。ストレージ場所として定義した各ボリュームで利用可能な空き容量は、1 GB 以上である必要があります。
- リポジトリのストレージ場所は、シンプルディスクまたはダイナミックディスクでもかまいません。最も重要な要素は処理速度です。
- Console Core 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（Core ベースの暗号化）。
- リポジトリ全体（または、暗号化キーを使用する場合は、各リポジトリ内の暗号化ドメイン全体）でデータが重複排除されます。
- 専用のサイズ変更可能な DVM 重複排除キャッシュを使用しており、Core 設定でストレージ場所を設定できます。
- すべてのデータは Core で処理され、Core のローカルリポジトリへのデータの書き込みとスナップショットデータの保存が最適化されています。
- 作成後に名前を変更することはできません。
- このタイプの新規リポジトリは、REST API、Rapid Recovery コマンドライン管理ユーティリティ（cmdutil.exe）、または Windows PowerShell コマンドレットを使用して作成することができます。

DVM リポジトリを作成すると、Rapid Recovery Core 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。DVM リポジトリの最小サイズは 1 GB ですが、これは、テストを除き、実用的な目的には小さすぎます。

DVM 重複排除には、プライマリおよびセカンダリキャッシュが必要であるため、重複排除キャッシュのサイズの 2 倍のストレージ容量を予約するようにしてください。たとえば、Core の DVM 重複排除キャッシュ設定で 1.5 GB が予約されている場合は、キャッシュボリュームで 3 GB を予約します。キャッシュのデフォルトのインストールパスは C ドライブ上です。詳細については、次を参照してください。 重複排除キャッシュと保存場所について。

階層化リポジトリ。階層化リポジトリは Rapid Recovery リリース 6.1 で導入されました。

- 階層化リポジトリテクノロジはセカンダリストレージでのみ使用されます。
- アーカイブに指定されていない既存のリカバリポイント (1 週間以上経過) は、プライマリRapid Recovery DVM リポジトリから再配置できます。この機能は、保持期間を経て有効になります。
- 階層化リポジトリは Rapid Recovery Core Console で作成および管理されます。
- 現在、階層化リポジトリは Quest DR シリーズバックアップおよび重複排除アプライアンスバージョン 4.0 でのみサポートされます。
- セカンダリリポジトリに階層化されたリカバリポイントは引き続き暗号化でセキュリティ保護され、ロールアップの対象になります。保持ポリシーとロールアップは、新しい場所で Core により継続して管理されます。
- ロールアップは夜間に実行され、これに伴い新しいリカバリポイントが常に階層化されます。保護対象マシン別にリカバリポイントを表示する場合、これらの階層化されたリカバリポイントは金色のデータベースアイコン で表示されます。

相互運用性については、プライマリ DVM リポジトリに保存されたリカバリポイントは、セカンダリリポジトリで階層化が可能です。階層化をサポートする DR アプリケーションは、CentOS オペレーティングシステムを使用するため、DVM リポジトリはそれらのアプリケーションでサポートされません。

リポジトリストレージに物理 / 仮想アプライアンスを使用する

Quest DL4300 およびリカバリアプライアンスで Rapid Recovery を使用する場合、DVM と階層化リポジトリを作成できます。リリース 6.2 では、階層化リポジトリは、オペレーティングシステム 4.0 を実行している DR バックアップおよび重複排除アプライアンスに保存する必要があります。

DL で管理される階層化リポジトリは容量ライセンスを使用します。このため、DL アプライアンスに関連付けられた DVM リポジトリから DR アプライアンスのセカンダリストストレージにリカバリポイントを階層化することはできますが、これらのリカバリポイントで消費される容量により DL 容量が影響を受けます。このため、DL アプライアンスからリカバリポイントをアーカイブし、そのアーカイブを DR に保存するとコスト効率が良くなります。

その他のストレージ、バックアップ、リカバリ、または重複排除アプライアンスは Rapid Recovery での使用は正式にテストされていません。使用する場合は自己責任で行ってください。

適切な RDS サービスがインストールされ、オペレーティングシステム 4.0 が実行されている場合、Virtual Dr2000v は階層化リポジトリに使用できます。その他の仮想アプライアンスは Rapid Recovery Core リリース 6.2 ではサポートされていません。

See also: DVM リポジトリの管理
See also: 階層化リポジトリの管理

Rapid Recovery での重複排除

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データ圧縮方法です。このプロセスでは、データの固有のブロックを一度のみ物理的にディスクに格納します。Rapid Recovery では、固有のデータブロックがリポジトリ内で 2 度目に出現すると、Core は、もう一度データを保存する代わりに、リポジトリ内のデータへの仮想参照を保存します。

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。 。
- DVM リポジトリはターゲットベースの暗号化を使用します。セキュリティ上の理由から、暗号化は重複排除の前に実行されます。重複排除は、さらに 1 つの暗号化キーで保護されているデータに制限されています。

重複排除キャッシュがいっぱいになった場合、重複排除は最適以下になります。この場合、重複排除は後処理として実行できます（ブロック再利用とも呼ばれます）。重複排除キャッシュのサイズを増やした後、リポジトリ最適化ジョブを実行します。その後、Core はブロックを再利用し、リポジトリ内の領域が増加します。

リポジトリ最適化ジョブの詳細については、「DVM リポジトリの最適化について」を参照してください。このタスクの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有効に利用されます。

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。 DVM 重複排除キャッシュ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。

DVM リポジトリの管理

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、適切なテクノロジタイプを検討してください。
   リポジトリタイプの詳細については、「リポジトリについて」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 レポジトリの作成」を参照してください。
2. **リポジトリへの接続**。現在別の Core によって管理されている既存のリポジトリに接続する方法の詳細については、「既存のリポジトリへの接続」を参照してください。
3. **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。
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. **リポジトリ設定の変更**。リポジトリの詳細を表示する方法またはリポジトリの設定を変更する方法の詳細については、次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
6. **DVM リポジトリ最適化の実行**。リポジトリ最適化ジョブの詳細については、「DVM リポジトリの最適化について」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。
7. **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。

階層化リポジトリの管理の詳細については、「階層化リポジトリの管理」を参照してください。

DVM レポジトリの作成

このプロセスでは、重複排除ボリュームマネージャ（DVM）リポジトリのテクノロジを使用して Core にリポジトリを作成する方法について説明します。

- DVM リポジトリを作成するマシンに対する管理アクセス権が必要です。
- このリポジトリタイプは、ストレージの場所として定義されたボリュームに 1 GB 以上のストレージ容量が使用可能である必要があります。
- DVM リポジトリのストレージの場所は、Core サーバに接続しているローカルドライブまたは CIFS 共有である必要があります。
- Core サーバは任意の DL シリーズアプライアンス（DL 1000 を含む）またはシステム要件を満たすソフトウェアベースの Windows サーバにすることができます。

NOTE: DVM リポジトリは DR シリーズディスクバックアップおよび重複排除アプライアンスではサポートされていません。DR アプライアンスは独自の重複排除を使用します。この重複排除は、Rapid Recovery Core が DVM リポジトリに適用する重複排除とは互換性がありません。

DVM リポジトリに最初に保存されたリカバリポイントのセカンダリストレージ用の階層化リポジトリを作成する場合、「階層化リポジトリの作成」を参照してください。

DVM リポジトリを作成するには、次の手順を実行します。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、 (その他) 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. ページの上部の リポジトリ ページタイトルの下で、**作成** の横の ドロップダウン矢印をクリックしてから、**DVM リポジトリ** を選択します。

   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 27.「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 (R)	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 ー 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。
Comments	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。

5. **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このリポジトリのボリュームを定義します。十分なストレージ容量のある高速プライマリストレージドライブを使用します。DVM リポジトリのストレージ場所は、ローカル (Core サーバにアタッチされたストレージ) または CIFS (Common Internet File System) ネットワーク共有場所のいずれかを指定できます。1 つのストレージ場所にこれらの両方を指定することはできません。

   CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。
6. **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。
7. **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 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 28. 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 29. CIFS 共有資格情報

テキストボックス	説明
UNC パスUNC ぱす	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 (などRepository) 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(A)	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. **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 30. 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 **NOTE:** 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 8 以降または Windows 2012 以降を使用する New Technology File System (NTFS) ボリュームの場合は、ファイルサイズが 256 TB に制限されます。

テキストボックス	説明
	NOTE: 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。 **NOTE:** 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 がキャッシュを制御します。 「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。

9. **保存** をクリックします。

   ストレージ場所の追加 ダイアログボックスが閉じ、設定が保存されます。**新しいリポジトリを追加** ダイアログボックスに、新規のストレージの場所が表示されます。
10. リポジトリ用のストレージの場所をさらに追加するには、手順 6〜手順 9 を繰り返します。
11. この時点でリポジトリに対して作成するすべてのストレージ場所が定義されたら、**新しいリポジトリを追加** ダイアログボックスで、**作成** をクリックします。

    新しいリポジトリを追加 ダイアログボックスが閉じ、変更が保存されます。**リポジトリ** ページが表示され、DVM リポジトリサマリテーブルに新しく追加したリポジトリが表示されます。

既存 DVM リポジトリへのストレージ場所の追加

この手順を実行するには、DVM リポジトリがリポジトリ内に存在している必要があります。

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。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、（その他）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。

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、 （その他のオプション）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 31. 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 32. 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（ などRepository）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(A)	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(A)	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 33. 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。デフォルトのサイズは、250 GB です。次から選択できます。 • GB • TB **NOTE:** 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 8、8.1、Windows Server 2012、2012 R2 または 2016 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。 **NOTE:** 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。 **NOTE:** 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 がキャッシュを制御します。 「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。

   Quest 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、「DVM リポジトリの最適化について」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

AppAssure リリース 5.3.6 以前のリリースでは、レプリケーションに、ソース Core からターゲット Core への定期的なリカバリポイントのコピープロセスが含まれていました。エージングリカバリポイントのロールアップは、ソース Core でのみ発生していました。結合された古いリカバリポイントは、夜間ジョブの実行時に毎日同期されていました。

AppAssure バージョン 5.4.1 以降、および Rapid Recovery Core の現在のリリースでは、ユーザーはソース Core とターゲット Core 間で異なる保持ポリシーを設定できます。さまざまな保持ポリシーでレプリケーションを正常に動作させるには、ターゲット Core のソフトウェアバージョンがソース Core と同じ (またはより新しい) である必要があります。

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、任意のレプリケートされたマシンに対して、カスタム保持ポリシーを定義できるようになりました。たとえば、ターゲット Core で、ソース Core よりも小さい粒度、保存容量でより高速にリカバリポイントをロールアップできます。または、ターゲット Core で、選択したレプリケートされたマシンのリカバリポイントをより低速にロールアップしてより大きい粒度を維持し、コンプライアンスの目的に役立てることもできます。Core のデフォルトとは異なる保持ポリシーの使用に関する詳細については、「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。

AppAssure リリース 5.3.6 以前のターゲット Core にレプリケートされたリカバリポイントに不整合が発生する場合がありました。この問題に対処するために、AppAssure リリース 5.4.1 以降には、各 DVM リポジトリ上で実行される Core ジョブが含まれています。Quest では、リポジトリがリリース 5.4.x 以前に作成された場合 (リリース 5.3.x 以前で作成された場合) 、レプリケートされたターゲット Core の各 DVM リポジトリで、整合性チェックジョブを 1 度だけ実行することをお勧めします。

このチェックを実行する手順については、「DVM リポジトリでの整合性チェックの実行」を参照してください。

次の場合は整合性チェックジョブを使用**できません**。

- Rapid Recovery リリース 5.4.1 以降または AppAssure で作成されたターゲット Core の新しい DVM リポジトリ上。
- ソース Core 上。
- このリポジトリですでに整合性チェックジョブ (またはリポジトリの確認ジョブ) を実行済みの場合。
- レプリケーションを使用したことがない場合。

Core が任意の時点で AppAssure 5.3.x 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は、ソース Core とターゲット Core 間で異なる保持ポリシーを設定する前にこのジョブを実行するか、レプリケートされたマシン上にカスタム保持ポリシーを設定する必要があります。

該当するリポジトリ (5.4.x 以前に作成され、実行されていない) が 1 つ以上ある場合を除き、このジョブは表示されず、実行することはできません。

このジョブを実行すると、指定されたリポジトリに保存されている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リカバリできるようになります。整合性チェックによりリポジトリ内のデータに問題が検出された場合には、ジョブはただちに停止します。Core 上のそのジョブのイベント詳細に、Quest Data Protection サポート に連絡するように促すメッセージが表示されます。サポート担当者と共同作業する時間をスケジュールし、データの不整合を特定して修復するための追加の手順を実行します。

CAUTION: このジョブの実行には長時間かかることが予想されます。所要時間はリポジトリ内のデータの量とタイプや、基盤となるストレージシステムによって異なります。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。

このジョブの実行中でも、他のリポジトリで他の操作を実行できます。

NOTE: このジョブでは、リポジトリ内のすべてのコンテンツの整合性がチェックされます。リポジトリがマウント可能および使用可能であることを確認する `Checking repository` ジョブの詳細については、「リポジトリのチェック」を参照してください。

DVM リポジトリでの整合性チェックの実行

整合性チェックは DVM リポジトリに使用できます。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。

NOTE: ターゲット Core 上にすでにリポジトリチェックジョブが完了した別の DVM 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 リポジトリでリポジトリ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。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、 (その他) をクリックして、**リポジトリ** を選択します。

   リポジトリ ページが表示されます。
3. DVM リポジトリ サマリ表で、チェックを行う DVM のリポジトリを表す行の (その他のオプション) をクリックして、ドロップダウンメニューから、**整合性チェック** を選択します。

   確認メッセージが表示されます。

   CAUTION: 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** 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. あるリポジトリに対する整合性チェック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などを判断するには、アイコンバーで (イベント) をクリックします。
6. **タスク** ページで、そのジョブの **ジョブの詳細** をクリックすると、ジョブステータスに関する詳細が表示されます。
   - 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 Quest のテクニカルサポート担当者に提供してください。
   - 整合性チェック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。

DVM リポジトリの最適化について

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と、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は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ると、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。

- 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
- リポジトリの最適化ジョブ

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。

時間が限られている場合は、必要に応じてリポジトリの最適化ジョブを中断できます。詳細については、「DVM リポジトリ最適化の中断または再開」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。

NOTE: Quest 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、 (その他) 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の (その他のオプション) をクリックし、**最適化** 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、「DVM リポジトリ最適化の中断または再開」を参照してください。

DVM リポジトリ最適化の中断または再開

このタスクでは、Core に DVM リポジトリが存在し、リポジトリ最適化ジョブが実行中である必要があります。

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、DVM リポジトリの最適化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。

NOTE: 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、 (その他) 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。

   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、該当するリポジトリの列から、 (その他のオプション) 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. クリックして中断を確認します。
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、該当するリポジトリの列から、 (その他のオプション) をクリックし、**最適化** 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。
   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。

階層化リポジトリの管理

階層化リポジトリは、Core 上に定義されたセカンダリリポジトリで、プライマリ DVM リポジトリからリカバリポイントを再配置することができます。

リカバリポイントは、移動された後、プライマリ DVM リポジトリから削除されます。最終的にロールアップされて削除されるまで、再配置されたリカバリポイントは引き続き Core が管理します。

バックアップデータを階層化するには、DVM リポジトリ内のリカバリポイントの階層化を開始する保持期間を定義する必要があります。この操作は、保持期間のページで行います。

リカバリポイントを階層化リポジトリに再配置するには、事前に Rapid Recovery Core にセカンダリリポジトリを作成する必要があります。

階層化リポジトリを管理するには、次の操作を実行します。

1. **階層化リポジトリの作成。**古くなったリカバリポイントをセカンダリストレージに階層化するには、最初に Rapid Recovery Core Console で階層化リポジトリを定義する必要があります。リリース 6.2.1 では、階層化は、OS 4.0 を実行している DR Series 重複排除アプライアンスでのみサポートされます。リポジトリには、DR アプライアンスにネイティブな RDS サービスが必要です。詳細については、「リポジトリに

ついて」を参照してください。階層化リポジトリの作成の詳細については、「階層化リポジトリの作成」を参照してください。

2. **リポジトリへの接続**。既存の階層化リポジトリに接続する方法の詳細については、「既存のリポジトリへの接続」を参照してください。
3. **保持期間の定義**。Core に階層化リポジトリを追加した後、保持期間のページで、DVM リポジトリから階層化リポジトリに階層化されるリカバリポイントの保持期間を定義します。 特定の保護対象マシンに対してカスタマイズされた保持ポリシーを使用して階層化を設定する必要があります。特定の保護対象マシンのリカバリポイントを階層化するための保持ポリシーの設定については、「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。
4. **リポジトリ設定の変更**。階層化リポジトリ用のリポジトリ設定を変更する方法の詳細については、「リポジトリの詳細の表示または変更」を参照してください。
5. **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。
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 リポジトリの管理については、「DVM リポジトリの管理」を参照してください。

階層化リポジトリの作成

この手順では、Core で保護されたマシンのバックアップ専用セカンダリストレージとして使用される階層化リポジトリを Rapid Recovery Core Console から作成する方法を説明します。

NOTE: リリース 6.2.1 では、階層化リポジトリをサポートする唯一の物理的な場所は、OS 4.0 を実行している DR シリーズの重複排除アプライアンスです。保持ポリシーを階層に設定すると、リカバリポイントが DVM リポジトリから DR アプライアンスの階層化リポジトリに再配置されるまでの時間を指定できます。DR アプライアンスには Rapid Data Storage (RDS) サービスが含まれます。

プライマリ DVM リポジトリを作成する場合は、「DVM レポジトリの作成」を参照してください。

- 計画のため、ストレージボリュームの 128 GB が重複排除辞書用にデフォルトで予約されています。
- Rapid Recovery のオペレーティングシステムとファイルシステムの要件を満たす適切なサイズのソフトウェアベースの Windows サーバを Core サーバにすることができます。DL1000 または DL4000 以外の DL バックアップアプライアンスも Core サーバにすることができます。現在、これらのアプライアンスモデルは、DVM リポジトリのみをサポートしています。

  NOTE: システム要件の詳細については、「*Rapid Recovery #########*」を参照してください。

- 階層化リポジトリを作成する DR アプライアンスへの管理アクセス権限が必要です。
- DR アプライアンスのホスト名を指定する必要があります。

シンプロビジョニングされたストレージボリューム上では、リポジトリボリュームはオペレーティングシステムから消費されたスペースの量を示します。シックプロビジョニングされたボリュームでは、データで消費される、ドライブのすべての内容が示される場合があります。リポジトリレポートを使用して定期的にリポジトリを監視すると、リポジトリボリュームがいっぱいになることを回避するのに役立ちます。手動でのレポジトリ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。継続的にレポートの生成を自動化することについては、「レポートのスケジュール設定」を参照してください。

階層化リポジトリを作成するには、次の手順を実行します。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、 (その他) 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. ページの上部の リポジトリ ページタイトルの下で、**作成** の横の ドロップダウン矢印をクリックしてから、**階層化リポジトリ** を選択します。

レポジトリ作成ウィザード が表示されます。

4. **接続** ページの サーバ テキストフィールドに、リポジトリを接続し追加するマシンの IP アドレスまたはネットワークサーバ名を入力します。次に、**次へ** をクリックします。

RDS サービスは DR アプライアンスに事前にインストールされています。マシンに RDS サーバが含まれており、オペレーティングシステム 4.0 を実行している場合、そのマシンに接続します。それ以外の場合、DR アプライアンス管理者に連絡して支援を受け、正しい RDS サーババージョンにアップグレードしてこの手順に戻ります。

5. **設定** ページで、次の表に記載されているようにリポジトリの設定情報を入力し、**次へ** をクリックします。

表 34. 設定 ページの設定

リポジトリの構成に使用可能な設定の説明です。

テキストボックス	説明
名前	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」という単語と番号で構成されます。候補として示された名前は、この Core に現在存在するリポジトリの番号に対応します。たとえば、最初のリポジトリに提案された名前はリポジトリ 1、2 番目のリポジトリに提案された名前はリポジトリ 2 などとなります。 1 つ以上のテクノロジタイプのリポジトリを使用している場合、`TieringRepository1` のように名前にそのタイプを含めることができます。 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。
Comments	この情報は任意です。 このリポジトリに保存する情報の種類を説明するために使用することができます。たとえば、「このリポジトリでは、Accounting ドメインにあるすべての SQL Server および Exchange Server の古いリカバリポイントを保持します」などです。 この情報は、いつでも変更できます。
ストレージグループとコンテナのオプション	次のように階層化リポジトリのオプションを選択します。 • **デフォルトのストレージグループとコンテナを使用** を選択して、デフォルトの場所にリポジトリの構造を作成します。ほとんどのユーザーはこのデフォルトオプションを選択できます。 • 階層化リポジトリの構造を指定して、適切なオブジェクトを選択する場合は、**既存のストレージグループとコンテナを選択** を選択します。このオプションはストレージグループとコンテナのオプションを理解している上級ユーザー向けです。

6. **セキュリティオプション** ページで、次のいずれかを実行します。

- 作成している Core へのアクセスを制限し、ネットワーク上の他のユーザーがこのリポジトリの情報にアクセスできないようにするには、**このリポジトリを固有のライセンスによって保護** を選択します。次に、「**終了**」をクリックします。

この手順はオプションの予防措置です。リポジトリはすでにセキュアですが、Rapid Recovery Core へのアクセスには認証が必要です。これらのセキュリティオプションは、ユーザーがこのリポジトリを別の Rapid Recovery Core から開こうとしたときに適用されます。セキュリティを強化する場合は、任意の保護対象マシンのバックアップに Core レベルの暗号化キーを適用することもできます。

- 同時にライセンスでリポジトリをセキュリティ保護せずに階層化リポジトリを作成するプロセスを完了するには、**このリポジトリを固有のライセンスによって保護** オプションをクリアし、**終了** をクリックして、**保護されていないリポジトリに関する警告** ダイアログボックスで **はい** をクリックします。

レポジトリ作成 ウィザードが閉じます。指定したリポジトリ情報によりリポジトリ作成ジョブが生成され、すぐに開始されます。このジョブとリポジトリ作成の完了には、数分かかることがあります。ジョブが完了したとき、**階層化リポジトリ** ペインが **Repository** ページの下部に表示され、今追加したばかりの新しい階層化リポジトリが表示されます。

7. 必要に応じて、階層化リポジトリ作成タスクの進行状況を追跡することができます。詳細については、「タスクの表示」を参照してください。

リポジトリのチェック

Rapid Recovery を使用すると、Core でエラーが発生したときに、リポジトリボリュームの診断チェックを実行できます。Core の不適切なシャットダウン、リポジトリのマウントまたはマウント解除の失敗、ハードウェア障害、または Rapid Recovery の機能で発生する可能性のあるその他の環境に起因する下位 IP スタック要因などにより、エラーが引き起こされる場合があります。

すべてのリポジトリテクノロジタイプについて、チェックを行うと次のタスクが実行されます。

- リポジトリの確認
- リポジトリのマウント
- リポジトリからリカバリポイントをロード

DVM リポジトリに限り、チェックを行うと「リポジトリの重複排除キャッシュの再計算」タスクも実行されます。

NOTE: 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、 (その他) 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. リポジトリをチェックするには、いずれかのリポジトリテクノロジタイプのサマリ表の任意の行で (その他のオプション) をクリックし、**チェック** をクリックします。

   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、リポジトリの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。

リポジトリ設定の変更

この手順では、機能している階層化リポジトリが Core に含まれていることを前提としています。DVM リポジトリのリポジトリ設定を表示または変更するには、「リポジトリの詳細の表示または変更」を参照してください。

リポジトリの設定で、表示名、コメント、およびセキュリティオプションを変更できます。

1. Rapid Recovery Core Console のアイコンバーで、 (その他) をクリックして、**リポジトリ** を選択します。
2. **レポジトリ** ページで、**階層化リポジトリ** ペインまで下にスクロールします。
3. 更新するリポジトリを表す行の (その他のオプション) をクリックして、**設定** を選択します。

リポジトリの設定を編集 ウィザードが表示されます。

4. **設定**ページで、次の表の説明に従って設定を変更できます。

オプション	説明
名前	リポジトリの表示名。たとえば、リポジトリ 1 などです。
コメント	このリポジトリに関連付けるメモや説明。

5. **次へ** をクリックします。
6. **セキュリティオプション** ページで、セキュリティを確立して、この Core と同じライセンスナンバーを持つ Core のみがリポジトリと通信することを許可できるように、**このリポジトリを固有のライセンスによって保護** を選択します。

   NOTE: この手順はオプションの予防措置です。リポジトリはすでにセキュアですが、Rapid Recovery Core へのアクセスには認証が必要です。これらのセキュリティオプションは、ユーザーがこのリポジトリを別の Rapid Recovery Core から開こうとしたときに適用されます。セキュリティを強化する場合は、任意の保護対象マシンのバックアップに Core レベルの暗号化キーを適用することもできます。

7. **終了** をクリックします。

   変更がリポジトリに適用されます。
8. 前の手順でリポジトリに付加的なセキュリティを追加しないよう選択した場合、**保護されていないリポジトリに関する警告** ダイアログボックスが表示されます。**はい** をクリックして、ライセンスキーでリポジトリを保護しないことを確定します。

   リポジトリの設定を編集 ウィザードが閉じます。リポジトリ設定に加えた変更がすぐに適用されます。

既存のリポジトリへの接続

この手順を実行するには、元の Core の適切な認証情報が必要です。また、ローカルまたはネットワークのパス、IP アドレスまたはサーバ名が必要です。

CAUTION: この手順は、法的なアクセス権のあるリポジトリおよびデータに対してのみ実行してください。

階層化 リポジトリに接続する場合、そのリポジトリは、以前リポジトリを使用していた Core から切断する必要があります。リポジトリの切断の詳細については、「リポジトリの切断」を参照してください。

現在、別の Core と関連付けられていない DVM リポジトリに接続する場合、他の前提条件は適用されません。

機能している別の Core が現在所有している DVM リポジトリに接続する場合、この後必要となる所有権の移譲を準備する必要があります。次の前提条件が適用されます。

- リポジトリを所有している元の Core が機能している場合、その Core でマシンの保護を一時的に停止します。
- 次に、所有権の移譲中は元の Core の Core サービスを停止します。
- この手順の説明どおりにリポジトリを新しい Core に接続した後は、元の Core に戻ります。保護を継続するすべてのマシンには、リポジトリが関連付けられていることを確認します。
- 元の Core で Core サービスを再起動します。

保護の一時停止の詳細については、「保護の一時停止と再開」を参照してください。Core サービスのシャットダウンと再起動の詳細については、「Core サービスの再起動またはシャットダウン」を参照してください。

Rapid Recovery Core Console から、現在、他の Core で管理されている既存のリポジトリに接続できます。この接続を完了すると、リポジトリの所有権が元の Core から現在の Core に変更されます。そのため、リポジトリに接続した後、情報には 2 つ目の Core からのみアクセスでき、元の Core ではアクセスできません。接続す

るリポジトリは、共有ネットワーク上の場所または 2 つ目の Core にアクセス可能なストレージデバイス上にあり、アクセス可能である必要があります。

このプロセスは、元の Core が停止していて、代替の Core を有効にする場合に役立ちます。後で、2 つ目の Core から 3 つ目の Core (または元の Core) に所有権を変更することができます。この場合、同じルールが適用されます。

リポジトリのない元の Core は使用できないようにする必要があります。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。

階層化リポジトリは固有のライセンスで保護できます。この追加のセキュリティ設定を選択すると、権限のない個人がリポジトリの制御を剥奪し、他のリポジトリに移すことを防止できます。リポジトリを固有のライセンスで保護すると、ライセンスキーにアクセスできる管理者のみがそのリポジトリに接続できます。リポジトリ設定の更新の詳細ついては、「リポジトリ設定の変更」の手順を参照してください。

既存のリポジトリに接続するには、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、 (その他) をクリックして、 **リポジトリ** を選択します。

   リポジトリ ページが表示されます。
3. 既存の DVM リポジトリに接続するには、**既存への接続** の横にあるドロップダウン メニューテキストをクリックして、**DVM リポジトリ** を選択します。

   既存の DVM リポジトリを接続 ダイアログボックスが表示されます。
4. 手順 6 に進みます。。
5. 既存の階層化リポジトリに接続するには、**既存への接続** の横にあるドロップダウン メニューテキストをクリックして、**階層化リポジトリ** を選択します。手順 7 に進みます。
6. **既存の DVM リポジトリを接続** ダイアログボックスで、開くリポジトリに関する次の情報を入力し、**接続** をクリックします。

表 35. 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(A)	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。
7. **接続** ページの **リポジトリの接続ウィザード** で、この Core に接続するリポジトリをホストしているマシンのサーバ名または IP アドレスを入力し、**次へ** をクリックします。
8. ウィザードの **Core** ページで、適切な Core をクリックして選択し、**次へ** をクリックします。
9. ウィザードの **詳細** ページで詳細を確認し、選択した Core が適切かどうかを確認します。選択した Core に接続するには、**完了** をクリックします。

   選択したリポジトリが使用中であることを示すエラーが表示される場合、その Core にログインし、リポジトリの所有権をこの Core に移譲する準備をします。既存の保護を一時停止します。次に、既存のレプリケーションを一時停止し、キューに存在するジョブが完了するまで待つか、それらのジョブをキャンセルします。Core サービスをシャットダウンするか、Core サーバの電源を通常の手順でオフにして、この手順を繰り返します。保護の一時停止の詳細については、「保護の一時停止と再開」を参照してください。レプリケーションの一時停止の詳細については、「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。Core サービスのシャットダウンと再起動の詳細については、「Core サービスの再起動またはシャットダウン」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

リポジトリの詳細を表示するには、最初に Core にリポジトリを含める必要があります。DVM リポジトリ または階層化リポジトリの作成の詳細については、それぞれ「 DVM レポジトリの作成 」、または「階層化リポジトリの作成」を参照してください。

DVM リポジトリ ペインには、Core に追加された各 DVM リポジトリが表示されます。

- (展開) をクリックすると、子行に DVM リポジトリのデータとメタデータの場所が表示されます。
- ビューを (折り畳む) こともできます。

階層化リポジトリ ペインでは、既存の各リポジトリを表すために少なくとも 3 行のデータが使用されます。

- 一番上の行は、 RDS サーバです。1 Core あたり最大 3 台の RDS サーバに接続できます。
- 2 番目の行には、 ストレージグループが表示されます。各 RDS サーバに、最大 5 つのストレージグループを含めることができます。
- 3 番目の行には、 階層化リポジトリがリストされます。

ビューを (展開) および (縮小) して**階層化リポジトリ** ペインで領域を節約できます。

リポジトリの詳細は、リポジトリのテクノロジタイプによって異なります。リポジトリの詳細を表示または変更するには、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、 (その他) をクリックして、**リポジトリ** を選択します。

   リポジトリ ページが表示されます。
3. 次の一般的なアクションが使用可能です。

オプション	説明
+ 作成	ドロップダウンメニューから、適切なリポジトリタイプを選択してリポジトリを作成します。次から選択できます。 • DVM リポジトリ • 階層化リポジトリ
既存への接続	ドロップダウンメニューからリポジトリタイプを選択して、別の Core のリポジトリを開きます。このプロセスにより、リポジトリの所有権が現在の Core に変更されます。次から選択できます。 • DVM リポジトリ • 階層化リポジトリ 詳細については、「既存のリポジトリへの接続」を参照してください。

オプション	説明
更新	ページに表示されているリポジトリのリストを更新します。

4. **DVM リポジトリ** ペインでは、任意の DVM リポジトリの（その他のオプション）ドロップダウンメニューから次のアクションを実行できます。

オプション	説明
ストレージ場所の追加	ストレージの場所を追加して、既存のリポジトリを拡張します。 **NOTE:** DVM リポジトリの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。このアクションによって、特定の転送フェーズと同時にボリュームの拡張を実行した場合にのみ発生する可能性がある、まれなエラーを防止することができます。
チェック	リポジトリチェックを実行します。
設定	リポジトリの設定を表示または変更します。これらの設定により、次の操作を実行できます。 • リポジトリ名の表示 • 最大同時操作数の表示または変更 • 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ているデータの有効化または無効化
最適化	リポジトリの最適化ジョブを実行します。詳細については、「DVM リポジトリの最適化について」を参照してください。
削除(D)	リポジトリを削除します。 **CAUTION: このオプションは、選択した DVM リポジトリと、それに含まれるすべてのデータを完全に削除します。**

5. **階層化リポジトリ** ペインでは、RDS サービスの（その他のオプション）ドロップダウンメニューから次のアクションを実行できます。

オプション	説明
認証情報を変更	現在選択されているホストに関連付けられたパスワードを変更できます。このアクションは、リポジトリの所有権を変更してセキュリティを維持する場合に役立ちます。

オプション	説明
	NOTE: 新しいパスワードを確認し、**保存** をクリックして認証情報を更新します。

6. ストレージグループで使用できるアクションはありません。
7. In the**階層化リポジトリ** ペインの （詳細オプション）ドロップダウンメニュー（任意の 階層化リポジトリ）から、以下の操作を実行できます。

オプション	説明
設定	リポジトリの設定を編集 ウィザードが開き、リポジトリ設定を表示または変更できます。これらの設定により、次の操作を実行できます。 • サーバまたはホストの表示 • リポジトリ名の表示または変更 • リポジトリ用のコメントの表示または変更
チェック	選択したリポジトリのすべてのアクティブなタスクをキャンセルし、リポジトリチェックを実行します。
接続解除	選択したリポジトリをマウント解除します。 **NOTE:** 接続を解除した後は、リポジトリページの上部にある **既存への接続** 機能を使用して、後で再びリポジトリに接続できます。
削除(D)	リポジトリを削除します。 **CAUTION: このオプションは、選択したリポジトリと、それに含まれるすべてのデータを完全に削除します。**

リポジトリの切断

この手順では、機能している 階層化リポジトリが Core に含まれていることを前提としています。

リポジトリ ページから、既存のリポジトリを切断できます。このプロセスでは、リポジトリのデータは削除されません。単にリポジトリとそのコンテンツとの現在の接続をマウント解除します。これは、別の Core からリポジトリに接続するような場合に有用です。

階層化リポジトリを切断するには、 次の手順を実行します。

1. Rapid Recovery Core Console のアイコンバーで （その他）メニューをクリックし、**リポジトリ** をクリックします。
2. **リポジトリ** ページで、切断するリポジトリを表す行の （その他のオプション）をクリックして、**接続解除** を選択します。

   リポジトリを切断 ダイアログボックスが開きます。
3. クリックして、既存のリポジトリを切断するアクションを確定します。

リポジトリが切断され、**リポジトリ** ページが更新されます。リポジトリは現在使用可能なリポジトリのリストには表示されなくなります。

リポジトリに再接続するには、「既存のリポジトリへの接続」の手順を参照してください。

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。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、 (その他) をクリックして、 **リポジトリ** を選択します。

   リポジトリ ページが表示されます。
3. 適切なリポジトリサマリ表の削除するリポジトリを表す行で (その他のオプション) 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。

   CAUTION: 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。
4. 「**はい**」をクリックして、リポジトリの削除を確認します。

プライバシーの管理

本項では、Rapid Recovery が収集できる個人情報、その情報の用途、およびユーザーがそのデータのプライバシーをどのように制御できるかについて説明します。

次のトピックで構成されています。

- 一般データ保護規則の遵守
- Rapid Recovery が個人情報を使用する方法
- Phone Home 以外のライセンスの制限
- Phone Home 以外のライセンスの取得と使用

一般データ保護規則の遵守

一般データ保護規制（GDPR）は、欧州連合（EU）内のすべての個人に対してデータ保護を強化および統一するために制定された法律です。EU 外の個人データのエクスポートにも対応するため、米国およびその他の国に拠点を置くソフトウェアの製造元にも関連しています。各個人データの処理を管理する規則が更新されます。GDPR は、ソフトウェア業界全体で広く採用されています。

GDPR を順守するため、Rapid Recovery Core で収集される個人情報（PII）の取り扱いについて、慎重に検討されてきました。データ収集が効率化され、収集された情報は明確に文書化されます。

Rapid Recovery Core のインストール時、Recovery and Update Utility（RUU）の実行時、または情報収集ツールの実行時に、Rapid Recovery で収集される情報とその情報を収集する弊社の目的に関する説明が提供されます。

記載されている個人データの使用に同意する場合は、（標準 Phone Home モードで動作している）ライセンスと Core を関連付けることができます。プライバシーポリシーで説明されている個人データの使用を拒否する場合は、特別な Phone Home 以外のライセンスを要求する必要があります。そのライセンスを受け取り、Core と関連付けた後、PII は使用されず、一部の機能（自動アップデート、および Core と Data Protection ポータル との間での統合の有効化）が無効にされます。

インストール時に選択したプライバシーオプションに関係なく、Core 一般設定 **個人データの使用に同意する** からこの設定を変更できます。Phone Home モードから Phone Home 以外のモード（またはその逆）に切り替えるには、適切なライセンスへのアクセス権を持っている必要があります。

GDPR の詳細については、EU 一般データ保護規則のウェブサイト（http://www.eugdpr.org/eugdpr.org.html）を参照してください。

プライバシーの管理の詳細については、『*Rapid Recovery #######*』の次のトピックを参照してください。

- **個人データの使用に同意する** 一般設定を使用して Phone Home と Phone Home 以外のモード間を切り替えるとき、特定のビジネスルールが適用されます。詳細については、「Core 一般設定の構成」のトピックを参照してください。
- Rapid Recovery がどの情報を、どの状況で収集するか、またなぜその情報が収集されるかを確認するには、「Rapid Recovery が個人情報を使用する方法」を参照してください。
- Phone Home 以外のライセンスを使用する際に実行できない機能を確認するには、「Phone Home 以外のライセンスの制限」のトピックを参照してください。
- Phone Home ライセンスをダウンロードするには、Rapid Recovery ライセンスポータル にログインします。ナビゲーションメニューから、**ライセンス** をクリックし、右上のドロップダウンメニューから、**ライセンスキー** を選択します。
- Phone Home 以外のモードでライセンスを取得する方法については、「Obtaining and using non-phone-home keys」（Phone Home 以外のキーの取得と使用）のトピックを参照してください。

Rapid Recovery が個人情報を使用する方法

ライセンスの管理 で説明されているように、Rapid Recovery では、サブスクリプション版ライセンス、永久版ライセンス、および試用版ライセンスという 3 つのタイプのソフトウェアライセンスを使用します。

ライセンスを使用できる、次の 2 つのモードがあります。

- **Phone Home モード**。すべてのライセンスは、特に要求がない限り Phone Home モードで発行されます。Phone Home ライセンスを Rapid Recovery ライセンスポータル に登録した場合、Rapid Recovery は個人を特定できる情報（PII）を収集します。収集する情報、およびその用途については、下記で説明します。
- **Phone Home 以外のモード**。インターネットに接続しているときでも、Phone Home 以外のライセンスを取得して、登録した場合、Rapid Recovery は PII を共有しません。このモードを使用すると、「Phone Home 以外のライセンスの取得と使用」のトピックで説明されているように、特定の機能を実行できなくなります。

サブスクリプションライセンスは、Phone Home モードでのみ使用できます。永久版ライセンスと試用版ライセンスは、Phone Home モードでも Phone Home 以外のモードでも使用できます。

Phone Home ライセンスを登録すると、Rapid Recovery に以下の PII を収集する権限を与えることになります。

- Rapid Recovery Core および Agent で動作するホストまたはこれらを操作するホストの IP アドレスとホスト名。
- Rapid Recovery ライセンスに関連付けられたメールアドレス、および
- ライセンスプールにあるライセンス数に対するライセンスの消費量。

この情報は、以下の目的で Quest Software Inc. に送信されます。

- 製品に適切なライセンス条項を正しく適用するため
- カスタマサポートを提供するため。たとえば、情報収集ツールを実行するとき、指定したログと診断データは、Quest に送信するためにローカルフォルダに収集されるか、Amazon にアップロードされ、Quest Data Protection サポート のみがアクセスできます。
- 利用可能なアップデートをユーザーに通知するため（Core のアップデート設定で **アップデートを確認しない** 以外のオプションが指定されている場合）、および
- Core と Data Protection ポータル 間の通信を可能にするため。この通信は、Core の **データプロテクションポータル** 設定を使用して有効または無効にすることができます。このポータルでは、期限内のサポート

契約があるライセンスユーザーによる Core と保護対象マシンの正常性の監視、複数の Core の管理、および必要に応じて関連する Core と保護対象マシンに関するレポートの生成が可能です。

ユーザーには、この情報を Quest と共有するかどうかを選択する権限があります。まず、Rapid Recovery Core をインストールまたはアップデートするとき、インストーラの **プライバシーポリシー** ページでこの情報を共有するかどうかを選択できます。また、Quest と情報を共有しない場合は、Core 一般設定 **個人データの使用に同意する** を変更できます。この設定を変更すると、ライセンスを入力するように要求されます。Phone Home 以外のライセンスを入力した場合、Data Protection ポータル への接続と同様に、自動アップデートが無効になります。

このトピックに関する追加リリースについては、次の関連リンクを参照してください。

- Phone Home 以外のモードを使用しているときに使用できない機能の詳細については、「Phone Home 以外のライセンスの制限」のトピックを参照してください。
- Phone Home 以外のモードを使用するライセンスの取得の詳細については、「Phone Home 以外のライセンスの取得と使用」のトピックでの説明に従い、Web フォームで Quest ライセンスチームにお問い合わせください。
- PII の共有を含む、一般設定の変更の詳細については、「Core 一般設定の構成」のトピックを参照してください。
- 1 台の保護対象マシンのライセンス情報の表示についての詳細は、「マシンのライセンス情報の表示」を参照してください。
- ライセンスキーまたはファイル情報 (たとえば、Phone Home 永久版ライセンスを Phone Home 以外の永久版ライセンスにアップデートする) の入力の詳細については、「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。
- 利用可能なライセンスのタイプの詳細については、「ライセンスの管理」を参照してください。
- ライセンスポータルサーバへのアクセスの詳細については、「Rapid Recovery ライセンスポータル サーバへの接続」を参照してください。
- ライセンスの管理に関するその他のトピックについては、「*Rapid Recovery ##################*」を参照してください。

Phone Home 以外のライセンスの制限

Phone Home 以外のモードで Rapid Recovery ライセンスを登録すると、Core が個人情報を共有することはできません。これには、メールアドレス、IP アドレス、およびライセンス消費情報が含まれます。

Phone Home 以外のライセンスを登録した後は、以下の操作ができなくなります。

- Core Console の **設定** ページからライセンスサーバ情報を表示する (Core と Rapid Recovery ライセンスポータル との通信が許可されないため)。
- Core Console からライセンスの消費を管理する。
- Rapid Recovery 情報収集ツールから Quest Data Protection サポート に情報を送信する。
- Data Protection ポータル から Core と保護対象マシンの正常性を監視する、複数の Core を管理する、および複数の Core で必要に応じて関連するマシンのレポートを生成する。
- 自動アップデート機能を使用して新しいバージョンの Rapid Recovery Core にアップデートする (新しいバージョンを利用できることが Core に通知されません)。
- 自動アップデート機能を使用して、yum、zypper、または apt などのパッケージマネージャにより保護対象 Linux マシンを直接アップデートする (インターネットにアクセスできる Linux マシンからインストールパッケージをダウンロードし、インストールファイルを手動でセキュリティ保護されたコンピュータへ移動することはできます)。

Phone Home 以外のライセンスの取得と使用

Rapid Recovery Core リリース 6.2.1 をアップグレードまたはインストールする前に Phone Home 以外のライセンスを取得した場合は、ライセンスを Core サーバに転送します。インストーラの実行時に、**プライバシーポリシー** ページで、データの共有を拒否するオプションを選択し、プロンプトが表示されたら、Phone Home 以外のライセンスを登録します。

Rapid Recovery Core リリース 6.2.1 がすでに Phone Home キーに登録されている場合、Core で一般設定にアクセスして、データの共有を拒否するオプションを選択し、プロンプトが表示されたら、Phone Home 以外のキーを登録します。

Core の一般設定を変更するための詳細情報または詳細手順については、「Core 一般設定の構成」のトピックを参照してください。

Rapid Recovery 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。

Quest ライセンスチームに連絡して Phone Home 以外のライセンスを取得するには、次の手順を実行します。

1. ウェブブラウザで、Quest ライセンスアシスタンスウェブサイト (https://support.quest.com/contact-us/licensing) に移動します。
2. **必要なサポート** ドロップダウンメニューから、**製品のライセンスを取得する** を選択します。
3. **製品の選択** ドロップダウンメニューから、**Rapid Recovery** を選択します。
4. **製品バージョン** ドロップダウンメニューから適切なオプションを選択します。

   たとえば、**6.2** を選択します。
5. 次の表の説明に従って、フォームの 連絡先情報 セクションで情報を追加します。

フィールド名	説明	必須フィールド
ビジネス用メールアドレス	Quest ライセンスチームからの返信を受け取るメールアドレスを入力します。Rapid Recovery ライセンスに関連付けられたメールアカウントにアクセスできる場合は、最短時間で回答が得られるようにそのメールアドレスを使用します。	はい
連絡先の名	名を入力します	はい
連絡先の姓	姓を入力します	はい
会社名	Rapid Recovery ライセンスに関連付けられた会社名を入力します。	
米国連邦	ライセンスが米国連邦組織と関連しているかどうかを選択します。	いいえ
国	国を選択します。	はい
電話番号	電話番号を入力します(市外局番を含む)。米国外の場合は、国番号を含めます。	はい
ライセンス番号 (該当する場合)		いいえ

フィールド名	説明	必須フィールド
ライセンスキー（該当する場合）	ライセンスキーは AppAssure 5.4.1 以前に使用されました。これは、通常、30 文字の文字列です（ハイフンで区切られた 6 つのグループの 5 つの数字とアルファベット大文字）。	いいえ
マシン ID	登録されている Core マシンの名前。	いいえ
サービスタグ（該当する場合）	該当する場合はサービスタグを入力します。	いいえ
ライセンス要求の詳細	このフィールドには、PII を保護するために Phone Home 以外のライセンスを Phone Home ライセンスの代わりに使用することを GDPR ごとに記述します。 **NOTE:** この要求をすることで、Phone Home 以外のキーを受け取り、登録したとき、Phone Home ライセンスキーを削除することに同意するものとします。また、このキーを共有しないことに同意するものとします。	はい
ライセンスファイル	Phone Home ライセンスがある場合、ライセンスファイルを添付できます。	いいえ

6. 要求を確認しフォームを送信するために、**ロボットではありません** を選択し、**次へ** をクリックします。

   フォームを送信し、サービスリクエスト（SR）番号が記載された電子メールメッセージを受け取ります。

Phone Home 以外のライセンスファイルを受け取ったら、Core サーバにアップロードしてライセンスを登録します。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。

暗号化

本項では、暗号化キーとマシンレベルのスナップショット暗号化設定を使用して、お使いの環境内でデータをセキュリティ保護するプロセスについて説明します。

暗号化キーについて

Rapid Recovery Core では、Core Console から定義および管理する暗号化キーを使用して、任意のリポジトリ内のすべてのボリュームのスナップショットデータを暗号化できます。

Rapid Recovery では、リポジトリ全体を暗号化する代わりに、1 つの Rapid Recovery Core で保護される 1 台または複数のマシンに暗号化キーを指定することができます。アクティブな各暗号化キーにより、暗号化ドメインが作成されます。Core 上に作成できる暗号化キーの数に制限はありません。

マルチテナント環境（1 つの Core が複数の暗号化ドメインをホストする）では、それぞれの暗号化ドメインでデータがパーティション化され、重複排除されます。そのため、Quest では一連の保護対象マシン間で重複排除の利点を最大限に活用するには、複数の保護対象マシンに 1 つの暗号化キーを使用することをお勧めします。

また、3 つのうちのいずれかの方法を使用して、Core 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、1 つの Rapid Recovery Core から暗号化キーをファイルとしてエクスポートし、それを別の Core にインポートすることです。2 つ目の方法は、暗号化キーでセキュリティ保護されたデータをアーカイブし、そのアーカイブされたデータを別の Rapid Recovery Core にインポートすることです。3 つ目の方法は、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トします。保護対象マシンをレプリケートすると、ソース Core で使用される暗号化キーが、レプリケートされた暗号化キーとしてターゲット Core に表示されます。

いずれの場合も、インポートされた暗号化キーは、「ロック」状態で Core に表示されます。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、暗号化キーをロック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、ロック解除の詳細については、「暗号化キーの管理」のトピックを参照してください。

キーセキュリティには次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文ブロック連鎖（CBC）モードで 256 ビットの高度暗号化標準（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。
- 暗号化の実行は、パフォーマンスに影響しません。
- 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、保護対象マシンに一度に適用できるのは 1 つの暗号化キーのみです。
- Rapid Recovery 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。

> **CAUTION:** Rapid Recovery **では、暗号化キーを保護対象マシンに適用するたびに、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場合も、新しいスナップショットが取得されます。**

Rapid Recovery Core から生成される暗号化キーは、次の表に示す 4 つのパラメーターを含むテキストファイルです。

表 36. 暗号化キーのコンポーネント

コンポーネント	説明
名前	この値は、Rapid Recovery Core Console でキーを追加するときに指定されたキー名と同じです。
キー	このパラメータは、ランダムに生成された 107 文字の英字、数値、算術演算子で構成されます。
ID	キー ID は、ランダムに生成された 26 文字の大文字と小文字で構成されます。
コメント	コメントには、キーの作成時に入力されたキーの説明テキストが含まれます。

ネットワーク経由の転送でデータを暗号化する

Rapid Recovery Coreリリース 6.2.1 は新しい暗号化機能を搭載しており、ネットワーク経由の転送ですべてのデータを暗号化できるようになりました。Quest では、Core と保護対象マシンの間 (またはレプリケーションの場合などのように 2 つの Core 間) のデータをパブリックネットワークまたはインターネットなどの信頼されていないネットワーク経由で送信する必要がある場合、この暗号化設定を有効にすることをお勧めします。

この暗号化を有効にするとごくわずかなパフォーマンスコストが発生しますが、Core と保護対象マシンがプライベートローカルエリアネットワークの制限内にある場合、このオプションを無効にしても安全です。

次の情報を読み、必要に応じて調整してください。

デフォルトでは、マシン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マシンを保護しているときは、ネットワーク経由で転送されるデータの暗号化が有効です。ウィザードの 詳細設定 オプションを選択した場合、暗号化オプションが表示されます。ウィザードの 暗号化 ページで、必要に応じて、**ネットワーク経由の転送データを暗号化する** オプションをクリアできます。

NOTE: ウィザードで 詳細設定 オプションを選択しない場合でも、転送でのデータの暗号化は有効にされます。

関連する保護ウィザードを完了した後は、マシンレベルで転送設定を変更して、スナップショットの暗号化をいつでも有効または無効にすることができます。保護対象マシンを選択して **設定** をクリックし、転送 設定の下の **スナップショットデータの暗号化** 設定で **はい** を選択して暗号化を選択するか、**いいえ** を選択して転送中の暗号化を無効にします。特定の詳細については、『*Rapid Recovery #######*』で「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。

暗号化キーの適用または削除

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ために、Quest で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回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回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。

  -  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。

CAUTION: 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回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 37. 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。
Passphrase (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。Quest 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。

テキストボックス	説明
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。

> **CAUTION:** 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、Quest では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回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。

> **NOTE:** 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 （その他）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。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 38. 各暗号化キーの情報

UI エレメント	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。
サムプリント	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、「暗号化キーのアンロック」のトピックを参照してください。
状態	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、「暗号化キーのアンロック」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、「暗号化キーの適用または削除」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
- 暗号化キーのアンロック
- 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、Quest では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。

CAUTION: 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、 （その他）をクリックして、 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 39. 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。

テキストボックス	説明
	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。
Passphrase（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。 **CAUTION: パスフレーズは安全な場所に保管してください。Quest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できる必要があります。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。

NOTE: 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、 （その他）をクリックして、 を選択します。

   暗号化キー ページが表示されます。
3. 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。

暗号化キーのアンロック

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 11:24 AM 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 11:24 AM にキーが自動的にロックされます。

NOTE: 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、 （その他）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。「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 をクリックして、**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、 (その他) 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。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で 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。

NOTE: 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。

CAUTION: 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回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、 (その他) 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. 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。詳細については、暗号化キーのアンロックを参照してください。
   - 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. 指定した暗号化キーのドロップダウンメニュー 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。

CAUTION: 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回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、（その他）をクリックして、 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。

CAUTION: 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。Quest では、パスフレーズを安全な場所に保管し、この情報を最新の状態にしておくことをお勧めします。Quest サポートでは、パスフレーズをリカバリできません。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、 （その他）をクリックして、 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 をクリックして、 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。

NOTE: 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、 （その他）をクリックして、 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。ドロップダウンメニュー をクリックし、 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。

   NOTE: 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。

NOTE: 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、 (その他) をクリックして、 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 をクリックして、 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 をクリックして、 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。

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、保護するワークステーション、サーバ、デスクトップ、およびノートパソコンの各マシンを Rapid Recovery Core に追加する必要があります。

Rapid Recovery Core Console でいずれかのマシン保護ウィザードを使用して、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、マシン保護ウィザードを使用して、1 台のマシンを保護する。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、クラスタを保護 ウィザードを使用して、ネットワーククラスタを保護する。クラスタを保護する方法の詳細については、「クラスタの保護」を参照してください。
- 複数のマシンを保護 ウィザードを使用して、複数のマシンを同時に保護する。このウィザードでは、Microsoft Active Directory サーバに関連付けられたマシン、vCenter または ESXi ホスト上のマシン、Hyper-V ホストまたは Hyper-V クラスタ上のマシンに接続することができます。また、複数のマシンの接続情報 (ネットワークホスト名または IP アドレス、ユーザー名とパスワード) を手動で入力することもできます。複数のマシンを保護する方法の詳細については、「複数のマシンの保護について」を参照してください。

NOTE: 保護操作が失敗する原因となるリソースの制約が発生しないように、Quest では同時に保護するマシンの台数を 50 台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)。

vCenter/ESXi または Hyper-V ホストで仮想マシンを保護するときは、Rapid Snap for Virtual 機能を使用してマシンを保護するか、または Rapid Recovery Agent をインストールして保護するかを定義する必要があります。詳細については、「エージェントベースの保護またはエージェントレス保護を選択するときの要因」を参照してください。

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。

Agent 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。

エージェントベースの保護またはエージェントレス保護を選択するときの要因

Rapid Recovery の Rapid Snap for Virtual 機能は vCenter/ESXi または Hyper-V ハイパーバイザでサポートされます。エージェントレス保護としても知られているこの機能により、 各ゲストマシンに Rapid Recovery Agent ソフトウェアをインストールせずに、Core で VM を保護できます。

一般的推奨事項

リリース 6.2.1 では、Rapid Recovery の Rapid Snap for Virtual 機能により、Rapid Recovery Agent ソフトウェアをインストールすることで得られるのとほぼ同等の保護が得られます。原則的に、Quest は、ESXi または Hyper-V 仮想マシンではエージェントレス保護を使用することをお勧めします。エージェントのソフトウェアが ESXi または Hyper-V VM にインストールされている場合、Rapid Recovery Agent を使用して VM を保護するやむを得ない理由がある場合を除き、Quest では、エージェントのソフトウェアを削除し、エージェントレスで保護することをお勧めします。

エージェントレスでの保護にはいくつかの利点があり、いくつかの制限もあります。これらについては、「Rapid Snap for Virtual について」のトピックで明確に説明されています。

次に、エージェントレス保護の使用を推奨する例外を示します。

- エージェントレスマシンのメタデータの収集は、Rapid Recovery Agent ソフトウェアで保護されたマシンより遅くなります。メタデータに関連したパフォーマンスの問題が (特にエージェントレスで保護された Exchange Server または SQL Server マシンで) 発生した場合、Quest Data Protection サポート では、トラブルシューティングの目的で特定のアプリケーションサーバにソフトウェアベースのエージェントをインストールするように提案することがあります。
- 複数のソケットのあるハイパーバイザで 1 つまたは 2 つの VM のみを保護している場合、エージェントをホストではなく VM に直接インストールすることで、消費するライセンスが少なくなる可能性があります。
- Rapid Recovery Agent に限定されている機能が必要な場合は、関連する VM にエージェントのソフトウェアをインストールします。

一部の機能は、Rapid Recovery Agent ソフトウェアをインストールすることによる、特有の保護機能となります。次の例が該当します。

- SQL アタッチ可否チェックの実行は、Rapid Recovery Agent ソフトウェアの機能です。SQL Server マシンをエージェントレスで保護している場合、Core サーバではなく SQL Server のインスタンスを使用して SQL アタッチ可否チェックを実行する必要があります。このチェックを実行するには、Core の Core アタッチ可否 設定を **Core で SQL Server を使用** に調整する必要があります。
- エージェントレスで保護されているダイナミックボリュームは、ボリュームレベルではなく、ディスクレベルで保護されています。
- Live Recovery は、Rapid Recovery Agent ソフトウェアの機能です。この機能は、Rapid Snap for Virtual を使用して保護されているボリュームを復元するときには使用できません。

特定の VM に前記のリストで説明した機能のいずれかが必要な場合、Quest では、VM をエージェントレスで保護する代わりにエージェントをインストールすることをお勧めします。

詳細については、「Rapid Snap for Virtual について」のトピックを参照してください。

リリース 6.2 ライセンス消費の概念

Rapid Recoveryリリース 6.2.1 では、Windows Server、Hyper-V ホスト、VMware ソケット、Exchange Server、SQL サーバ、Linux サーバ、などに適用される特定のライセンスプールの使用を中止します。新しいモデルは大幅に簡素化されます。

ライセンスの管理 のトピックで説明されているように、Rapid Recovery リリース 6.2.1 で使用するライセンスプールは、容量とエンタープライズの 2 つのみです。Core のライセンスが容量ベースのプールを使用するように設定されている場合、別のプールタイプは使用できません。

NOTE: 将来的に、Quest では他の測定単位に基づくライセンスプールの追加を計画しています。容量プールおよびエンタープライズプールは、引き続きサポートされます。

DL Appliance は容量ベースのライセンスを使用するため、ライセンスプールの制限には影響されません。フロントエンド容量ライセンスを使用するソフトウェアベースの Rapid Recovery 環境も同様にエージェントレス保護を使用することで得られるライセンス上の利点はありません。エージェントレス保護を使用するその他の利点は、容量ライセンスプールが使用中でも関連性があります。

Rapid Recovery リリース 6.2.1 環境でエンタープライズライセンスプールを使用している場合は、次のルールが適用されます。

- Rapid Recovery Agent で保護されている Hyper-V または vCenter/ESXi ハイパーバイザホストは、各プロセッサソケットにつき 1 つのライセンスをプールから消費します。ハイパーバイザホストに 6 つの CPU ソケットがある場合、エンタープライズプールから 6 ライセンス消費します。
- Rapid Recovery Agent により Core で保護されているその他のマシン（物理または仮想）は、そのプールから 1 ライセンス消費します。これは、複数の CPU ソケットがあるアプリケーションサーバ（Exchange Server、SQL Server、または Oracle Database 12c など）の場合でも同様です。

エージェントレス保護を使用するライセンス上の利点

複数のマシンの保護ウィザードを実行して、vCenter/ESXi ハイパーバイザホストでゲスト VM を保護できます。このウィザードの **接続** ページで、**選択した VM をエージェントレスに保護** を指定した場合、そのホスト上のゲスト VM はエージェントレスで保護されます。これらの VM の場合、ライセンスプールからライセンスは消費されません。Rapid Recovery Agent はホストにインストールされませんが、そのホストを Core に追加すると、各 CPU ソケットにつき 1 ライセンスが消費されます。

Hyper-V サーバを保護するときは、Rapid Recovery Agent がホストにインストールされます。そのハイパーバイザホスト上の各 CPU ソケットについて、エンタープライズプールから 1 ライセンス消費されます。Hyper-V サーバをエージェントレスで保護するように指定する場合、ゲスト VM はエージェントレスで保護され、それらの VM については、利用可能なライセンスプールからライセンスは消費されません。

Hyper-V クラスタを保護するときは、クラスタ内の各ノードに Rapid Recovery Agent がインストールされます。ライセンスプールから 1 つのライセンスのみが消費されます。クラスタ内の CPU ソケットの合計数が消費されます。Hyper-V クラスタをエージェントレスで保護するように指定する場合、ゲスト VM はエージェントレスで保護され、それらの VM については、クラスタで利用可能なライセンスプールからライセンスは消費されません。

Rapid Snap for Virtual を使用する主なライセンス上の利点は、保護する VM に対してエンタープライズライセンスプールからのライセンスの消費を削減できることです。ESXi ハイパーバイザホスト、または Hyper-V サーバまたはクラスタのエージェントレス保護を指定した場合、ホストで作成されたすべての新しい VM は自動的にエージェントレスで保護され、エンタープライズライセンスプールからライセンスを消費しません。

そのハイパーバイザホスト上のいくつかの VM に Rapid Recovery Agent が以前にインストールされていて、Core が Rapid Recovery リリース 6.2.1 を実行している場合、次のいずれかを実行する必要があります。

- エージェントのソフトウェアを削除して VM をエージェントレスで保護する。プールからライセンスは消費されません。
- マシンを手動でエージェントレス保護に追加する。
- マシンをエージェントで保護する必要があり、ホストが Core に追加されている場合は、VM を親ホストに関連付けます。エージェントベースの保護の利点が得られ、ライセンスは消費されません。
- 何も変更しない。VM は API を使用して Rapid Recovery Agent で保護され、1 ライセンス消費されます。

Core に追加されたハイパーバイザ上の各仮想マシンは、ライセンスを消費せずにエージェントレスで保護されます。この利点を得るには、以下を実行する必要があります。

Rapid Snap for Virtual を使用する主なライセンス上の利点は、保護する VM に対してエンタープライズライセンスプールからのライセンスの消費を削減できることです。Core に追加されたハイパーバイザ上の各仮想マシン

は、ライセンスを消費せずにエージェントレスで保護されます。この利点を得るには、以下を実行する必要があります。

- **VM をエージェントなしで保護する。**複数のマシンを保護 ウィザードを使用して、VM を明示的に保護できます。ハイパーバイザホストを保護しているとき、新しい VM が作成されたときに暗黙的に保護する、**新しい仮想マシンを自動保護する** オプションも選択できます。
- **ゲスト VM とその保護対象ハイパーバイザホストを関連付ける。**Rapid Recovery Agent がインストールされている場合、(ハイパーバイザにネイティブのものではなく) その API が VM の保護に使用されます。ただし、Core に追加されているホストと VM を関連付けることで、消費されるライセンスを減らすことができます。この関連付けは、各仮想マシンのマシンレベルで実行されます。ゲスト VM をその親ハイパーバイザホストとリンクするプロセスは、手順 保護対象マシンの設定の表示と変更 の手順 3 で説明されています。
- **Agent をアンインストールする。**特に推奨がない限り、仮想マシンから Agent ソフトウェアのすべてのコピーを削除します。

エージェントレス保護に関する利点と制限、推奨される追加ソフトウェア、ホストの最小要件、などの説明については、「Rapid Snap for Virtual について」のトピックを参照してください。

Rapid Recoveryを使用した Linux マシンの保護について

Rapid Recovery Agent ソフトウェアは、複数の Linux ベースオペレーティングシステムと互換性があります (詳細については、『*Rapid Recovery #########*』に現在明示されているシステム要件を参照) 。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 マシンの対応する手順と異なる点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。

NOTE: 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。

単一の Linux マシンを保護する場合は、マシンを保護 ウィザードを使用できるようになりました。「マシンの保護」のトピックを参照してください。Core Console からウィザードを使用して複数の Linux マシンを同時に保護する場合は、「手動での複数マシンの保護」のトピックを参照してください。

Core Console から Linux マシンに Agent ソフトウェアを展開またはインストールするには、以下の準備が必要です。

- ユーザーアカウントに SUDO 権限が必要です。
- 保護する Linux マシンが SSH サーバにアクセスできる必要があります。

保護する Linux マシンがこれらの前提条件を満たしていない場合は、Linux 管理者に問い合わせてください。これらの要件を満たすと、関連するウィザードのすべてのステップを実行して、Agent ソフトウェアを展開およびインストールできます。

Oracle データベースサーバの保護について

Rapid Recoveryリリース 6.2.1 のアプリケーションサポートが拡張され、Oracle 12c リレーショナルデータベースサーバのエージェントベースの保護が含まれるようになりました。Oracle データベースサーバとそのすべてのデータベースを保護して、関連するタスクを実行することができます。

このリリースでは、次の制限が適用されます。

- Rapid Recovery Core の保護対象としてテスト済みの、サポート対象バージョンは Oracle 12c のみです。Oracle のその他のバージョンは、各自の責任においてご使用ください。
- 保護対象の Oracle データベースサーバは、64 ビット版の Windows Server 2012 R2 x64 または Windows Server 2016 を実行している必要があります。
- Rapid Recovery Agent ソフトウェア（リリース 6.2.1 以降）を Oracle サーバにインストールする必要があります。エージェントレス保護は、将来のリリースでサポートされる予定です。
- Oracle12c データベースの保護は、ARCHIVELOG モードでボリュームスナップショットサービス（VSS）を使用している場合に限定されます。

> **NOTE:** NOARCHIVELOG（Oracle データベースのデフォルトのログモード）は、将来のリリースでサポートされる予定です。また、ARCHIVELOG モードを有効にした Oracle データベースを、ARCH（アーカイブ）プロセスを使用してすべてのオンライン REDO ログをアーカイブするように設定することも必要です。データベース管理者（DBA）は、Oracle SQL*Plus または Oracle Enterprise Manager を使用して、モードの変更や REDO ログのアーカイブの設定を行うことができます。ARCHIVELOG モードの有効化およびアーカイブの詳細については、Oracle のドキュメントを参照するか、Oracle 12c の認定 DBA に問い合わせてください。

Oracle サーバを完全に保護するには、次のタスクを実行します。

- Rapid Recovery Agent ソフトウェア（リリース 6.2.1 以降）を Oracle サーバにインストールして、保護を開始します。マシン保護ウィザードを使用してネットワーク上の Oracle サーバの場所を特定し、Agent ソフトウェアを展開して、保護スケジュールを設定します。詳細については、「Rapid Recovery によるマシンの保護について」を参照してください。
- Rapid Recovery Core Consoleで各データベースの資格情報を入力します。Core により資格情報が安全にキャッシュされ、ユーザーは UI を使用してメタデータにアクセスできます。資格情報を入力するまでは、保護対象の Oracle サーバ上のデータベースに関する詳細を表示することはできません。詳細については、「Oracle データベースの認証情報の入力または編集」を参照してください。
- Core Console で、保護対象の Oracle サーバのアーカイブログモードを有効にし、Oracle VSS ライターを確認します。詳細については、「保護対象 Oracle データベースのアーカイブログモードの有効化と VSS ライターの追加」を参照してください。
- ログの切り捨てポリシーを確認し、必要に応じて設定します。Oracle データベースがアーカイブログモードに設定されている場合、ログは迅速に蓄積されますが、ディスク容量が大量に消費されます。このため、夜間ジョブでは Oracle ログを自動的に切り捨てるようにデフォルト設定されます。このような夜間ジョブに用意された 3 つの削除オプションを設定するか、または夜間ジョブを無効にすることができます。詳細については、「Oracle ログの切り捨てについて」を参照してください。

  または、必要に応じて、Oracle データベースログを手動で切り捨てることもできます。この手順の詳細については、「Oracle データベースログの手動による切り捨て」を参照してください。

Agent をインストールし、マシンを Core 内で保護して、適切に設定を構成した後、次の操作を実行できます。

- **メタデータを表示する。**保護対象マシンの **[サマリ]** ページで、Oracle サーバ上の各データベースに関するメタデータを表示できます。これらのデータには、接続、および各ログファイル、制御ファイル、データファイルのステータスなどが含まれます。
- **データベースの整合性をチェックする。**Core Console で DBVERIFY ユーティリティを使用して、整合性チェックを実行できます。
- **アーカイブログを切り捨てる。**3 つの削除ポリシーのいずれかを使用します。
- **データベースをリストアする。**すべてのボリュームをリストアするか、選択したデータベースを含むボリュームをリストアできます。アーカイブログモードを有効にすると、Oracle データベースのスナップショットは、Oracle サービスから見てクラッシュ整合性が保たれている状態になります。
- **仮想エクスポートを実行する。**1 回限りのエクスポートを行うか、または仮想スタンバイ VM をセットアップして、保護対象データベースでバックアップが取得されると VM が新しい情報で随時更新されるようにすることができます。

Oracle データベースの VM を起動する場合、データベースサービスを手動で開始し、データベースデータファイルのバックアップモードを手動で無効にすることが必要になる場合があります。

Oracle データベースの認証情報の入力または編集

この手順を実行する前に、まず Core の保護対象に Oracle データベースサーバを追加する必要があります。

Oracle データベースの認証情報を入力または編集するには：

- この手順を実行する Rapid Recovery ユーザーの Windows ユーザーアカウントには、保護対象データベースサーバの SYSDBA 権限が必要です。
- データベースが Rapid Recovery Core サーバからアクセス可能で、接続が正常に確立されている必要があります。

NOTE: SYSDBA は、高レベル管理操作の実行に必要な Oracle システムのデータベース管理権限です。これらの機能には、Oracle データベースの作成、起動、シャットダウン、バックアップ、またはリカバリが含まれます。

Oracle データベースサーバを保護した後、データベースごとに認証情報を入力するまで、データベースのメタデータにアクセスしたり、データベースの詳細を表示したりすることはできません。この 1 回限りの手順により、データベース認証情報が安全にキャッシュされ、Core Console には、Oracle データベースを構成するすべての保護対象トランザクションログファイル、制御ファイル、およびデータファイルに関するステータス情報へのアクセスが提供されます。

たとえば、保護対象 Oracle マシンの **サマリ** ページでは、認証情報を入力する前に、Oracle Server 情報 ペインで保護対象データベースの詳細を展開することはできません。

NOTE: これは、新規の保護対象 Oracle データベースごとに必要な 1 回限りの手順です。

この手順を実行して、保護対象 Oracle データベースに必要なメタデータへのアクセスを Rapid Recovery Core Console に提供します。

1. Rapid Recovery Core Console で保護対象の Oracle マシンに移動します。

   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、**Oracle Server 情報** ペインまで下にスクロールします。
3. 表内の最初のデータベースで、 （その他のオプション）ドロップダウンリストをクリックし、**認証情報を編集** を選択します。

   インスタンス認証情報の編集 ダイアログボックスが表示されます。
4. サポートされている接続タイプは、基本、および Transparent Network Substrate （TNS、独自の Oracle ネットワーキング技術）の 2 つです。次のいずれかを実行します。
   - 基本接続を使用して接続するには、次の表の情報を入力します。

オプション	説明
接続タイプ	基本
ホスト名	ホスト名または IP アドレスを入力します。
ポート(O)	適切なポートを入力します。この目的で開いているデフォルトのポートは 1521 です。

オプション	説明
SID または サービス名	適切な接続方法を選択します。次のいずれかを使用できます。 • **SID**。Oracle システム識別子（SID）は、データベースインスタンスを一意に識別する固有の ID です。 • **サービス名**。サービス名は、データベースにリモート接続するために使用される TNS エイリアスです。 **NOTE:** サービス名は、TNSNAMES.ORA ファイルで見つけることができます。
サービス名	サービス名は、データベースと該当サービスにリモートで接続するときに指定する TNS エイリアスです。

- TNS を使用して接続するには、次の表の情報を入力します。

オプション	説明
接続タイプ	TNS
ネットワークエイリアス	このドロップダウンメニューを選択して、ネットワークで使用可能なデータベースエイリアスを表示し、適切なエイリアスを選択します。

5. Oracle、およびオペレーティングシステムの2 つの認証情報タイプがサポートされています。次のいずれかを実行します。
   - Oracle 認証情報を使用して接続するには、関連するテキストフィールドに Oracle データベースのユーザー名とパスワードを入力します。

     NOTE: Windows ユーザーアカウントに、SYSDBA 権限が必要です。
   - オペレーティングシステムにキャッシュされた認証情報を使用して接続するには、**オペレーティングシステム** を選択します。

     NOTE: Windows ユーザーアカウントは、ORA_DBA ローカルグループのメンバーである必要があります。これにより、ユーザーは SYSDBA 権限を持つようになります。
6. 認証情報を検証するには、**確認** をクリックします。

   テスト接続が成功したかどうかを示すダイアログボックスが表示されます。
7. 次のいずれかを実行します。
   - 検証が成功した場合は、**OK** をクリックして、メッセージダイアログボックスを閉じます。
   - 成功しなかった場合は、ダイアログボックスを閉じて、接続が検証されるまでインスタンスの認証情報を変更します。認証情報について質問がある場合は、システム管理者に問い合わせてください。
8. **インスタンス認証情報の編集** ダイアログボックスで、検証が成功したら **OK** をクリックします。

   ダイアログボックスが閉じ、Rapid Recovery Core Console はすぐに認証情報を適用してキャッシュします。その後すぐに、Core Console でメタデータが取得され、選択したデータベースのステータスインジケータには緑色の（オンライン）ステータスが表示されます。
9. Oracle Server 情報 ペインにリストされている各データベースに対して、手順 3 から手順 8 を繰り返します。

この保護対象 Oracle マシンのすべてのデータベースの認証情報を入力してキャッシュした後、「保護対象 Oracle データベースのアーカイブログモードの有効化と VSS ライターの追加」で説明されている手順を実行します。

保護対象 Oracle データベースのアーカイブログモードの有効化と VSS ライターの追加

この手順を実行する前に、まず Core の保護対象に Oracle データベースサーバを追加し、各データベースの認証情報を Core Console に入力する必要があります。

データベースアプリケーションでは、アプリケーション整合性を確保するために、それぞれが特定の状態に設定された、特定のファイル (構成ファイル、ログファイル、制御ファイルなど) の組み合わせの存在が必要です。リリース 6.2.1 では、Oracle データベースでアーカイブログモードを有効にする必要があります。この手順を実行するまで、データベースサーバのスナップショットには、クラッシュ整合性はありますが、アプリケーション整合性はありません。

Volume Snapshot Service を使用してスナップショットを取得するために、Oracle VSS ライターが使用されます。このライターを有効にする必要があります。

NOTE: これらは、新しい保護対象 Oracle データベースごとに 1 回のみ必要となる手順です。

アーカイブログモードが有効になっているかどうかを確認するには、次の手順を実行します。必要に応じてそのモードを有効して、Core に VSS ライターを追加します。

1. Rapid Recovery Core Console で保護対象の Oracle マシンに移動します。

   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、**Oracle Server 情報** ペインまで下にスクロールします。
3. **Oracle Server 情報** ペインで、アーカイブログモードが無効になっていることを警告する通知が表示された場合は、**これらのデータベースのアーカイブモードを有効にする** をクリックして、次にデータベースインスタンスの再起動を確認します。

   NOTE: アーカイブモードを有効にすると、関連するデータベースインスタンスが再起動されます。これには数分かかる場合があります。
4. **Oracle Server 情報** ペインで、Oracle VSS ライターがスナップショットから除外されていることを警告する通知が表示された場合は、**Oracle VSS ライタを含める** をクリックして確定します。

   警告メッセージが閉じ、VSS ライターが Core に追加されます。
5. 必要に応じて、アーカイブログモードを有効にするまでの進捗状況、または VSS ライターを追加するまでの進捗状況を追跡できます。詳細については、タスクの表示を参照してください。

Oracle ログの切り捨てについて

リリース 6.2.1 の Oracle サポートに必要とされるアーカイブログモードでは、多数のログファイルがデータベースサーバに蓄積されて、貴重なストレージ領域が消費されます。リカバリポイントのスナップショットが取得されるたびに、関連するログファイルが Oracle サーバのバックアップに含まれるため、ローカルログが必要以上に増えていきます。このため、Rapid Recovery Core には、Oracle ログを切り捨てるための方法がいくつか用意されています。

1. Rapid Recovery Core には、Oracle ログを切り捨てる夜間ジョブ設定があります。Oracle ログの切り捨ては、**自動** 削除ポリシーを使用している夜間ジョブでは、デフォルトで有効になります。このモデルでは、ログは毎日 1 回、夜間ジョブの実行時に切り捨てられます。

   この設定は、ほとんどのユーザーのニーズに合うように設計されています。この方法で問題がなければ、設定を変更する必要はありません。この設定はデフォルトで有効になっています。

2. 特定の Oracle サーバについて、Oracle ログの切り捨ての夜間ジョブ設定をカスタマイズすることができます。その他 2 つの削除ポリシーから選択できます。
   - **最新を保持** 削除ポリシーでは、Oracle ログを保持する期間 (n 日、週間、か月、年) を指定します。この期間を過ぎるとログは切り捨てられます。この期間が終了した後、しきい値を超えたログファイルは、毎日 1 回夜間ジョブの実行時に切り捨てられます。
   - **指定された数を保持** 削除ポリシーでは、保持するログファイルの具体的な数を指定できます。そのしきい値に達した後は、新しいログが保存され、古いログは毎日 1 回、夜間ジョブの実行時に切り捨てられます。

   夜間ジョブで実行する切り捨ての詳細については、「夜間ジョブについて」のトピックを参照してください。
3. ログは、いつでも必要に応じて手動で切り捨てることもできます。これを行う詳細については、「Oracle データベースログの手動による切り捨て」を参照してください。

夜間ジョブまたは必要時の手動による Oracle ログの切り捨ては、転送ジョブを必要とせずに実行されます。

Oracle データベースログの手動による切り捨て

この手順は、Core で保護されている Oracle データベースサーバにのみ適用されます。

リリース 6.2.1Rapid Recovery で Oracle データベースの保護をサポートするために、Oracle アーカイブログを切り捨てる夜間ジョブがデフォルトで有効になっています。この夜間ジョブを無効にできますが、その場合ローカルデータベースサーバに大量のログファイルが蓄積されます。

保護対象 Oracle サーバに対して、必要に応じていつでも Oracle データベースログを手動で切り捨てることができます。切り捨てを行うと、ローカルサーバからアーカイブログが削除されます。リポジトリに保存された各リカバリポイントでは、バックアップスナップショットが取得された時点のデータベースの状態を反映するデータベースログが保持されます。

Oracle ログファイルを手動で切り捨てるには、次の手順を実行します。

1. Rapid Recovery Core Console で保護対象の Oracle マシンに移動します。

   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、**Oracle Server 情報** ペインまで下にスクロールします。
3. 表の中の、ログを切り捨てる Oracle データベースインスタンスを表す行で、 (その他のオプション) ドロップダウンリストをクリックして、**ログの切り捨てを強制** を選択します。

   ログの切り捨てを強制 ダイアログボックスが表示されます。
4. ローカルデータベースサーバから、すべての Oracle ログを削除する場合は、**削除ポリシー** ドロップダウンメニューから **自動** を選択して、**強制** をクリックします。

   ログ切り捨てジョブが、キューに登録されます。システムがビジー状態でない場合、ジョブはすぐに実行され、ログは切り捨てられます。
5. Oracle サーバからローカルに保存されているすべてのログを削除する場合 (最新のリカバリポイントにコピーが保存される) は、次の手順を実行します。
   a. **削除ポリシー** ドロップダウンメニューから、**最新を保持** を選択します。
   b. **次のログを保持** テキストフィールドに数値を入力し、期間のドロップダウンメニューから、該当する期間 (**日**、**週**、**月**、または **年**) を選択します。
   c. **強制** をクリックします。

   ログ切り捨てジョブが、キューに登録されます。システムがビジー状態でない場合、ジョブはすぐに実行され、ログは切り捨てられます。
6. 指定した件数の Oracle ログファイルを保持し、残りのログを切り捨てる場合は、次の手順を実行します。
   a. **削除ポリシー** ドロップダウンメニューから、**指定された数を保持** を選択します。
   b. **アーカイブファイル数** テキストフィールドに、保持する最新のデータベースログの合計を表す数値を入力します。
   c. **強制** をクリックします。

ログ切り捨てジョブが、キューに登録されます。システムがビジー状態でない場合、ジョブはすぐに実行され、ログは切り捨てられます。

7. このサーバ上の他のデータベースインスタンスのログを切り捨てる場合は、Oracle Server 情報 ペインにリストされている該当する各データベースに対して、手順 3 から手順 6 を繰り返します。

Rapid Recovery Core での保護対象アプリケーションサーバの管理について

Rapid Recovery は、SQL Server、Exchange Server、Oracle などのアプリケーションサーバをサポートします。Rapid Recovery がサポートする特定のバージョンについては、「*Rapid Recovery #########*」を参照してください。

これらのサポート対象アプリケーション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。

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 Server** ドロップダウンメニューが含まれます。

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。

保護対象の Oracle サーバを選択した場合、その保護対象マシンの **サマリ** ページで、保護対象の Oracle データベースサーバに独自の Oracle Server 情報 ペインまでスクロールダウンします。

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。保護対象の SQL Server、Exchange Server、Oracle サーバにのみ実行できる機能には以下が含まれています。

- **サーバログの切り捨ての強制実行**。SQL Server、Exchange メールサーバ、および Oracle データベースサーバにはサーバログがあります。SQL Server 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。Oracle についても同じことが当てはまり、ログの切り捨てにより Oracle サーバからアーカイブログファイルが削除され、保護対象サーバの領域が解放されます。
- **関連サーバの資格情報の設定**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 および Oracle 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、Exchange Server または Oracle 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、Exchange Server または Oracle Server マシン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。これらのアプリケーションサーバ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。

以下のトピックでは、SQL Server、Exchange Server または Oracle の保護対象マシンの管理について説明します。

- 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 SQL Server の設定と機能
- 保護対象 Exchange Server の設定と機能
- Oracle データベースサーバの保護について

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ティティ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、仮想スタンバイの設定、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。

サポートされるアプリケーションバージョンとクラスタ設定、およびクラスタ共有ボリュームのサポートの詳細については、「*Rapid Recovery #########*」を参照してください。

Rapid Snap for Virtual について

Rapid Recovery の Rapid Snap for Virtual 機能は、Rapid Recovery Agent をすべての VM にインストールせずに Core で仮想マシン (VM) を保護できるため、エージェントレス保護としても知られています。

> **CAUTION:** Quest **は、一度に 200 VM を超えない数にエージェントレスの保護を制限することをお勧めします。複数のマシンの保護ウィザードを使用する場合は、200 VM を超える値を選択しないでください。200 を超える VM の保護を開始しようとすると、UI パフォーマンスが遅くなります。対象の時間が異なっている場合、Core がエージェントレスで保護できる VM の数に制限はありません。たとえば、今日 200 VM を保護し、別の 200 VM を明日保護することは可能です。**

詳細については、VMware vCenter/ESXi VM の保護およびHyper-V サーバおよびクラスタでの VM の保護を参照してください。

VMware vCenter/ESXi VM の保護

Rapid Recovery を使用すると、VM または ESXi ホストに Rapid Recovery Agent をインストールしなくても vCenter/ESXi VM を保護し、完全なエージェントレス保護を実現することができます。Rapid Recovery は、ESXi クライアントおよび VMware にネイティブのアプリケーションプログラムインタフェース (API) を使用して、単一のホスト上で選択された VM を検出して保護します。Rapid Recovery Core はさらに仮想マシンディスク (VMDK) と通信し、保護対象ボリュームの必要な詳細情報を確認します。Rapid Recovery では VMDK ではなくボリュームに基づいてリカバリポイントが作成されるため、各ボリュームは別々にマウント、リストア、エクスポートを実施できます。

Rapid Recovery は、厳密に言えば、VMware vCenter/ESXi ハイパーバイザホストを保護しません。複数のマシンの保護ウィザード を使用して vCenter/ESXi ホストを選択するとき、そのホストを Rapid Recovery Core 上の親エンティティとして追加します。実際のホストからのデータファイルまたはデータは、Core 上のスナップショットに含まれていません。ただし、ホスト上の VM ゲストは保護できます。保護対象 VM は、Core GUI では親ホストの下にある子として表されます。ESXi VM にエージェントレス保護を選択した場合、保護対象 VM のアイコン () は、Rapid Recovery Agent を使用して保護されている ESXi VM のアイコンとは表示が異なります (たとえば、 )。

NOTE: Quest では、vSphere または ESXi ホストで保護する仮想マシン (VM) に VMware Tools をインストールすることを推奨しています。Windows オペレーティングシステム (OS) を使用する VM に VMware Tools がインストールされている場合、Rapid Recovery Core がキャプチャするバックアップは、Microsoft ボリュームシャドウコピーサービス (VSS) を使用します。これにより、アプリケーション整合性バックアップのための容量が得られます。VMware Tools を使用する場合、または使用しない場合のエージェントレス 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ハイパーバイザツールをインストールする利点」および「クラッシュ整合性バックアップとアプリケーション整合性バックアップについて」を参照してください。

VMware Tools がインストールされているとき、エージェントレス保護では VMware Changed Block Tracking (CBT) を使用して、増分スナップショットに必要な時間を短縮します。CBT により、VMDK ファイルで変更されているブロックが決定されるため、Rapid Recovery では最後のスナップショット以降に変更されたディスクの一部のみがバックアップされます。このバックアップ方法では多くの場合、バックアップ処理時間が短くなり、ネットワークとストレージのエレメントのリソース消費量が削減されます。

エージェントレス保護の使用には複数の利点があります。もっとも有用な属性の一部として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。
- エージェントレス保護により、ESXi ホストまたは Hyper-V ホストに追加された新しい仮想マシンを自動的に保護することを選択できます。
- 保護プロセス中に再起動は必要ありません。
- 個々の VM の認証情報は必要ありません。
- エージェントレス保護により、電源がオフになっていても VM を保護することができます。
- エージェントレス保護により、ディスクにリストアすることができます。
- エージェントレス保護では、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ています。
- ゲスト VM を保護されている親ハイパーバイザホストと関連付けた場合、Core で VM を保護するときにエンタープライズライセンスは消費されません。
- 必要に応じて、SQL Server および Exchange のメタデータを保護および収集できます。
- Core (Agent ではなく) は、保護対象の SQL Server および Exchange Server から取得したリカバリポイントの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す。
- エージェントレス保護により、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することができます。

  NOTE: ダイナミックボリュームが複雑 (ストライプ、ミラーリング、スパン、または RAID を適用) である場合、ディスクイメージとしてエクスポートされ、エクスポート対象仮想マシン上でエクスポート操作が完了した後、ボリュームへと解析されます。

ESXi 仮想マシンにエージェントレス保護を使用する理由は多数ありますが、環境と業務のニーズに最も適した保護方法を選択してください。前述した利点とともに、エージェントレス保護を選択するときには次の考慮事項にも注意してください。

- Oracle データベースサーバのエージェントレス保護では、Oracle 関連メタデータは収集されません。ファイルとオペレーティングシステムはスナップショットでバックアップされますが、Oracle 関連機能は

サポートされません。Oracle データベースのアプリケーションのサポートについては、Rapid Recovery Agent を使用してサーバを保護します。

- エージェントレス保護では動的ボリュームの保護をボリュームレベルでサポートしていません（たとえば、スパン、ストライプ、ミラーリング、または RAID の適用ボリューム）。ディスクレベルで保護します。
- エージェントレス保護は、Live Recovery をサポートしていません。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 に対する単一ボリュームの復元プロセス中、VM は自動的に再起動されます。
- エージェントレス保護では、仮想ディスクのタイプがシックプロビジョニング（Eager Zeroed）である場合、VM の使用中スペースの実際の量が表示されません。

エージェントレス保護を ESXi 仮想マシンに使用することを選択した場合、エージェントレス保護が正常に完了するには、ホストが次の必要最小要件を満たしている必要があります。

- ホストマシンで ESXi バージョン 5.0.0 Build 623860 以降が実行されている必要があります。
- ホストマシンは、『*Rapid Recovery #########*』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には、VMDK に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）のいずれかが含まれている必要があります。これらのパーティションテーブルがない VMDK は、個々のボリュームではなくディスク全体で保護されます。
- 各 VMware 仮想マシンには、スナップショットの整合性を確保するため、VMware Tools がインストールされている必要があります。

Hyper-V サーバおよびクラスタでの VM の保護

Hyper-V VM をエージェントレスで保護するには、各 VM に Rapid Recovery Agent を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。Agent はホスト上の仮想ハードディスクを保護し、ハードディスクファイルへの変更をファイルシステムに応じてボリュームイメージまたはディスクイメージに変換します。新しいドライバではホスト上およびクラスタ共有ボリューム（CSV）上の VM にファイルレベルのサポートを提供します。

Hyper-V のエージェントレスサポートは、ホスト上のオペレーティングシステムにより決定されます。オペレーティングシステム、およびそれぞれでサポートされる Rapid Recovery コンポーネントの完全なリストは、『*Rapid Recovery #########*』で維持管理されています。詳細については、その文書の「Rapid Recovery リリース 6.2 のオペレーティングシステムのインストールと互換性対照表」のトピックを参照してください。

Quest では、Hyper-V ホストで保護する仮想マシン（VM）に Hyper-V 統合サービスをインストールすることを推奨しています。Windows OS を使用して Hyper-V 統合サービスを VM にインストールするとき、Rapid Recovery Core でキャプチャされるバックアップには Microsoft VSS が使用されます。これにより、アプリケーション整合性バックアップのための容量が得られます。Hyper-V 統合サービスを使用する場合、または使用しない場合のエージェントレス 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ハイパーバイザツールをインストールする利点」および「クラッシュ整合性バックアップとアプリケーション整合性バックアップについて」を参照してください。

NOTE: Rapid Recovery では 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 上で VM を保護するには、複数のマシンの保護 ウィザードの自動展開機能を使用して、Rapid Recovery Agent とドライバを各クラスタノードにインストールする必要があります。ノードからは、Agent が各ファイルに 2 種類の変更を作成することにより、CSV で動作しているすべての VM を保護できます。1 番目の変更タイプは、スナップショット取得またはクリーンなシステム再起動の前または後にのみ保存されます。2 番目の変更タイプはディスク上に存在し、電源障害またはダーティ（不適切な）シャットダウンの場合でも、増分スナップショットが使用可能になります。ノード上にインストールされている Agent では、データを転送する前に、すべての変更が 1 つに結合されます。

ホストまたはノードが動作しているときに Rapid Recovery はバックアップを作成します。ホストが動作していない場合は、バックアップは作成できません。ただし、ノートのどれかが動作していない場合、Rapid Recovery はクラスタ上の VM のスナップショット取得を続行できます。

NOTE: 最適なパフォーマンスを得るには、Hyper-V ホストまたはノードの最大同時転送数はデフォルトの 1 に設定することをお勧めします。

エージェントレス Hyper-V による保護には、Agent がすべての VM にインストールされている場合に、従来の保護と同じ機能の多くが含まれます。

- アーカイブあーかいぶ
- リカバリポイントの整合性のチェック
- リカバリポイントのマウント
- 新しい仮想マシンの自動検出（エージェントレス保護に対して一意）
- SQL Server および Exchange Server の保護とそれらのメタデータの収集
- Exchange マウント可否チェックの実行
- SQL アタッチ可否チェックの実行
- レプリケーション
- CSV への復元、または CIF 共有フォルダへの復元を含む VM の復元
- ゲスト VHDX 形式でのファイルの復元
- ロールアップ
- Hyper-V VM および ESXi、VMware Workstation、VirtualBox などその他のハイパーバイザーへの仮想エクスポート

ただし、Hyper-V のエージェントレス保護を選択する際に考慮すべき制限があります。実行されない機能には以下のものがあります。

- Live Recovery
- VHD 形式を使用した CIFS 上の VM の復元
- ゲスト VHD（.vhd）形式でのファイルの復元
- ゲスト VHD セット（.vhds）形式でのファイルの復元

NOTE: アプリケーション整合性のあるスナップショット取得のため、各 VM に SCSI コントローラがインストールされている必要があります。このコントローラがないと、結果は常にクラッシュ整合性のあるスナップショットになります。

アプリケーションサポート

Rapid Snap for Virtual では、Hyper-V および ESXi VM で動作している SQL Server および Exchange アプリケーションのエージェントレス保護を有効にすることができます。このオプション機能は、Windows オペレーティングシステムで実行している VM で使用できます。

NOTE: アプリケーションサポートは、Linux VM にインストールされているアプリケーションには適用されません。

アプリケーションサポートを有効にすると、VM の **サマリ** ページにアプリケーションのメタデータが表示され、マシン ページの VM 名の横に アイコンが表示されます。エラーが発生しアプリケーションサポートが正常に実行できない場合、アイコンの色が緑から赤に変わります。

エージェントレスでのSQL Server または Exchange Server の保護を選択する前に、以下の考慮事項に注意してください。

- アプリケーションを保護するには、VM が起動している必要があります。Core は起動していないマシンからメタデータを取得しません。
- VMware Tools または Hyper-V 統合サービスユーティリティは、保護対象の VM 上にインストールする必要があります。
- Exchange Server と SQL Server の両方がインストールされている VM では、ログを個別に切り捨てることはできません。2 つのアプリケーションがインストールされている場合、すべてのログが切り捨てられます。
- SQL Server アタッチ可否チェックは、Core でのみ使用でき、保護対象マシンでは実行できません。
- ESXi VM でログの切り捨てを実行するには、ホストが ESXi バージョン 6.5 以降を使用している必要があります。

エージェントレス保護のためにハイパーバイザ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、Quest は vSphere または ESXi ホストで保護対象 VM に VMware Tools をインストールすることをお勧めします。同様に、Quest は、Hyper-V ホストで保護する VM に Hyper-V 統合サービスをインストールすることをお勧めします。

これらのネイティブハイパーバイザユーティリティをインストールすると、Rapid Recovery は Microsoft Volume Shadow Copy Services（VSS）機能をフル活用することができます。

これらのユーティリティが Windows オペレーティングシステムを実行している VM にインストールされているとき、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。これらの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、クラッシュ整合性でのみです。詳細については、「クラッシュ整合性バックアップとアプリケーション整合性バックアップについて」を参照してください。

次の条件は、VMware Tools または Hyper-V 統合サービス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 40. VM のバックアップタイプの条件

ハイパーバイザツール	VM の電源オン	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
インストール済み	はい	アプリケーション整合性
インストール済み	いいえ（ダーティシャットダウン）	クラッシュ整合性
インストール済み	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

クラッシュ整合性バックアップとアプリケーション整合性バックアップについて

Rapid Snap for Virtual 機能を使用して、仮想マシンをエージェントレスで保護しているとき、キャプチャしたバックアップスナップショットのデータは、次の 2 つのうちいずれかの状態になります。

- クラッシュの整合性：少なくとも、Rapid Recovery Core によりキャプチャされたすべてのエージェントレスバックアップにはクラッシュ整合性がある必要があります。バックアップは、ファイルがキャプチャされた時点での、各保護ボリューム上のすべてのデータとオペレーティングシステムファイルのそのときのスナップショットです。クラッシュ整合性リカバリポイントから復元する場合、VM OS が起動して、ファイルシステムとその中にあるすべてのファイルを読み込んで認識できます。

  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。

- **アプリケーション整合性**。アプリケーション整合性バックアップは、Microsoft の Volume Shadow Copy Service（VSS）を使用して、シャドウコピーが作成されるときにアプリケーションデータの整合性を確保します。スナップショットがキャプチャされる前に、VSS ライターを使用して、保留中の入力/出力操作が完了され、ログファイルがコミットされます。結果として、アプリケーション整合性リカバリポイントから復元した場合、VM OS が起動し、ファイルシステムを読み込んで認識できます。また、SQL Server または Exchange などの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 ログはデータファイルと一致し、データベースは何の修復も必要とせずにすばやく表示されます。

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。

NOTE: Agent のインストーラへのアクセスについては、「Rapid Recovery Agent 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、『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 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。

NOTE: Core のダウンロードは、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、『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。

Rapid Recovery Agent インストーラのダウンロード

Rapid Recovery Agent 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. ウェブブラウザで、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 のアイコンバーで、**その他** アイコンをクリックして **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。

Core Console からの複数マシンへの Agent の同時展開

Rapid Recovery Agent ソフトウェアを同時に複数の Windows マシンに展開することができます。マシンは Active Directory ドメイン、vCenter または ESXi の仮想ホストまたは Hyper-V 仮想ホストの一部にすることができます。あるいは、Rapid Recovery Agent ソフトウェアのアップグレード時など、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することができます。また、特定のドメインやホストに関連付ける必要がないマシンに、ソフトウェアを手動で展開することも可能です。

また、Core Console から 1 台または複数の Linux マシンに手動で Rapid Recovery Agent ソフトウェアを展開することができます。

CAUTION: AppAssure Agent が以前に Linux マシン上にインストールされていた場合、Rapid Recovery Agent をインストールする前に、シェルスクリプトを使用してマシンから AppAssure Agent を削除します。Linux マシンからの Agent の削除については、『*Rapid Recovery ##########*』の「Uninstalling the AppAssure Agent software from a Linux machine（Linux マシンからの AppAssure Agent ソフトウェアのアンインストール）」のトピックを参照してください。Agent ソフトウェアを Linux マシン上に正しく展開するには、同じドキュメントの「About installing the Agent software on Linux machines（Linux マシンでの Agent ソフトウェアのインストールについて）」のトピックの前提条件を参照してください。

Rapid Recovery Agent ソフトウェアを展開しても、マシンは自動的には保護されません。展開後に、Core Console のボタンバーから **複数のマシンを保護** オプションを選択する必要があります。

NOTE: これまで、複数のマシンに同時に展開する機能は、一括展開と呼ばれてきました。また、複数のマシンを同時に保護する機能は、一括保護と呼ばれてきました。

複数のマシンに同時展開してそれらを保護するには、次のタスクを実行します。

- Rapid Recovery Agent を複数のマシンに展開します。詳細については、「Core Console からの複数マシンへの Agent の同時展開」を参照してください。
- 展開を監視します。詳細については、「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。詳細については、「複数のマシンの保護について」を参照してください。

  NOTE: 展開中に 複数のマシンを保護 のインストールオプションを選択した場合は、このタスクをスキップします。
- 一括保護のアクティビティを監視します。詳細については、「複数マシンの保護の監視」を参照してください。

Agent ソフトウェアの展開 ウィザードを使用した 1 台または複数のマシンへの展開

Rapid Recovery Agent ソフトウェアを 1 台または複数のマシンに展開するタスクは、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。

Linux マシンに展開する場合、この方法が適切です。

NOTE: これまで、この機能は「一括展開」と呼ばれていました。

Agent ソフトウェアの展開 ウィザードを使用すると、Rapid Recovery Core では次のことができます。

1. Active Directory ドメイン上の Windows マシンを検出し、選択したマシンへ Agent ソフトウェアをプッシュする。
2. VMware vCenter または ESXi ホストに接続して、ゲストを検出し、選択したマシンへ Agent ソフトウェアをプッシュする。
3. ローカルの Rapid Recovery Core に接続して、すでに Core によって保護されている Windows マシンに最新の（新しい）Agent ソフトウェアを展開する。（Linux マシンの場合、手動で展開するオプションを使用）。
4. Hyper-V サーバまたはクラスタに接続し、ゲストを検出して、選択したマシンに Agent ソフトウェアをプッシュする。
5. IP アドレスおよび資格情報を使用して、Linux または Windows マシンを手動で指定し、Agent ソフトウェアを選択したマシンにプッシュする。

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/ESXi 仮想ホスト上のマシンへの展開
- Rapid Recovery Agent 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

NOTE: Quest では、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。

NOTE: 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利用できない場合は、Core Console を使用してインストーラを USB ドライブなどのストレージメディアにダウンロードします。その後、保護するマシンにこのソフトウェアを実際にインストールします。詳細については、「Rapid Recovery Agent 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

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。

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。

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、**Agent ソフトウェアの展開** 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 41. ドメイン情報と資格情報

テキストボックス	説明
Host	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(A)	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場合でも選択内容に問題がなければ、**終了** 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 ドメインでの複数マシンの保護」の完了後に開始されます。

VMware vCenter/ESXi 仮想ホスト上のマシンへの展開

Rapid Recovery Agent ソフトウェアを 1 つまたは複数の VMware vCenter/ESXi 仮想ホスト上のマシンに同時に展開するには、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/ESXi 仮想ホスト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。

NOTE: 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、**Agent ソフトウェアの展開** をクリックします。

   Agent ソフトウェアの展開 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 / ESXi** 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 42. Center/ESXi 接続の設定

テキストボックス	説明
Host	VMware vCenter Server/ESXi 仮想ホストの名前または IP アドレス。
ポート(O)	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(A)	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。
   - ホストおよびクラスタ
   - 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`。

   NOTE: 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場合でも選択内容に問題がなければ、**終了** 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「VMware vCenter/ESXi 仮想ホスト上での複数のマシンの保護」の完了後に開始されます。

Rapid Recovery Agent 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

Agent ソフトウェアの展開 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 Windows マシンに Rapid Recovery Agent 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。

NOTE: Linux ユーザーは、Agent の以前のバージョンが AppAssure ブランド（リリース 5.4.3 またはそれ以前）の場合、最初に特定の AppAssure Agent のバージョンに該当する shell スクリプトを使用して、Agent ソフトウェアを削除する必要があります。Rapid Recovery Agent のインストール後に AppAssure Agent を削除すると、Linux マシンと Core の間の接続が切れることがあります。Linux マシンから AppAssure Agent をアンインストールする方法の詳細については、『*Rapid Recovery I########## ########*』の「Uninstalling the AppAssure Agent software from a Linux machine」（Linux マシンからの AppAssure Agent ソフトウェアのアンインストール）を参照してください。

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、**Agent ソフトウェアの展開** をクリックします。

   Agent ソフトウェアの展開 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 Agent 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。

   NOTE: この時点では、このプロセスを使用して保護対象 Linux マシンをアップデートすることはできません。

5. 最良の方法は、Agent ソフトウェアのインストールまたはアップデート後に各マシンを再起動することです。展開後にマシンを再起動する場合は、デフォルトオプション **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する（推奨）** のままにします。アップグレードされたマシンをすぐに起動しない場合は、このオプションをクリアしてください。
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。

手動によるマシンへの導入

Rapid Recovery Agent をローカル Core、Active Directory、vCenter/ESXi、Hyper-V 以外の任意のタイプのホスト上にある複数マシンに展開するには、次の手順に従います。

CAUTION: AppAssure Agent が以前に Linux マシン上にインストールされていた場合、Rapid Recovery Agent をインストールする前に、シェルスクリプトを使用してマシンから AppAssure Agent を削除します。Linux マシンからの Agent の削除については、『*Rapid Recovery ##########*』の「Uninstalling the AppAssure Agent software from a Linux machine (Linux マシンからの AppAssure Agent ソフトウェアのアンインストール) 」のトピックを参照してください。Agent ソフトウェアを Linux マシン上に正しく展開するには、同じドキュメントの「About installing the Agent software on Linux machines (Linux マシンでの Agent ソフトウェアのインストールについて) 」のトピックの前提条件を参照してください。

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、**Agent ソフトウェアの展開** を選択します。

   Agent ソフトウェアの展開 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、エージェントを展開する各マシンに対して、ダイアログボックスにマシンの詳細を入力します。**Enter** を押して、各マシンの情報を区別します。`Hostname::username::password::port` の形式を使用します。Windows マシンの場合、ポート設定はオプションです。Linux マシンの場合、常に SSH ポート (デフォルトは 22) を含めます。例 :

   ```
   10.255.255.255::administrator::&11@yYz90z
   abc-host-00-1::administrator::99!zU$o83r::8006
   Linux-host-00-2::administrator::p@$$w0rD::22
   ```
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 Agent 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、次に **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、次回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. 変更する設定をクリックして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、以下のいずれかのオプションを変更します。次に をクリックして設定を保存します。

表 43. 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 の保護対象に追加されたマシンの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）がリポジトリに保存されます。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リポジトリに保存されます。このタイプ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の間隔）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、毎正時（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できます。

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（12:00 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、「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。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。

See also: シンプルモードでのカスタム保護スケジュールの作成
See also: 詳細設定モードでの複数の保護スケジュール期間の作成

マシンの保護

保護するマシンに Rapid Recovery Agent ソフトウェアがすでにインストールされているけれども、まだ再起動していない場合は、今すぐマシンを再起動します。

このトピックでは、マシンの保護 ウィザードを使用して、指定した1 つのマシン上のデータの保護を開始する方法について説明します。1 つのプロセスを使用して同時に複数のマシンを保護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。

NOTE: エージェントレスの保護を VMware または ESXi ホストまたは Hyper-V ホストで使用する場合を除き、保護対象マシンには、保護のために Rapid Recovery Agent ソフトウェアをインストールする必要があります。Agent ソフトウェアは、この手順の前にインストールするか、マシンの保護 ウィザードで指定したターゲットマシンに導入するかのどちらかを選択できます。エージェントレスの保護とその制限事項の詳細については、「Rapid Snap for Virtual について」を参照してください。

NOTE: Agent ソフトウェアのインストールの詳細については、『*Rapid Recovery ##########################*』の Rapid Recovery Agent ソフトウェアのインストールに関する項を参照してください。マシンを保護する前に Agent ソフトウェアがインストールされていない場合は、このウィザードで特定の保護対象ボリュームを選択できません。この場合、デフォルトでは、エージェントレスで保護されているマシン上のすべてボリュームが保護されます。Rapid Recovery では、EISA パーティションで設定されたマシンの保護およびリカバリがサポートされています。Windows リカバリ環境 (Windows RE) を使用する Windows 8 および 8.1、および Windows 2012 および 2012 R2 マシンもサポートされます。

保護を追加するときには、IP アドレスやポートなどの接続情報の定義と、保護するマシンの資格情報の入力が必要です。必要に応じて、IP アドレスの代わりに Core Console に表示される表示名を入力できます。表示名を入力すると、Core Console で詳細を表示したとき、保護対象マシンの IP アドレスが表示されなくなります。また、マシンの保護スケジュールを定義することもできます。

保護プロセスには、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)、このマシンの Core に保存されるデータに適用することもできます。暗号化キーの詳細については、「暗号化」を参照してください。

環境によっては、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 Agent 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 Agent 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 にリポジトリが既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。

CAUTION: 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。今後、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 ext3 または ext4 に変換する必要があります。

1. 次のいずれかを実行します。
   - マシン保護ウィザードから開始する場合、手順 2 に進みます。
   - Rapid Recovery Core Console から開始する場合、ボタンバーの **保護** をクリックします。

   マシン保護ウィザード が表示されます。
2. **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。
   - リポジトリの定義や暗号化の設定が必要ない場合、**一般** を選択します。
   - リポジトリを作成する必要がある場合、選択したマシンのバックアップ用に別のリポジトリを定義する必要がある場合、またはウィザードを使用して暗号化を設定する必要がある場合は、**詳細 (任意指定のステップを表示)** を選択します。
   - マシン保護ウィザードの **ようこそ** ページが今後表示されないようにするには、オプション **ウィザードが次に開かれたときにこの「ようこそ」ページをスキップする。** を選択します。
3. ようこそ 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。

   接続 ページが表示されます。
4. **接続** ページで、次の表の説明に従って、接続するマシンに関する情報を入力し、**次へ** をクリックします。

表 44. マシンの接続設定

テキストボックス	説明
オペレーティングシステム	保護するマシンのオペレーティングシステムに応じて、Windows または Linux を選択します。
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(O)	Rapid Recovery Core 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（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	このマシンに接続するために使用するパスワード。

次回、マシン保護ウィザードで **エージェントのインストール** ページが表示された場合、これは、Rapid Recovery がマシン上で Rapid Recovery Agent を検知せず、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 6 に進みます。

ウィザードで、次に **Agent をアップグレード** ページが表示された場合は、保護するマシンに旧バージョンの Agent ソフトウェアが存在することを示します。

NOTE: Core にバックアップするには、保護するマシンに Agent ソフトウェアをインストールして、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対象マシンを再起動するには、**インストール後に、マシンを自動的に再起動します（推奨）** オプションを選択してから 次へ をクリックします。

5. **Agent をアップグレード** ページで、次のいずれかを実行します。
   - Rapid Recovery Core のバージョンに合わせて、Agent ソフトウェアの新規バージョンを導入するには、**Rapid Recovery Agent ソフトウェアを最新バージョンにアップグレードします** を選択します。
   - Agent ソフトウェアのバージョンを更新せずにマシンの保護を継続するには、オプション **Rapid Recovery Agent ソフトウェアを最新バージョンにアップグレードします** をオフにします。
6. **次へ** をクリックします。

   「**保護**」ページが表示されます。
7. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

   64 文字まで入力できます。「使用禁止文字」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「禁止語」で説明した文字の組み合わせを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設定を選択します。
   - 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。

     デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、**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。

スケジュール オプションがウィザードワークフローに追加されます。

9. **保護** ページの下部で、この Core で以前に保護されていたマシンを再保護していて、元のリポジトリとは異なるリポジトリを指定する場合は、**このマシンに新しいリポジトリを選択する** オプションを選択します。

   詳細設定 オプション (リポジトリ と 暗号化 を含む) がウィザードワークフローに追加されます。

10. 次のように設定を続けます。

    - 手順 2 でマシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 13 に進みリポジトリを作成します。
    - マシン保護ウィザード の 一般設定 を選択して、カスタム保護を指定した場合は、**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。
    - 手順 2 で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、**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。
    - マシン保護ウィザード の 詳細設定 を選択し、カスタム保護を指定した場合は、**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。

    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。

11. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。

12. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    すでにリポジトリ情報を設定している場合、リポジトリを変更することを示さずに、手順 2 で 詳細設定 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 16 に進みます。

    すでにリポジトリ情報を設定している場合、手順 2 で 詳細設定 オプションを選択した場合、またはリポジトリを変更することを示した場合は、**リポジトリ** ページが表示されます。手順 13 に進みます。

13. **リポジトリ** ページで、次の手順を実行します。

    - 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 15 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 45. リポジトリの設定

テキストボックス	説明
名前	リポジトリの表示名を入力します。

テキストボックス	説明
	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

14. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
15. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 46. ストレージ設定の詳細

テキストボックス	説明
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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

16. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 47. 新しい暗号化キーを定義

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。
Passphrase（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。

テキストボックス	説明
	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。Quest Data Protection 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。

17. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
18. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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。

NOTE: 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、「リポジトリについて」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. ウィザードの **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。
   - 一般
   - 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、次の情報を入力します。

表 48.「クラスタに接続」の設定

テキストボックス	説明
Host	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(O)	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。 デフォルトのポートは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）。

テキストボックス　説明

> **NOTE:** 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(A)　このマシンに接続するために使用するパスワード。

5. **次へ** をクリックします。

> **NOTE:** クラスタノードにすでに古いバージョンの Rapid Recovery Agent がインストールされている場合、ウィザードに アップグレード ページが表示され、Agent をアップグレードする機会が提供されます。

6. ウィザードの **ノード** ページで、保護するノードを選択します。

   システムは、選択された各マシンを自動的に検証します。

7. **次へ** をクリックします。

   クラスタを保護 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、ウィザードの **警告** ページで、マシンを選択してツールバーの **確認** 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、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。

> **NOTE:** Quest 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。

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Rapid Recovery 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. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「」で説明した文字の組み合わせを使用しないでください。

12. 次の説明に従って、適切な保護スケジュール設定を選択します。

    - 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。

デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

13. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 16 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**次へ** をクリックして手順 16 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の詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。
14. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。
15. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 19」に進みます。
16. **リポジトリ** ページで、次の手順を実行します。
    - 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 49. リポジトリの設定

テキストボックス	説明
名前	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。

テキストボックス	説明
	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

17. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
18. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 50. ストレージ設定の詳細

テキストボックス	説明
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。

テキストボックス	説明
レコードあたりのバイト数	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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

19. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 51. 新しい暗号化キーを定義

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。
Passphrase（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。Quest Data Protection 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。

テキストボックス	説明
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。

20. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
21. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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 52.「クラスタノードを保護」の設定

テキストボックス	説明
Host	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(O)	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(A)	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。

   NOTE: 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. 詳細については、シンプルモードでの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。

シンプルモードでのカスタム保護スケジュールの作成

保護ウィザード内からのカスタム保護スケジュールの作成手順は、シンプルモードで既存マシンの保護スケジュールを作成する手順と同じです。ウィザード内またはシンプルモードで作成された保護スケジュールは、テンプレートとして保存されません。テンプレートまたは複数の保護スケジュールを作成するには、「詳細設定モードでの複数の保護スケジュール期間の作成」を参照してください。この手順のステップを完了して、Rapid Recovery を使用するためのカスタムスケジュールを作成し、保護対象マシンからデータをバックアップします。

1. 次のいずれかのオプションを実行します。

   - 保護ウィザード（マシンを保護、複数のマシンを保護、クラスタを保護）を使用している場合、ウィザードの **保護** ページで **カスタム保護** を選択し、**次へ** をクリックします。
   - すでに保護されているマシンに保護スケジュールを作成する場合は、保護対象マシンの サマリ ページで保護対象マシンのボリュームを展開し、該当するボリュームを選択した後、**スケジュールを設定** をクリックします。

   保護スケジュール ページまたはダイアログボックスが表示されます。

2. **保護スケジュール** ページまたはダイアログで、次のいずれかを行います。

   - 設定日付または指定時間に実行される保護期間を設定するには、**複数の期間** を選択して、手順 3 に進みます。
   - 毎日マシンをバックアップする特定の時間を設定するには、**毎日の保護時間** を選択して、手順 7 に進みます。

3. 任意の期間のスケジュール間隔を変更するには、次の手順を完了します。

   a. **開始** 時刻と **終了** 時刻を選択して、時間の間隔を作成します。

   b. 各期間について 間隔 テキストボックスをクリックした後、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。

4. 業務時間のピーク時とオフピーク時のスナップショット取得をカスタマイズするには、次の手順を完了します。ピーク期間の最適な間隔を設定し、**残り時間のスナップショットを取得** を選択してから、次の操作を行ってオフピークの時間間隔を設定します。

   a. **平日** を選択します。

   b. **開始** 時刻と **終了** 時刻を設定して、ピーク時の業務時間中の間隔を作成します。

   c. **X 分間隔** ボックスに、このピーク時の勤務時間中に Rapid Recovery がリカバリポイントを作成する必要がある頻度を示す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。

   d. オフピーク時の業務時間にスナップショット取得をスケジュールするには、**残された時間にスナップショットを取得** を選択します。

   e. **X 分間隔** ボックスに、このオフピーク時の勤務時間中に Rapid Recovery がリカバリポイントを作成する必要がある頻度を示す間隔を分単位で入力します。

たとえば、このオフピーク時間中は業務活動が少なく、バックアップへの変更も少ないため、スナップショット取得数を少なくし、デフォルトの間隔を 60 分に維持するよう決定することが考えられます。

5. 手順 7 に進みます。
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。

   ウィザードを使用している場合、ウィザードで次の手順に進みます。該当ウィザードの手順を参照して、残りの要件を完了します。

See also: 保護スケジュールについて
See also: シンプルモードでのカスタム保護スケジュールの作成
See also: 詳細設定モードでの複数の保護スケジュール期間の作成

詳細設定モードでの複数の保護スケジュール期間の作成

保護スケジュールは保護対象マシンから 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。

特定の保護対象マシンの サマリ ページでいつでも既存の保護スケジュールを変更できます。

NOTE: 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、「シンプルモードでの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、「詳細設定モードでの複数の保護スケジュール期間の作成」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マシンの名前をクリックします。
2. 選択したマシンの サマリ ページで、ボリューム ペインにある保護対象マシンのボリュームを展開して、該当する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。

   最初は、すべてのボリュームで 1 つの保護スケジュールを共有しています。

   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。(保護グループ) をクリックして保護されるボリュームを展開し、すべてのボリュームが表示されるようにして 1 つまたは複数を選択します。

   NOTE: 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。
   - ダイアログの初期ページで既存のスケジュール期間を変更する（シンプルモードと呼ばれる）には、「詳細設定モードでの複数の保護スケジュール期間の作成」の手順を参照してください。
   - 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、**詳細設定モード** をクリックして **テンプレート** ドロップダウンリストからそのテンプレートを選択し、**OK** をクリックして確認し、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。
     - 平日（月 - 金）：この時間の範囲は、一般的な週休 2 日制を意味します。
     - 週末（土、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、**詳細設定モード** をクリックして 手順 4 に進みます。
4. 期間とは、各スナップショットの取得を何分間おきにするかを決定する、指定された間隔です。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、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。
   青いバーは、この間隔を視覚的に表したものです。
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、保護を定義する期間をさらに追加します。
   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、間隔を 60 分から 120 分に変更して、2 時間に 1 回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。

> **NOTE:** 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、**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。

See also: 保護スケジュールについて
See also: シンプルモードでのカスタム保護スケジュールの作成
See also: 詳細設定モードでの複数の保護スケジュール期間の作成

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のかを選択できます。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。

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 Agent ソフトウェアをインストールする必要があります。

NOTE: このルールの例外は、VMware/ESXi または Hyper-V 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、「Rapid Snap for Virtual について」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。例:

- Agent 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 Agent ソフトウェアをインストールできます。詳細については、「Agent ソフトウェアの展開 ウィザードを使用した 1 台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 Agent 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 Agent 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 Agent 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 ドメインでの複数マシンの保護
- VMware vCenter/ESXi 仮想ホスト上での複数のマシンの保護
- Hyper-V 仮想ホスト上の複数のマシンの保護
- 手動での複数マシンの保護

Active Directory ドメインでの複数マシンの保護

次の手順を実行して、Active Directory ドメインにある 1 台以上のマシンを同時に保護します。

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. ウィザードの **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。
   - 一般
   - 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 **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認証情報を入力します。

表 53. ドメイン情報と資格情報

テキストボックス	説明
Host	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(A)	ドメインへの接続に使用するパスワード。

6. **次へ** をクリックします。
7. ウィザードの **マシンを選択** ページで、保護するマシンを選択します。

   システムは、選択され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。

   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 12 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。
9. 必要に応じて、ウィザードの **警告** ページで、マシンを選択してツールバーの **確認** をクリックすることでマシンを検証できます。
10. 必要に応じて、**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。

    NOTE: Quest 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。
11. 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Rapid Recovery 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。

12. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「」で説明した文字の組み合わせを使用しないでください。

13. 次の説明に従って、適切な保護スケジュール設定を選択します。

    - 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。

    デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

14. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 17 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**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設定します。
    - マシン保護ウィザードの詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。

15. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。

16. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 20」に進みます。

17. **リポジトリ** ページで、次の手順を実行します。

    - 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 20 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 54. リポジトリの設定

テキストボックス	説明
名前	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

18. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです)。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
19. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 55. ストレージ設定の詳細

テキストボックス	説明
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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

20. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 56. 新しい暗号化キーを定義

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。
Passphrase（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。

テキストボックス	説明
	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。Quest Data Protection 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。

21. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
22. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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。

VMware vCenter/ESXi 仮想ホスト上での複数のマシンの保護

この手順を使用して、VMware vCenter/ESXi 仮想ホスト上で 1 台、または複数のマシンを同時に保護します。

CAUTION: エージェントレス保護を使用する場合、Quest では、保護対象マシンが一度に 200 VM を超えないように制限することをお勧めします。たとえば、複数のマシンの保護ウィザードを使用する場合は、200 VM を超える値を選択しないでください。200 VM を超えて保護すると、パフォーマンスが低下します。対象の時間が異なっている場合、Core がエージェントレスで保護できる VM の数に制限はありません。たとえば、今日 200 VM を保護し、別の 200 VM を明日保護することは可能です。

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。
   - 一般
   - 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 **vCenter / ESXi** 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認証情報を入力します。

表 57. Center/ESXi 接続の設定

テキストボックス	説明
Host	VMware vCenter Server/ESXi 仮想ホストの名前または IP アドレス。
ポート(O)	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。

テキストボックス	説明
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(A)	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。

- エージェントレス保護を使用するには、**選択した VM をエージェントレスに保護** を選択し、「エージェントレスの保護を使用した vCenter/ESXi 仮想マシンの保護」を参照してください。

6. **次へ** をクリックします。
7. **マシンを選択** ページで、次のいずれかを実行します。
   - 表示されている VM のリストから、保護する VM を選択します。
   - VMware のツリー構造内を移動して、さらに VM を検索するには、**ツリーの表示** をクリックしてから、**ホストおよびクラスタ** または **VM およびテンプレート** を選択します。保護する VM を選択します。

   Rapid Recovery がオフラインのマシンまたは VMware Toolsがインストールされていないマシンを検出すると、通知が表示されます。
8. **次へ** をクリックします。
9. **調整** ページで、各マシンの資格情報を次の形式で入力します。`hostname::username::password`。

   NOTE: 各行に 1 台のマシンを入力してください。
10. **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 14 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。
11. 必要に応じて、**警告** ページでマシンを選択し、ツールバーの **確認** をクリックすることでマシンを検証できます。
12. 必要に応じて、**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。

    NOTE: Quest 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。
13. 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する必要があります。

    「**保護**」ページが表示されます。
14. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「」で説明した文字の組み合わせを使用しないでください。
15. 次の説明に従って、適切な保護スケジュール設定を選択します。
    - 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。

デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

16. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 19 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**次へ** をクリックして手順 19 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の詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。
17. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。
18. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 22」に進みます。
19. **リポジトリ** ページで、次の手順を実行します。
    - 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 22 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 58. リポジトリの設定

テキストボックス	説明
名前	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。

テキストボックス	説明
	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

20. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
21. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 59. ストレージ設定の詳細

テキストボックス	説明
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。

テキストボックス	説明
レコードあたりのバイト数	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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

22. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 60. 新しい暗号化キーを定義

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。
Passphrase（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。Quest Data Protection 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。

テキストボックス	説明
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。

23. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
24. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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。

エージェントレスの保護を使用した vCenter/ESXi 仮想マシンの保護

次の手順に従って、ESXi 仮想マシンをエージェントレスで保護します。

NOTE: Rapid Recovery では、vSphere または ESXi ホストで保護する仮想マシン（VM）に VMware Tools をインストールすることを推奨しています。Windows オペレーティングシステム（OS）を使用する VM に VMware Tools がインストールされている場合、Rapid Recovery Core がキャプチャするバックアップは、Microsoft Volume Shadow Services（VSS）を使用します。VMware Tools を使用する場合、または使用しない場合のエージェントレス 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ハイパーバイザツールをインストールする利点」を参照してください。

CAUTION: Quest は、一度に 200 VM を超えない数にエージェントレスの保護を制限することをお勧めします。たとえば、複数のマシンの保護ウィザードを使用する場合は、200 VM を超える値を選択しないでください。200 VM を超えて保護すると、パフォーマンスが低下します。対象の時間が異なっている場合、Core がエージェントレスで保護できる VM の数に制限はありません。たとえば、今日 200 VM を保護し、別の 200 VM を明日保護することは可能です。

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。
   - 一般
   - 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 **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認証情報を入力します。

表 61. vCenter/ESX（i）の接続設定

テキストボックス	説明
Host	仮想ホストの名前または IP アドレス
ポート(O)	仮想ホストへの接続に使用するポート。

テキストボックス	説明
	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(A)	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. **選択済み 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ています）。
7. **マシンを選択** ページで、次のいずれかを実行します。
   - 表示されている VM のリストから、保護する VM を選択します。
   - VMware のツリー構造内を移動して、さらに VM を検索するには、**ツリーの表示** をクリックしてから、**ホストおよびクラスタ** または **VM およびテンプレート** を選択します。保護する VM を選択します。
8. 新しい VM がホストに追加されたときに、この VM を自動的に保護するには、**新しいマシンを自動保護** を選択して、**次へ** をクリックします。

   NOTE: 保護する各 VM で、VMware Changed Block Tracking（CBT）を有効にする必要があります。有効になっていない場合、確実に保護できるように Rapid Recovery は自動的に CBT を有効にします。

   a. **自動保護** ページで、新しいマシンの追加先とするコンテナを選択します。
9. **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 12 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。
10. 必要に応じて、**警告** ページでマシンを選択し、ツールバーの **確認** をクリックすることでマシンを検証できます。
11. **次へ** をクリックします。

    保護 が表示されます。
12. 次の説明に従って、適切な保護スケジュール設定を選択します。
    - 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。

デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

13. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 15 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**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。
    - マシン保護ウィザードの詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。
14. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 18」に進みます。
15. **リポジトリ** ページで、次の手順を実行します。
    - 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 18 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 62. リポジトリの設定

テキストボックス	説明
名前	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル（Core マシン上のドライブ）または CIFS 共有ネットワークドライブを指定できます。

テキストボックス	説明
	CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

16. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
17. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 63. ストレージ設定の詳細

テキストボックス	説明
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。
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。

テキストボックス	説明
	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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

18. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 64. 新しい暗号化キーを定義

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 ー 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。
Passphrase (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。Quest Data Protection 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。

19. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
20. **終了** をクリックし、設定を保存して適用します。

マシンに対してはじめて保護が追加されると、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。

Hyper-V 仮想ホスト上の複数のマシンの保護

この手順を使用して、Hyper-V 仮想ホスト上で 1 台、または複数のマシンを同時に保護します。

CAUTION: エージェントレス保護を使用する場合、Quest では、保護対象マシンが一度に 200 VM を超えないように制限することをお勧めします。たとえば、複数のマシンの保護ウィザードを使用する場合は、200 VM を超える値を選択しないでください。200 VM を超えて保護すると、パフォーマンスが低下します。対象の時間が異なっている場合、Core がエージェントレスで保護できる VM の数に制限はありません。たとえば、今日 200 VM を保護し、別の 200 VM を明日保護することは可能です。

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。
   - 一般
   - 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次のいずれかのオプションを選択します。
   - Hyper-V サーバ
   - Hyper-V クラスタ
5. 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 65. Hyper-V の接続設定

テキストボックス	説明
Host	仮想ホストの名前または IP アドレス
ポート(O)	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 8006 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(A)	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. 必要に応じて、エージェントレスの保護を使用するには、**ゲスト VM 内で Agent を必要とせずに Hyper-V サーバを保護する** を選択し、「エージェントレス保護を使用した Hyper-V 仮想マシンの保護」を参照してください。
7. **次へ** をクリックします。
8. **マシンを選択** ページで、保護する VM を選択します。
9. 必要に応じて、新しい VM がホストに追加されたときに VM を自動的に保護する場合は、**新しい仮想マシンを自動保護する** を選択します。
10. **次へ** をクリックします。
11. **調整** ページで、各マシンの資格情報を次の形式で入力します。`hostname::username::password`。

NOTE: 各行に 1 台のマシンを入力してください。

12. **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 15 にスキップします。

    保護するマシンに Agent ソフトウェアが存在する場合、または指定したマシン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。

13. 必要に応じて、**警告** ページでマシンを選択し、ツールバーの **確認** をクリックすることでマシンを検証できます。
14. 必要に応じて、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。

NOTE: Quest 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。

15. 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する必要があります。

    「**保護**」ページが表示されます。

16. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「」で説明した文字の組み合わせを使用しないでください。

17. 次の説明に従って、適切な保護スケジュール設定を選択します。

    - 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。

    デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

18. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 20 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**次へ** をクリックして手順 20 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の詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。

19. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

NOTE: 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。

20. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 23」に進みます。

21. **リポジトリ** ページで、次の手順を実行します。

    - 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 23 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 66. リポジトリの設定

テキストボックス	説明
名前	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。

テキストボックス	説明
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

22. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
23. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 67. ストレージ設定の詳細

テキストボックス	説明
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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

24. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 68. 新しい暗号化キーを定義

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。
Passphrase（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。Quest Data Protection 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。

25. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
26. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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。

エージェントレス保護を使用した Hyper-V 仮想マシンの保護

Rapid Snap for Virtual 機能を使用すると、すべての仮想マシン（VM）ではなく Hyper-V ホスト上のみに Rapid Recovery Agent をインストールすることにより Hyper-V 仮想マシンまたはクラスタをエージェントレスで保護することができます。

CAUTION: Quest は、一度に 200 VM を超えない数にエージェントレスの保護を制限することをお勧めします。たとえば、複数のマシンの保護ウィザードを使用する場合は、200 VM を超える値を選択しないでください。200 VM を超えて保護すると、パフォーマンスが低下します。対象の時間が異なっている場合、Core がエージェントレスで保護できる VM の数に制限はありません。たとえば、今日 200 VM を保護し、別の 200 VM を明日保護することは可能です。

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。
   - 一般
   - 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次のいずれかのオプションを選択します。
   - Hyper-V サーバ
   - Hyper-V クラスタ
5. 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 69. Hyper-V の接続設定

テキストボックス	説明
Host	仮想ホストの名前または IP アドレス
ポート(O)	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 8006 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(A)	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. 手順 4 での選択に応じて、**ゲスト VM 内で Agent を必要とせずに Hyper-V サーバを保護する** または **ゲスト VM 内で Agent を必要とせずに Hyper-V クラスタを保護する** が選択されていることを確認します。（このオプションは、デフォルトで選択されています）。
7. **次へ** をクリックします。
8. **マシンを選択** ページで、保護する VM を選択します。
9. 必要に応じて、新しい VM がホストに追加されたときに VM を自動的に保護する場合は、**新しい仮想マシンを自動保護する** を選択します。
10. **次へ** をクリックします。
11. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「使用禁止文字」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「禁止語」で説明した文字の組み合わせを使用しないでください。
12. 次の説明に従って、適切な保護スケジュール設定を選択します。
    - 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。

デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

13. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 16 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**次へ** をクリックして手順 16 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の詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。
14. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。
15. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 19」に進みます。
16. **リポジトリ** ページで、次の手順を実行します。
    - 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 70. リポジトリの設定

テキストボックス	説明
名前	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。

テキストボックス	説明
	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

17. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです) 。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
18. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 71. ストレージ設定の詳細

テキストボックス	説明
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。

テキストボックス	説明
レコードあたりのバイト数	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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

19. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 72. 新しい暗号化キーを定義

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。
Passphrase（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。Quest Data Protection 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。

テキストボックス	説明
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。

20. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
21. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

手動での複数マシンの保護

Agent ソフトウェアを使用して同時に保護する複数のマシンの詳細を手動で指定するには、次の手順を使用します。この詳細により、ネットワーク上の各マシンは一意に識別されます。また、詳細には、接続情報と資格情報が含まれます。このアプローチは、Linux マシンを保護する際に一般的に使用されます。ただし、このプロセスを使用すると、Windows マシンのみ、Linux マシンのみ、またはその両方の組み合わせを保護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、**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。
   - 一般
   - 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** ページで、保護するマシンごとに、ダイアログボックスにマシンの詳細を入力します。**Enter** を押して、追加する各マシンの情報を区切ります。`hostname::username::password::port` の形式を使用します。ポート設定はオプションです。Windows または Linux マシンに Agent をインストールするためのデフォルトのポートは 8006 です。例：

   ```
   10.255.255.255::administrator::&11@yYz90z
   Linux-host-00-2::administrator::p@$$w0rD::8006
   ```
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。

   NOTE: Quest 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. Rapid Recovery Core Console で、この保護対象マシンを IP アドレスではなく名前で表示するには、**保護** ページで、ダイアログボックスの **表示名** フィールドに名前を任意で入力します。

    64 文字まで入力できます。「」のトピックで説明した特殊文字は使用しないでください。また、表示名の先頭に、「」で説明した文字の組み合わせを使用しないでください。

12. 次の説明に従って、適切な保護スケジュール設定を選択します。

    - 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。

    デフォルトの保護スケジュールでは、Core で 1 時間ごとに保護対象マシンのすべてのボリュームのスナップショットが取得されます。ウィザードを閉じた後に任意のタイミングで保護設定（保護するボリュームなど）を変更するには、特定の保護対象マシンの **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、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。

13. 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に、レポジトリが存在する場合は、**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。
    - マシン保護ウィザード の 一般設定 を選択して、デフォルトの保護を指定した場合にレポジトリが存在しない場合は、**次へ** をクリックして、手順 16 に進みリポジトリを作成します。
    - マシン保護ウィザードの一般設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。
    - 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、**次へ** をクリックして手順 16 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の詳細設定を選択し、カスタム保護を指定した場合は、**次へ** をクリックして次の手順に進み、保護するボリュームを選択します。

    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。

14. **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ます。保護しないボリュームがリストされている場合、「チェック」列内をクリックして、選択をクリアします。次に、**次へ** をクリックします。

    NOTE: 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。

15. **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て、**次へ** をクリックします。カスタム保護スケジュールの定義の詳細については、「シンプルモードでのカスタム保護スケジュールの作成」を参照してください。

    リポジトリ情報がすでに設定されており、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。「手順 19」に進みます。

16. **リポジトリ** ページで、次の手順を実行します。

    - 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は、**リポジトリ** ページで、次の表の説明に従って情報を入力し、必要に応じて、**次へ** または **完了** をクリックします。

表 73. リポジトリの設定

テキストボックス	説明
名前	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。
場所	保護対象データを保存する場所を入力します。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。場所には、ローカル (Core マシン上のドライブ) または CIFS 共有ネットワークドライブを指定できます。 CIFS 共有の場合、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。 **CAUTION: 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、リポジトリのストレージ場所にあるすべてのファイルも削除されます。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。** 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。
ユーザー名	管理アクセスのあるユーザーのユーザー名を入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
パスワード	管理アクセスのあるユーザーのパスワードを入力します。この情報は、指定されたリポジトリの場所がネットワークパスである場合にのみ必要です。
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。

17. **リポジトリ設定** ページで、リポジトリに割り当てるディスクでの容量を設定します。Quest では、メタデータにボリュームの 20 パーセントを予約することをお勧めします (この値はデフォルトです)。必要に応じて、スライダコントロールまたは **サイズ** フィールドを使用して、リポジトリのボリュームで割り当てる領域を増減できます。
18. 必要に応じて、ストレージ場所の設定に関する詳細情報を表示および入力する場合は、**詳細設定オプションを表示** を選択し、次の表の説明に従って、設定を調整します。これらのオプションを非表示にするには、**詳細設定オプションを表示** オプションをクリアします。リポジトリ設定を完了したら、必要に応じて、**次へ** または **終了** をクリックします。

表 74. ストレージ設定の詳細

テキストボックス	説明
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。
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。 **NOTE:** 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 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 がキャッシュを制御します。 「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。

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。

19. 必要に応じて、リポジトリに保存されているデータに暗号化キーを使用する場合、**暗号化** ページで、**リポジトリ内の保存データを暗号化する** を選択してから、次のいずれかを実行します。
    - 既存の暗号化キーを選択して、リポジトリに保存されているすべての新しいデータに適用するには、**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、**暗号化キーの選択** ドロップダウンメニューから暗号化キーを選択します。
    - 現時点の新しい暗号化キー定義して、リポジトリに保存されている以降すべてのデータに適用するには、次の表に説明されているとおりに、**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** を選択してから、キーに関する情報を入力します。

表 75. 新しい暗号化キーを定義

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。
Passphrase（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。

テキストボックス	説明
	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。Quest Data Protection 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。

20. 必要に応じて、**暗号化** ページで、ネットワーク経由で転送されるすべてのデータを暗号化するには、**ネットワーク経由の転送データを暗号化する** を選択します。このオプションはデフォルトで有効になっているため、この方法でデータを暗号化しない場合は、このオプションをクリアします。
21. **終了** をクリックし、設定を保存して適用します。

    マシンに対してはじめて保護が追加されると、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。

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。

1. 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。

   NOTE: 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、「ログ記録されたすべてのイベントのジャーナルを表示」を参照してください。

アプリケーションサポートの有効化

VM がエージェントレス保護下に置かれると、そのマシンにインストールされている Exchange または SQL アプリケーションをサポートできます。

開始する前に、次の前提条件を満たしている必要があります。

- **Rapid Recovery Core で VM を保護する**。アプリケーションサポートを有効にするオプションは、保護プロセス中は使用できません。この機能を有効にするボタンは、SQL または Exchange マシンが保護下に置かれると、UI の複数のページに表示されます。詳細については、「エージェントレスの保護を使用した

vCenter/ESXi 仮想マシンの保護」または「エージェントレス保護を使用した Hyper-V 仮想マシンの保護」を参照してください。

- **リモート WMI アクセスを有効にする。**WMI アクセスを許可するには、ターゲット仮想マシン（VM）に Windows リモート管理をインストールして構成する必要があります。詳細については、https://msdn.microsoft.com/en-us/library/aa384372(v=vs.85).aspx のマイクロソフトサポート技術情報記事を参照してください。
- **ローカルユーザーにリモートで管理者権限を付与する。**次の管理コマンドプロンプトを実行して、LocalAccountTokenFilterPolicy を構成します。

  ```
  winrm quickconfig
  ```

- **WMI ルート名前空間アクセス許可を取得する。**Core がエージェントを使用せずにアプリケーションに接続するには、VM で TCP ポート 135 と 445、および動的に割り当てられるポート 1024 ～ 1034 に対する着信ネットワークトラフィックを許可する必要があります。
- **SQL Server および Exchange へのリモートアクセスを許可する。**この前提条件は、サポートするアプリケーションによって異なります。
  - **SQL：**ポート 1433 および 1434 を開き、Windows ファイアウォールを構成します。
  - **Exchange：**TCP および UDP 389 ポートを開きます。
- **ホストとゲストを統合する。**統合は、ハイパーバイザに固有の最適化パッケージをインストールすることによって行われます。
  - ESXi VM の場合、エージェントレス ESXi VM 保護に必要な **VMware ツール**を使用します。
  - Hyper-V の場合、ほとんどの Windows Server オペレーティングシステムにプリインストールされている **統合サービス**バンドルを使用します。

エージェントレスで保護されている VM のアプリケーションサポートを有効にするには、次の手順を実行します。

1. Core Console から、**マシン** ページに移動します。
2. 次のいずれかのアクションを実行します。
   - 単一の VM のアプリケーションサポートを有効にするには、その VM の**アクション** メニューをクリックし、**アプリケーションサポートの有効化** をクリックします。
   - 同時に複数の VM のアプリケーションサポートを有効にするには、複数の VM を選択し、**アプリケーションサポート** ドロップダウンをクリックして、**アプリケーションサポートの有効化** をクリックします。
3. **アプリケーションサポートの編集** ダイアログボックスで、VM の認証情報を入力します。

アプリケーションサポートが有効になっている保護対象マシンの名前の横には、緑のアイコンが表示されます。

アプリケーションの認証情報を追加する場合は、特定のマシンの **サマリ** ページの上部にある **SQL** または **Exchange** をクリックします。

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、「夜間ジョブについて」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. **サマリ** ページの一番上にあるリンクで、Exchange メニューの右側の下向き矢印 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。

NOTE: マウント可否チェックは、Microsoft Exchange Server 2007、2010、2013、および 2016 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側にある ▸ 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. 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 **リカバリポイントの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、およびジャーナルページ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** ペインまで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側にある ▸ 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. 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 リカバリポイントに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、およびジャーナルページ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、「夜間ジョブについて」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. **サマリ** ページの一番上にあるリンクで、SQL メニューの右側の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。

     1. **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。
     2. **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。
     3. 「**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。

     1. 資格情報のタイプ（デフォルト、Windows、または SQL）を選択します
     2. **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。
     3. **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。
     4. 「**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。

NOTE: 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。

1. 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。

2. **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。
3. 「**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。

NOTE: 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。

NOTE: 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、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側にある ▸ 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. 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 **リカバリポイントの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、およびジャーナルページ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 Rapid Recovery Core Console から管理できます。これには次のようなタスクが含まれます。

- 「」に記載されているオプションを使用して、Rapid Recovery Core Console 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。
- 特定のマシンの設定を構成して、Core のデフォルト設定と置き換えることができます。設定タスクには、ハイパーバイザホストや VM 設定の変更、システム情報へのアクセス、転送設定の変更、夜間ジョブのカスタマイズ、イベントの通知の設定などがあります。詳細については、「マシン設定の構成」を参照してください。
- マシンまたはクラスタを保護対象から除外することや、保護対象マシンに対するライセンス情報を表示すること、また保護対象マシンのログファイルを確認して問題を診断することができます。これらをはじめとするタスクの詳細については、「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。

NOTE: 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。このページでは、各マシンのサマリ情報を確認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、「」を参照してください。

マシン設定の構成

Rapid Recovery Core でマシンを保護すると、その保護対象マシンの動作を制御する設定を簡単に表示および変更できるようになります。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。

Rapid Recovery Core Console では、次のマシン設定を表示および構成できます。

- **一般**。一般的なマシンの構成設定には、表示名、ホスト名、ポート、暗号化キー、リポジトリ、およびハイパーバイザホストへのリンクなどが含まれます。マシンの一般設定の構成については、「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。
- **夜間ジョブ**。特定の保護対象マシン用に表示される夜間ジョブ Core 設定のサブセットは、Core レベルの夜間ジョブ設定のセットよりも優先させることができます。これには、保持ポリシーを管理するロールアップが含まれます。保護対象マシンのタイプに応じて一部の設定が異なる場合があります。
- **転送設定**。選択した保護対象マシンのデータ転送プロセスを管理するための設定です。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。
- **除外されるライター**。これらの設定を使用して、ライターを除外することができます。これらはマシン固有の設定です。ライターは、その他のソフトウェアコンポーネントが Microsoft Volume Shadow Services (VSS) を使用できるようにするため、Microsoft によって公開されている特別な API です。ボリュームのスナップショットに参加している Rapid Recovery の各ライターは、除外されるライター 設定にリストされます。ライターが干渉したり、成功したバックアップ転送から除外されたりするイベントが発生した場合は、それらを 1 つずつ無効にすることができます。Quest サポートの担当者から指示されないかぎり、Quest Data Protection サポート ではこれらの設定をそのままにしておくことをお勧めします。
- **ライセンスの詳細**。特定の保護対象マシンのライセンスに関する詳細です。これらの設定により、Core と Rapid Recovery ライセンスポータル ライセンスポータルからの情報がレポートされます。これらは、読み取り専用の設定です。これらの設定を変更するには、Core とライセンスポータル間のライセンス情報をアップデートします。ライセンス管理者の詳細を参照してください。詳細については、「*Rapid Recovery ##########*」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、除外されるライター、ライセンスの詳細 で同じです。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。

ただし、マシンの夜間ジョブを変更する手順については異なります。マシンの夜間ジョブ設定の構成については、「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したいことがあります。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。

同様に、保護対象の Hyper-V 仮想ホストは、管理している仮想マシンとは異なるマシン設定がされています。詳細については、「ホストのサマリ情報の表示」を参照してください。

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。

NOTE: 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。

1. Rapid Recovery Core Console の 保護対象マシン メニューで、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 ページが表示され、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、その設定が編集可能なコントロールになります。次のいずれかを実行します。

   - コントロールがドロップダウンメニューである場合、下向き矢印をクリックしてオプションを表示し、メニューから目的のオプションを選択します。
   - コントロールがテキストフィールドである場合は、値を入力します。
   - オプションに **はい** または **いいえ** が表示されたときは、値をクリックすると、チェックボックスに置き換えられます。はい の設定には、チェックボックスを選択します。いいえ の値には、チェックボックスをクリアします。
   - オプションに日時の値 (たとえば、時、分、秒を表示している場合) 、それぞれのコンポーネントをクリックして、新しい値を入力するか上下の矢印を使用して新しい値を選択します。

   各設定の変更が完了したら、✔ をクリックして変更内容を確認して保存し、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。
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 76. 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」は適用できません。
ホスト名	これは、マシンのメタデータ内にある保護対象マシンの名前です。 **NOTE:** この設定は変更しないでください。変更すると、保護対象マシンと Core 間の接続が切断される可能性があります。
リポジトリ	この設定は、共有仮想ハードディスクをサポートする、保護対象 Hyper-V クラスタにのみ表示されます。保護対象 Hyper-V クラスタの共有仮想ハードディスクのリカバリポ

テキストボックス	説明
	イントが保存されている Rapid Recovery Core に設定されているリポジトリを表示します。
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。デフォルトのポートは8006です。
暗号化キー	この Rapid Recovery Core にすで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。 **NOTE:** 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、次回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。 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。 **NOTE:** 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。
ハイパーバイザ	この設定は、仮想マシンにのみ表示されます。この設定の値は、選択した仮想マシンが保護対象ハイパーバイザホストの子として関連付けられているかどうかを示します。 • 保護対象ホストの IP アドレスまたは表示名が表示されている場合、関連付けが存在します。この結果は、保護対象マシンが、利用可能なライセンスプールから不必要にライセンスを消費していないことを示しています。 • 関連付けを削除する場合は、ハイパーバイザホストの IP アドレスまたは表示名をクリックして、ドロップダウンメニューから **リンクされていません** を選択し、チェックマークをクリックして、変更を確認します。その後は、この保護対象 VM がプールからライセンスを消費します。 • リンクされていません と表示されている場合、そのマシンは現在、保護対象ホストで VM として Core と関連付けられておらず、プールからライセンスを消費しています。ライセンスを節約したい場合にホストが Agent に保護されているときは、**リンクされていません** をクリックしてホストを関連付け、ドロップダウンメニューからホストを選択します。

テキストボックス	説明
OS バージョン	この設定は、保護対象ハイパーバイザホストに関連付けられているゲスト仮想マシンにのみ表示されます。通常、Rapid Recovery は、保護対象 VM で実行されているオペレーティングシステムを検出して表示します。

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。

   NOTE: 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 77. 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 ー 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。 **NOTE:** 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。 **NOTE:** Questでは、この値を 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。 **NOTE:** Quest では、「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が使用されます。

テキストボックス	説明
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。 Quest 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。
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。
スナップショットデータの暗号化	保護対象マシンと Core の間で転送されるデータが暗号化されるかどうかを指定します。このオプションはデフォルトで有効になっています。この設定は、ネットワーク経由で送信中のデータに適用されます。このオプションが有効なとき、DVM リポジトリに転送されるすべてのスナップショットデータが暗号化されます。 **NOTE:** Quest は、Core と保護対象マシンの間のデータをパブリックネットワークまたはインターネットなどの信頼されていないネットワーク経由で送信する必要がある場合、このオプションを はい に設定することをお勧めします。

7. 除外されているライターの設定を変更するには、適切な設定をクリックし、ライターを除外する場合は、対象のライターを選択します。

   NOTE: リストに表示されるライターは、マシン固有であるため、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。

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 78. 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	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—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。

See also: Hyper-V ホストまたはノードの設定変更
See also: Hyper-V の保護対象仮想マシンの設定変更
See also: VMware 保護対象仮想マシンの vSphere 設定の変更

Hyper-V ホストまたはノードの設定変更

この手順は、Rapid Recovery Rapid Snap for Virtual (エージェントレス保護) を使用して仮想マシン (VM) を保護する Hyper-V ホストまたはノードに適用されます。

VM の保護に Rapid Snap for Virtual (エージェントレス保護) を使用している Hyper-V ホストは、左のナビゲーションエリアにホストアイコンで表示されます。VM をエージェントレスで保護している 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たすべての変更は、そのホスト上の VM に適用されます。

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. **一般** 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。
4. 次の表の説明に従って、設定情報を入力します。

表 79. 一般 の設定情報

テキストボックス	説明
表示名	Rapid Recovery Core Console での保護対象マシンの表示名です。64 文字まで入力できます。デフォルトでは、マシンのホスト名になります。必要に応じて、わかりやすい表示名に変更できます。「使用禁止文字」または「禁止語」は適用できません。
ホスト名	マシンのメタデータ内で確認できる保護対象マシンの名前です。 **NOTE:** この設定は変更しないでください。変更すると、保護対象マシンと Core 間の接続が切断される可能性があります。

5. ホストで一度に実行する転送ジョブの数を変更するには、**転送キュー** で **最大同時転送数** の設定をクリックします。

NOTE: 最適なパフォーマンスを得るには、Hyper-V ホストまたはノードの最大同時転送数はデフォルトの 1 に設定することをお勧めします。

6. 使用可能な夜間ジョブの設定を変更するには、**夜間ジョブ** で **変更** をクリックします。

   夜間ジョブ ウィンドウが表示されます。

7. 次の表の説明に従って、設定情報を入力します。

表 80. 夜間ジョブ の設定情報

テキストボックス	説明
保護対象の Hyper-V の孤立したレジストリキーを削除します。	データ転送中に仮想ディスクの接続と切断の結果としてできた不要なファイルをレジストリから削除します。
リカバリポイントの整合性チェック	Hyper-V ホスト上の仮想マシン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. Hyper-V ホストに新しい仮想マシンが追加されたときに自動的にそのホストを保護するかどうかを決定するには、**自動保護** で **新しい仮想マシンを自動保護する** 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 81. 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	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

テキストボックス	説明
失敗した場合は、チェックポイントを作成します	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 Snap for Virtual によって保護（エージェントレス保護）される VMware ESXi 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 82. vSphere の設定情報

テキストボックス	説明
Vmware で作成したユーザーの 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、保護対象マシンに対するデータ転送プロセスを管理するための設定を変更できます。本項で説明されている転送設定は、保護対象マシンレベルの設定です。Core で転送を反映する方法については、「転送キュー設定の変更」を参照してください。

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。すべての保護対象データのベースイメージと、最後のスナップショット以降にアップデートされたデータの増分スナップショットの 2 つのタイプのスナップショットを使用できます。このタイプの転送では、Core に関連付けられたリポジトリに保存されるリカバリポイントが作成されます。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。
- **仮想マシンのエクスポート**。保護対象マシンのバックアップのすべてのデータ、オペレーティングシステム、ドライバ、および関連データが含まれるリカバリポイントから仮想マシン (VM) を作成し、仮想マシンが起動可能であることを確認します。詳細については、「VM のエクスポート」を参照してください。
- **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、「データリカバリポイントからのボリュームのリストア」を参照してください。

> **NOTE:** Windows システムのリストア時には、常に EFI システムパーティションを使用してボリューム全体が書き直されます。

Rapid Recovery でデータを転送する場合は、ネットワーク経由で保護対象マシンから Core にデータボリュームが転送されます。レプリケーションの場合、ソース Core からターゲット Core への転送も発生します。

データ転送は、特定のパフォーマンスオプションの設定でシステムに合わせて最適化できます。これらの設定では、保護対象マシンのバックアップ、VM のエクスポート、リストアを実行するプロセス中に使用するデータ帯域幅を制御します。次に、データ転送のパフォーマンスに影響する要素を示します。

- Agent データの同時転送数
- 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
- リポジトリの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で使用できるメモリ容量

ビジネスニーズに合わせてパフォーマンスオプションを調整し、環境に基づいてパフォーマンスを微調整できます。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。

> **CAUTION: 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（1 GbE または 10 GbE など）、アーキテクチャ、設定、意図的な NIC チーミングの使用や、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。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。

Machine-Level 設定	デフォルト設定	推奨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
1 ストリームあたりの未処理の読み取り	0	24から開始

Quest のサポート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 レベルまたは保護対象マシンレベルで設定できます。夜間ジョブを Core レベルで設定すると、変更内容はその Core の保護対象であるすべての該当マシンに適用されます。マシンレベルで行われた夜間ジョブへの変更は、Core レベルで行われた変更より優先され、指定したマシンにのみ適用されます。

すべての夜間ジョブの完全なリスト（各ジョブの説明と使用可能なスコープを含む）については、夜間ジョブについてを参照してください。

1 台の保護対象マシンの夜間ジョブに変更を行うには、次の手順を実行します。

1. Rapid Recovery Core Console の 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 **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. 必要に応じて、**設定** ページで **夜間ジョブ** リンクをクリックし、スクロールダウンして、夜間ジョブの設定を表示します。
4. 夜間ジョブ の見出しの下で、  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. **夜間ジョブ** ダイアログボックスで、夜間の実行に含めるジョブを選択するか、そのマシンで省略するオプションをオフにします。

   NOTE: オプションはマシンによって異なります。たとえば、Exchange Server を使用している保護対象マシンには、「Exchange データベースのチェックサムチェック」および「Exchange ログを切り捨て」が表示されます。

   NOTE: カスタム保持ポリシーの設定など、**ロールアップ**設定の詳細については、「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。
6. **OK** をクリックします。

   NOTE: この手順の結果は、選択した保護対象マシンにのみ適用されます。カスタマイズするすべてのマシンに適用するには、カスタマイズする各マシンでこの手順を繰り返します。Core によって保護されているすべてのマシン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。

特定の保護対象マシンのシステム情報を表示すると、Core およびリポジトリとの関係を含む、保護対象マシンに関する一般的な情報が **システム情報** ペイン表示されます。**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、物理メモリ、表示名、完全修飾ドメイン名、および仮想マシンタイプ（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、使用済み容量などが含まれます。
   - **プロセッサ**。アーキテクチャ、Core とスレッドの数、クロック速度、および説明が含まれます。
   - **ネットワークアダプタ**。ネットワークアダプタのタイプと速度が含まれます。
   - **IP アドレス**。IP アドレスとファミリが含まれます。

マシンの管理

本項では、マシンを管理する保護対象マシンの管理の際に実行できるさまざまなタスクについて説明します。

- 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 Core 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選択する 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。マシンが保護下にあったときにマシンから取得されたリカバリポイントから、引き続きリストアおよびマウント操作を実行できます。ただし、保護対象マシンのバックアップは継続されません。

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、保護されていたマシンのスナップショットデータが Rapid Recovery Core からすべて削除されます。

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。

   CAUTION: 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 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 の下で、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。

   CAUTION: リカバリポイントを削除すると、そのクラスタのデータをリストアできなくなります。

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 の下で、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。

   CAUTION: リカバリポイントを削除すると、クラスタノードのデータをリストアできなくなります。
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。

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。

CAUTION: 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 の下で、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 83. 「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。 **CAUTION: リカバリポイントを削除すると、そのクラスタのデータをリストアできなくなります。**

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、Quest サポートの担当者とマシン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。**その他** 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。

See also: Core ログファイルのダウンロードと表示
See also: 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

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クラスタが示さ

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。

See also: カスタムグループの作成
See also: カスタムグループ名の変更
See also: カスタムグループの削除
See also: グループアクションの実行
See also: 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。

   NOTE: 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。

4. **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。

   NOTE: 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。

5. 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。

6. 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。

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、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。
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、「**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。
4. 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。

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、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。
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、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。
   - 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、再開パラメーターを指定します。
   - 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。
   - 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。
   - 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。
   - 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。
   - 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。
   - 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。
   - （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。

See also: スナップショット作成の強制実行
See also: レプリケーションの強制実行
See also: レプリケーションの一時停止と再開
See also: 保護の一時停止と再開
See also: 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

See also: カスタムグループ名の変更
See also: カスタムグループの削除

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。

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。

NOTE: 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 84. 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。
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。
リポジトリのステータス	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 85. 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。
Encrypted（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。 • Exchange サーバの場合は、をクリックしてサーバに関する情報を表示します。
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。
•••	[その他] 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。

関連資料

See also: 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。

NOTE: 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 86. 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	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	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	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	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 87. 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	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	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	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	アタッチ可否チェックに合格したことを示します。

NOTE: 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、Windows マシンのリカバリポイントをマウントして、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できます。

NOTE: `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。

NOTE: 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 88. 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。

NOTE: 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、およびジャーナルページ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。

NOTE: 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、 (その他) をクリックして、**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。

   NOTE: 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。

NOTE: 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。

NOTE: 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
- 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。

NOTE: 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。

   ```
   lm
   ```
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。

   ```
   lr <line_number_of_machine>
   ```

   NOTE: 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。

NOTE: 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) 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：m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>)。たとえば、`lm` 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 `lr` 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、コマンドは次のようになります。

```
m 2 23 b /tmp/mount_dir
```

NOTE: 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 (『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)、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。

```
l
```

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。たとえば、次のように入力します。

```
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 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 Core 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>
   ```

   NOTE: 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. `l ### 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、`l ### 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。

   ```
   unmount <path_of_nbd-device>
   ```
8. `l ### 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。

NOTE: 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、Windows Server 2012 R2 および Windows Server 2016 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。

NOTE: 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。

   CAUTION: 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。

   CAUTION: 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。

CAUTION: 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、レプリケーションが使用された場合、Quest では移行を開始する前にターゲット Core 内の各リポジトリで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 リポジトリでの整合性チェックの実行」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。

   NOTE: 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 レ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。

NOTE: 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。

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 のレプリケーションの理解と設定に役立つ概念と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 は指定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、マウント可否チェック、アタッチ可否チェック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。あらゆるタイプのログの切り捨ても、リカバリポイントまたは Oracle データベース.の整合性チェックと同様に、レプリケーションジョブをトリガします。夜間ジョブにこれらのいずれかの操作が含まれている場合、夜間ジョブが完了すると、レプリケーションジョブもトリガされます。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。

NOTE: クラスタデータをレプリケートする場合、クラスタ全体をレプリケートする必要があります。たとえば、レプリケートするノードを選択した場合、そのクラスタが自動的に選択されます。同様に、クラスタを選択した場合は、そのクラスタ内のすべてのノードが選択されます。

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

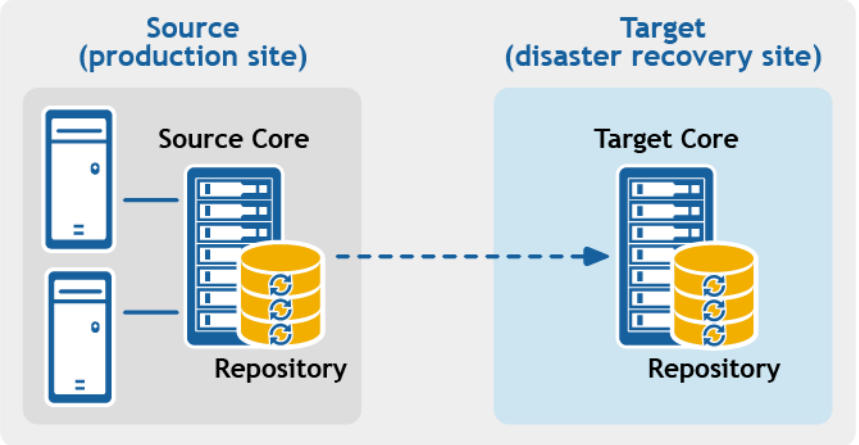
Core で、MSP パートナーにより、1 つ、または複数の顧客が、リカバリポイントを顧客のサイトにあるソース Core から MSP のターゲット Core に有料でレプリケートすることができます。

NOTE: 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。

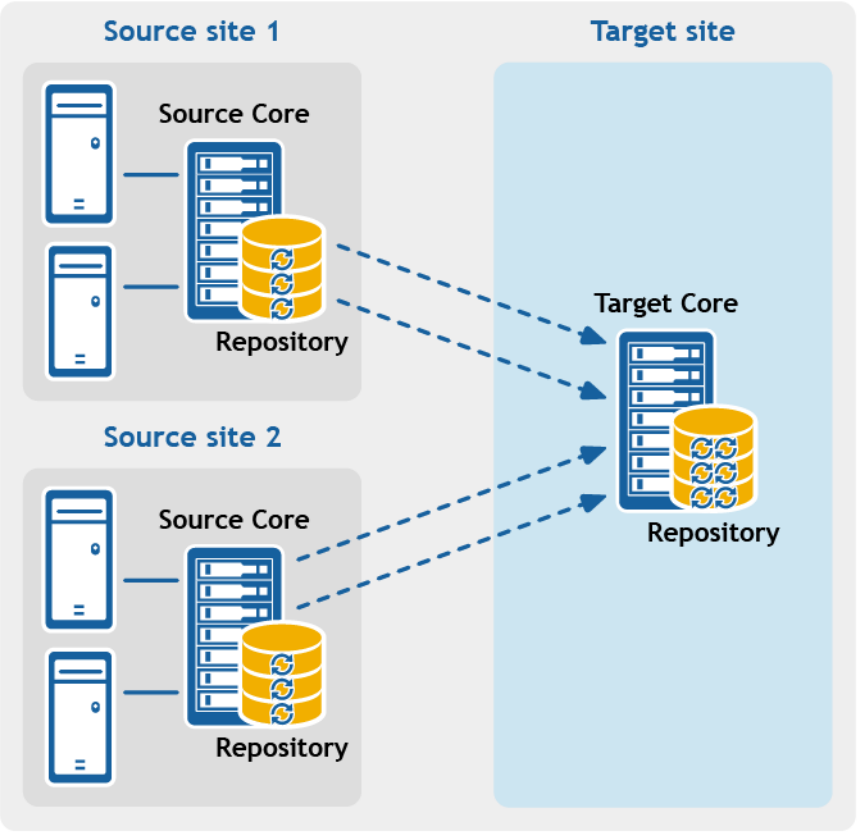
- **Point-to-Point レプリケーション。**1 つ、または複数の保護対象マシンを 1 つのソース Core から 1 つのターゲット Core にレプリケートします。

図 1. Point-to-Point レプリケーションの設定



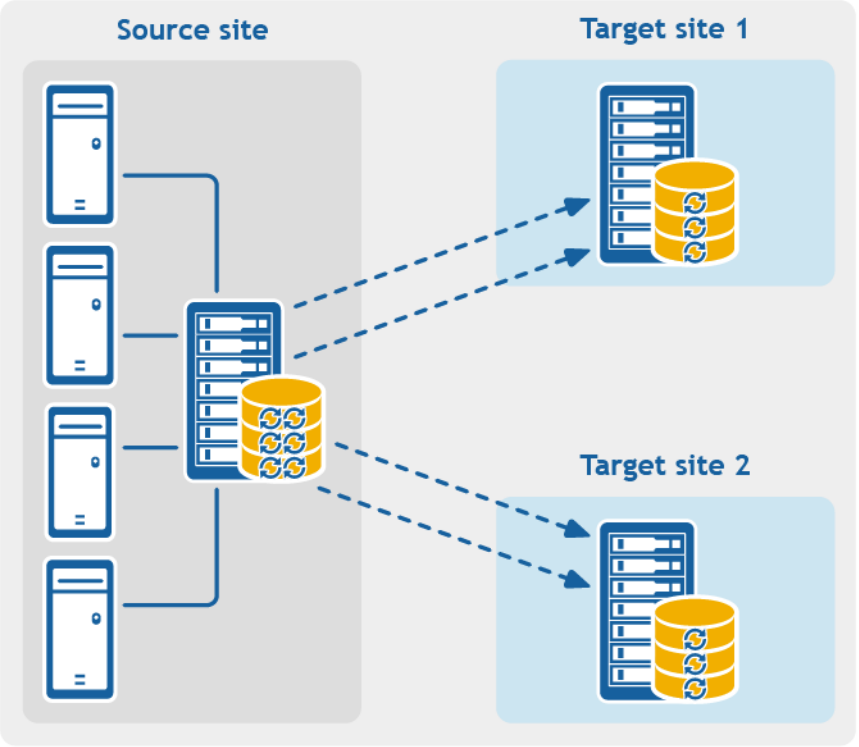
- **Multipoint-to-Point レプリケーション。**複数のソース Core から 1 つのターゲット Core に保護対象マシンをレプリケートします。

図 2. Multipoint-to-Point レプリケーションの設定



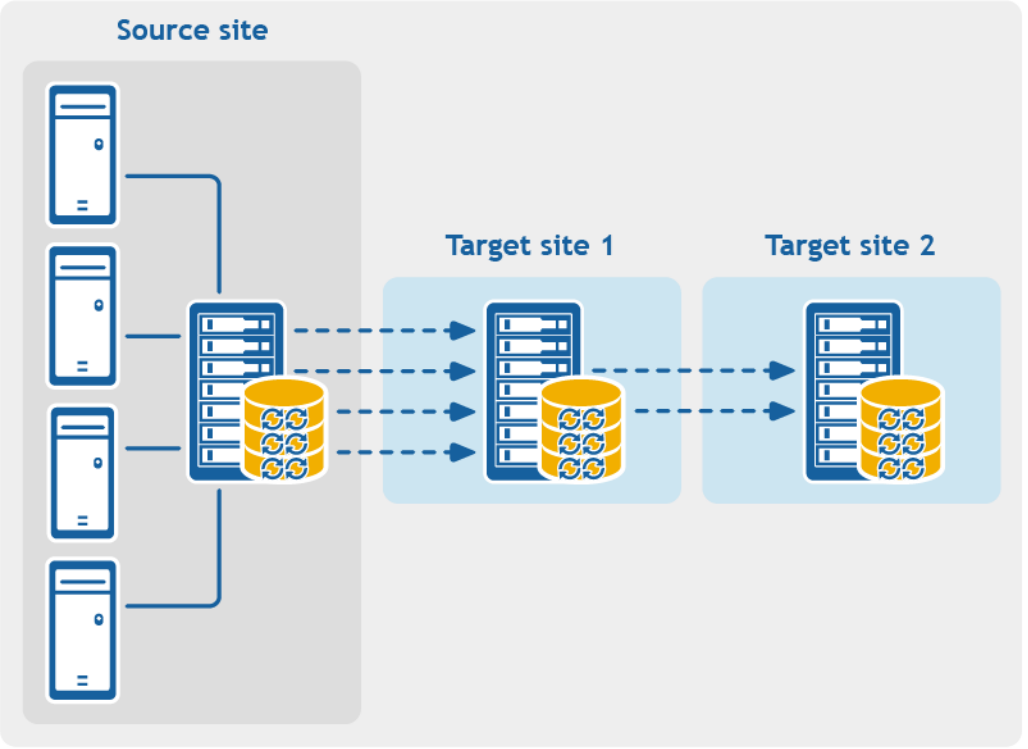
- **Point-to-Multipoint レプリケーション。**1 つ、または複数の保護対象マシンを 1 つのソース Core から複数のターゲット Core にレプリケートします。

図 3. 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 4. マルチホップレプリケーションの設定



DL シリーズのバックアップアプライアンスを使用している場合は、レプリケート先のターゲット 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.quest.com/contact-us/licensing）にアクセスするか、license@quest.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られます。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回のバックアップスナップショットから開始されます。

NOTE: 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。

  NOTE: このような場合、Quest 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する方法を決定します。

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。

   NOTE: Quest 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。

NOTE: 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。

NOTE: 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が、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ーファン化したままで、レプリケートされたベースイメージと組み合わされます。

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。
- オーファ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。

See also: ターゲット Core 上のシードドライブの消費
See also: 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。

  NOTE: 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 89. 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

NOTE: 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スフレーズが必要です。

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。

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 **レプリケート** 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、この Rapid Recovery Core からの出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 90. 出力方向のレプリケーションに関する情報

UI エレメント	説明
項目選択	サマリ表の各列でチェックボックスを選択して、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かを示します。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 その他 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 91. 出力方向のレプリケーション ペインで使用できるグローバルアクション

UI エレメント	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(R)	テーブル内の表示されている情報を更新します。
強制	レプリケーションを強制実行します。
一時停止	確立されたレプリケーションを一時停止します。
再開	一時停止したレプリケーションを再開します。
コピー	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。
削除(D)	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。
	この行で その他 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 92. 入力方向のレプリケーションに関する情報

UI エレメント	説明
項目選択	サマリ表の各列でチェックボックスを選択して、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かを示します。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。

UI エレメント	説明
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 その他 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 93. 入力方向のレプリケーション ペインで使用できるグローバルアクション

UI エレメント	説明
更新(R)	テーブル内の表示されている情報を更新します。
強制	レプリケーションを強制実行します。
一時停止	確立されたレプリケーションを一時停止します。
再開	一時停止したレプリケーションを再開します。
削除(D)	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、レプリケーションのためのソース Core とターゲット Core を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、およびリカバリを実行することができます。

NOTE: クラスタデータをレプリケートする場合、クラスタ全体をレプリケートする必要があります。たとえば、レプリケートするノードを選択した場合、そのクラスタが自動的に選択されます。同様に、クラスタを選択した場合は、そのクラスタ内のすべてのノードが選択されます。

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 Core のリポジトリの設定。ターゲット Core にリポジトリを追加する方法の詳細については、「DVM レポジトリの作成」を参照してください。
- 自己管理レプリケーションの設定。自己管理ターゲット Core へのレプリケートの詳細については、「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。
- サードパーティレプリケーションの設定。サードパーティのターゲット Core へのレプリケートの詳細については、「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のレプリケート。ソース Core によってすでに保護されているマシンのレプリケートの詳細については、「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。
- シードドライブの消費。ターゲット Core での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。
- 保護対象マシンのレプリケーション優先度の設定。保護対象マシンのレプリケーション優先度の設定の詳細については、「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の設定。レプリケーションスケジュール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。
- 必要に応じたレプリケーションのモニタ。レプリケーションのモニタリングの詳細については、「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。
- 必要に応じたレプリケーション設定の管理。レプリケーション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が発生した場合のレプリケートされたデータのリカバリ。レプリケートされた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。

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、オフサイト場所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。次の手順が前提条件となります。

- Rapid Recovery Core が、すべてのソースマシンおよびターゲット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、このタスクを、すべてのソース Core および 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。
- 既存のリカバリポイントの最初の転送を実行するために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準備しておく必要があります。また、ドライブを接続してシードドライブアーカイブをコピーするために、ソース Core マシンに物理的にアクセスできることも必要です。
- 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は、ユーザーまたは信頼された管理者がターゲット Core に物理的にアクセスできることが必要です。

自己管理ターゲット Core とは、ユーザーがアクセスできる Core です。たとえば、自己管理コアは、多くの場合、オフサイトの場所にある部署で管理されるか、ソース Core とは異なる地理的場所でホストされています。シードドライブを使用してデータをシーディングする場合を除き、レプリケーション全体をソース Core 上で設定することができます。このような場合は、以下の手順を使用し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 に接続して、アーカイブされたリカバリポイントデータを取り込む必要があります。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。

自己管理ターゲット Core にレプリケートするようにソース Core を設定するには、次の手順を実行します。

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。

   レプリケーションウィザード が表示されます。
3. このソース Core とペアリングされたことのあるターゲット Core のレプリケーションを確立する場合は、レプリケーションウィザード の **ターゲットコア** ページで **既存のターゲット Core を使用する** を選択し、適切なターゲット Core をドロップダウンリストから選択します。手順 5 に進みます。
4. このソース Core からターゲット Core によるレプリケーションを初めて確立する場合は、レプリケーションウィザードの **ターゲット Core** ページで**ターゲット Core を所有しています** を選択し、次の表の説明に従って情報を入力します。

表 94. ターゲット Core 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 Core 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(O)	Rapid Recovery Core 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(A)	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(A)	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。

   NOTE: ターゲット Core にリポジトリが存在しない場合は、ソース Core とターゲット Core をペアリングできますが、リポジトリが確立されるまで、この場所に Agent (保護対象マシン) をレプリケートできないことを通知する警告が表示されます。Core に対するプライマリリポジトリの設定方法については、「 DVM レポジトリの作成」を参照してください。
6. **リクエスト** ページで、SourceCore1 など、このレプリケーション設定の名前を入力します。これは、ターゲット Core の 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 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. **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。
9. 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。データをシードしない場合は、次の手順に進みます。

   NOTE: 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、Quest ではポータブルストレージデバイスへの 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、これらの保護対象マシンをシードドライブに含めることができます。
   - この手順を完了した後即座にレプリケーションを開始しない場合は、**最初にレプリケーションを一時停止** を選択します。

     NOTE: このオプションを選択した場合、明示的に再開するまでレプリケーションが開始されません。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。

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. 場所 フィールドで、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 95. 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。これを使用して、`D:\work\archive` など、シードドライブアーカイブを格納する場所のパスが定義されます。
ネットワーク	出力先	出力の場所を入力します。これを使用して、`\\servername\sharename` など、シードドライブアーカイブを格納する場所のパスが定義されます。
	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(A)	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。 **NOTE:** 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 96. 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セグメントの最大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で指定したパスの使用可能なすべての領域を、今後使用するために確保します。たとえば、場所が `D:\work\archive` の場合、シードドライブをコピーするために必要であれば、D: ドライ

アイテム	説明
	ブ上の使用可能な領域のすべてが確保されますが、コピープロセスを開始した直後には確保されていません。 • 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。デフォルトは 250MB です。
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。これにより、すでに複製された一部のリカバリポイントがシードドライブに追加され、オーファンの発生を防止します。このオプションは、デフォルトで選択されています。 **NOTE:** 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ていました。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** を選択した場合は、手順 10 に進みます。

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、そのシードドライブをターゲット Core に送信します。

ソース Core とターゲット Core 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というオプションを選択していない限り、レプリケーションプロセスがただちに開始されます。

1. シードドライブを使用するという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、レプリケーションによって、孤立したリカバリポイントがターゲット Core に作成されます。
2. ドライブの使用を指定した場合は、シードドライブアーカイブファイルをボリューム（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）に転送します。そして、シードドライブを消費します。

See also: クラウドアカウントの追加
See also: DVM レポジトリの作成

See also: Rapid Recovery でのレプリケーション
See also: シーディングの要件と戦略の決定
See also: レプリケーション

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の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。

NOTE: 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 をサブスクライブしている 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 97. 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(O)	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。

- 追加する必要のある 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 98. 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
E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。

NOTE: 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 99. 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。これを使用して、`D:\work\archive` など、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。
	ユーザー名(A)	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。

オプション	テキストボックス	説明
	パスワード(A)	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。 **NOTE:** 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 100. 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。

アイテム	説明
	NOTE: 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ていました。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。

   保留中のレプリケーションリクエスト 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。

   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。

NOTE: 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。

   保留中のレプリケーションリクエスト 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。

   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。

   保留中のレプリケーションリクエスト 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。

   NOTE: 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** 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 101. 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。

オプション	テキストボックス	説明
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(A)	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(A)	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。 **NOTE:** 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. 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 102. 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。

アイテム	説明
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。 **NOTE:** 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。

NOTE: 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 103. 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 (A)	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 (A)	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。 **NOTE:** 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。

CAUTION: 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。

NOTE: 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、矢印 をクリックして折り畳んだ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. 破棄するシードドライブファイルに対して、（その他のオプション）をクリックして、**破棄** をクリックします。
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、全体レベル、Core レベル、または保護対象マシンレベルで、レプリケーションを監視、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、を参照してください。 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。
- 保護対象マシンの入力方向または出力方向の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、「出力方向の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。

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 ペインのレプリケーションのスケジュールを実行する Core で、 (その他のオプション) をクリックし、**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。

        NOTE: 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 104. 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。
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 (A)	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 (A)	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。 **NOTE:** 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 105. 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。 **NOTE:** 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 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 106. 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。 **NOTE:** 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。
出力方向のレプリケーション	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 …（その他）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、カスタマ 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

項	説明	利用可能なアクション
		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。
入力方向のレプリケーション	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 ... （その他）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。
レプリケーションリクエストを保留しています	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。

1. 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。
   a. 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。
   b. 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。
3. 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。
   a. 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、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。
   b. 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。
   c. 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。
4. 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。
   a. 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。
   b. 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。
5. 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。
   a. 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、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。
   b. 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、オーファ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、**オーファ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。

出力方向の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 107. 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。
デフォルトにリストア	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。 **NOTE:** 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。

   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 108. ターゲット Core の設定

オプション	説明
Host	ターゲット Core のホストを入力します。
ポート(O)	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。 **NOTE:** 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 ー 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 ー 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 ー 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れられます。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マシンとしてキューに入れられます。

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、任意のソース 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、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. 優先度を設定する保護対象マシンの ••• （その他）ドロップダウンメニューをクリックし、**設定を変更** 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。

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 ▶ 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 と任意のターゲット 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、任意のターゲット Core の ••• （その他）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。

NOTE: 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、 （その他）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。

   WARNING: 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、「データリカバリポイントからのボリュームのリストア」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」を参照してください。
- **ベアメタル復元 (BMR) を実行する**。詳細については、「Windows マシンでのベアメタル復元の実行」を参照してください。

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 の重大な不具合について、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について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。

タスク、アラート、およびジャーナル ページ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、その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 または特定のマシン上の）イベント ページには、タスク、アラート、および ジャーナル の 3 つのビューがあります。いずれかのカテゴリに表示されたアイテムは、すべてイベントです。これらのビューによって、さまざまなイベントのサブセットについての詳細を適宜フィルタリングできます。デフォルトのビューでは、タスクを表示します。

- **タスク**は、ジョブに関連付けられたイベントです。**ジョブ**は、Rapid Recovery Core が実行する必要がある 1 つの処理です。各ジョブには、現在の状態、およびタスクの開始日時と終了日時があります。一部のタスクは、手動で開始されるか、ユーザーによってスケジュール設定されます。例には、スナップショットの強制、バックアップのスケジュール設定、またはリカバリポイントからのリストアの実行などがあります。その他のタスクは、夜間ジョブの実行や、デフォルトの保持ポリシーを使用したロールアップの実行などの自動機能のタスクです。
- **アラート**は、エラー、警告、または重要な情報メッセージなどの優先順位が付けられたイベントです。特定のイベントの通知をすべて要求した場合、これらの通知は、アラート のサブセットに表示されます。
- **ジャーナル**では、記録されたすべてのイベントの完全なリストを表示します（Core または選択したマシンにイベントがある場合）。このリストは、より包括的なものであり、ジョブ、優先度が高いイベント、および優先度が低いイベントを表示します。このカテゴリには、パッシブな、ジョブによらないイベント（Core の正常起動、またはライセンスポータルからのステータスレポートなど）が含まれます。

タスク、アラート、または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
- ログ記録されたすべてのイベントのジャーナルを表示
- 任意の Core コンソールページからの実行中タスクの表示
- タスク、アラート、およびイベントのジャーナル間の移動

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。

NOTE: 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、**アクティブなタスクをモニタ** ダイアログボックスが表示されます。ここから、1 つ以上の実行中のタスクをキャンセルすることができます。詳細については、「任意の Core コンソールページからの実行中タスクの表示」のトピックを参照してください。また、Core での将来のタスクのスケジュールを一時停止することもできます。これは、OS のアップグレードやサーバのメンテナンスを実行する場合などに役に立ちます。この機能の詳細については、「スケジュールされたタスクの一時停止または再開」を参照してください。

Rapid Recovery Core に限定したタスク、または特定のマシンに関連するタスクを表示するには、次の手順を実行します。

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。デフォルトのビューに Core のすべてのタスクが表示されます。

   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。デフォルトのビューには、選択したマシンのすべてのタスクが表示されます。

2. 必要に応じて、キーワード、開始日時、終了日時、またはそれらの任意の組み合わせでタスクのリストをフィルタして、**Enter** を押します。

   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」、「エクスポート」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 8:00 AM と入力します。
   - 現在の日時を選択するには、**開始** テキストボックスで カレンダー ウィジェットをクリックし、今日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てから、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。カレンダーの外側をクリックし、選択した変更を受け入れます。

   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。

3. 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。
	キューに登録済みの実行待ち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。
	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。

オプション	説明
	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。
	デフォルトでは表示されない Core のサービスイベントを含む、すべてのイベントを表示するには、**サービス** アイコンをクリックします。

4. 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 109. エクスポート形式

レポートのダウンロードに使用可能な出力形式です。

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 ワークブック
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。

5. 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、タスクの詳細が表示されます。

関連タスク

See also: タスクの表示
See also: スケジュールされたタスクの一時停止または再開
See also: アラートの表示
See also: ログ記録されたすべてのイベントのジャーナルを表示
See also: 任意の Core コンソールページからの実行中タスクの表示
See also: タスク、アラート、およびイベントのジャーナル間の移動

任意の Core コンソールページからの実行中タスクの表示

この手順を完了するには、Rapid Recovery Core に現在実行中のタスクがある必要があります。

Rapid Recovery では、任意の Core Console ページから Core で現在実行中のタスクを素早く表示できます。

ボタンバーの右側には、**実行中のタスク** キューがあります。画面解像度が低い場合、またはブラウザウィンドウのスペースが不十分の場合は、キューがアイコン  で表示されます。1 つまたは複数のタスクが実行中の場合、Core で現在実行中のタスクの数を示す数値はキューの横に表示され、アイコンはアニメーションで動きます。キューをクリックすると、実行中タスクのドロップダウンリストが表示され、次の手順で説明するアクションを完了させることができます。

1. Core Console で、タスクの実行中に **実行中のタスク** またはタスク実行中のアイコンをクリックします。

小さなボックスに実行中のタスクの種類とその進捗状況が表示され、1 つまたは複数のタスクのキャンセルまたは詳細確認のオプションが提示されます。

2. 1 つまたは複数のタスクをキャンセルするには、次のオプションのいずれかを実行します。
   - 単一のタスクをキャンセルするには、タスクの説明の横にある **X** をクリックします。
   - 実行中のすべてのタスクをキャンセルするには、**すべてキャンセル** をクリックします。
3. 実行中のタスクに関する詳細を表示するには、タスクの説明 をクリックします。

   アクティブなタスクをモニタ ウィンドウが開き、進行状況と開始時刻などの詳細が表示されます。

関連タスク

See also: タスクの表示
See also: タスク、アラート、およびイベントのジャーナル間の移動
See also: スケジュールされたタスクの一時停止または再開

スケジュールされたタスクの一時停止または再開

Core スケジューラを再開するには、手順 3 で説明するように、先に Core スケジューラが一時停止されている必要があります。

Core は、スケジュールに基づいてタスクを追跡します。バックアップの転送、レプリケーション、およびアーカイブは、すべてスケジュールすることができます。レポートは、毎週や毎月などの頻度で生成できます。スケジュールされたタスクを開始する時間になると、ジョブがキューに登録され、優先度に基づいて連続または同時に実行されます。この機能は、Core スケジューラと呼ばれます。

ユーザーは、スケジューラを一時停止するように Core に通知できるようになりました。一時停止された場合、一時停止されなければ Core で自動的に実行されるようにスケジュールされた今後のジョブがキューに一時的に保持され、新しいタスクはスケジュールされません。この機能は、Core サーバでの OS の更新、ソフトウェアのインストール、またはメンテンスの実行などの状況で役立ちます。一時停止されると、ジョブはキューに蓄積されますが、Core スケジューラ機能が明示的に再開されるまで開始されません。その間、Core スケジューラが一時停止していることを示すバナーが Core Console 全体に表示されます。

NOTE: この機能により、この後すぐにスケジュールされているタスクが実行されなくなります。今後のタスクを一時停止しないで、すでにキューに入っているタスクを表示またはキャンセルするには、「任意の Core コンソールページからの実行中タスクの表示」のトピックを参照してください。

Core スケジューラ機能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 に移動します。
2. アイコンバーで、✦ (イベント) をクリックします。

   タスク ページが表示されます。
3. Core スケジューラ機能を一時停止するには、次の手順を実行します。
   a. ⏸ **スケジューラの一時停止** をクリックします。
   b. 実行中のタスクをすべてキャンセルして今後のタスクを一時停止する場合は、ダイアログボックスで **アクティブなタスクをキャンセルして一時停止** を選択します。
   c. 今後のタスクのみを一時停止するには、**一時停止** をクリックします。

   タスクが一時停止され、Core Console のすべてのページにバナーが表示され、スケジュールされたすべてのタスクが一時停止されたことが通知されます。
4. 一時停止したタスクを再開するには、**タスク** ページから、▷ **スケジューラを再開** をクリックします。

NOTE: スケジューラが一時停止しているときは、Core Console の上部にあるバナーの **再開** をクリックすることもできます。

関連タスク

See also: 任意の Core コンソールページからの実行中タスクの表示
See also: タスクの表示
See also: スケジュールされたタスクの一時停止または再開

See also: アラートの表示
See also: ログ記録されたすべてのイベントのジャーナルを表示
See also: タスク、アラート、およびイベントのジャーナル間の移動

アラートの表示

アラートとは、優先順位が付けられたイベント通知のことです。通知を特別に要求したいずれのイベントも、エラー、警告、または重要な情報メッセージとともにアラートの一覧に表示されます。

Rapid Recovery Core は、アラートとして優先順位が付けられたイベントのデフォルトセットが設定された状態で出荷されます。アラートとして表示されるイベントは、デフォルトの通知グループを編集する（または新しい通知グループを設定する）ことでカスタマイズすることができます。また、**アラート** ページにこれらのイベントが表示されるだけでなく、通知オプションを変更することで通知方法を変更することができます。アラートとして表示されるイベントの変更、または通知オプションの変更についての詳細は、「Rapid Recovery のイベント通知について」のトピックを参照してください。

Rapid Recovery Core に限定したアラート、または特定のマシンに関連するアラートを表示するには、次の手順を実行します。

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）をクリックします。タスク ページのタイトルの右側にあるドロップダウン メニューをクリックし、**アラート** を選択します。

   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. アラートのカテゴリ（エラー、情報メッセージ、または警告）によってフィルタするには、ステータス ドロップダウンメニューをクリックして、ステータス状況または条件を選択します。アラートのカテゴリによるフィルタのオプションには、エラー、情報メッセージ、および 警告、またはこれら 3 つの任意の組み合わせがあります。
   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 8:00 AM と入力します。
   - ★（data and time -> date and time）現在の日時を選択するには、**開始** テキストボックスで **カレンダー** ウィジェットをクリックし、今日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てから、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。カレンダーの外側をクリックし、選択した変更を受け入れます。

   c. 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」などと入力します。

   d. 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。

関連タスク

See also: 通知グループの設定
See also: タスクの表示
See also: スケジュールされたタスクの一時停止または再開
See also: アラートの表示
See also: ログ記録されたすべてのイベントのジャーナルを表示
See also: 任意の Core コンソールページからの実行中タスクの表示
See also: タスク、アラート、およびイベントのジャーナル間の移動

関連資料

See also: Rapid Recovery のイベント通知について

ログ記録されたすべてのイベントのジャーナルを表示

ジャーナルには、記録されたすべてのイベントがリストされています。これは、ジョブに関連するイベントと、ジョブに関連しないイベントの両方を含む包括的なリストです。リストには、通知を設定した特定のイベントも含まれます。ジャーナルでは、Core やライセンスポータルなどからのパッシブイベントおよびステータスに関するイベントもリストされます。

NOTE: お使いの環境で繰り返し回数の削減機能を使用している場合、一部の重複するイベントは、イベントが発生するたびにログ記録されることはなくなります。この機能の詳細については、次を参照してください。 繰り返し回数の削減について

Rapid Recovery Core のすべてのイベントのジャーナルを表示するか、または特定のマシンのすべてのイベントのジャーナルを表示するには、次の手順を実行します。

1. Rapid Recovery Core でログ記録された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）をクリックします。タスク ページのタイトルの右側にあるドロップダウン メニューをクリックし、**ジャーナル** を選択します。

   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. イベントのカテゴリ（エラー、情報メッセージ、または警告）によってフィルタするには、ステータス ドロップダウンメニューをクリックして、ステータス状況または条件を選択します。イベントのカテゴリによるフィルタのオプションには、エラー、情報メッセージ、および 警告、またはこれら 3 つの任意の組み合わせがあります。

   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 8:00 AM と入力します。
   - ★（data and time -> date and time）現在の日時を選択するには、**開始** テキストボックスで **カレンダー** ウィジェットをクリックし、今日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てから、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。カレンダーの外側をクリックし、選択した変更を受け入れます。

   c. 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」と入力します。

d. 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。

関連概念

See also: 繰り返し回数の削減について

関連タスク

See also: タスクの表示
See also: スケジュールされたタスクの一時停止または再開
See also: アラートの表示
See also: ログ記録されたすべてのイベントのジャーナルを表示
See also: 任意の Core コンソールページからの実行中タスクの表示
See also: タスク、アラート、およびイベントのジャーナル間の移動

タスク、アラート、およびイベントのジャーナル間の移動

Core ログに記録されたイベントは、Core Console から見ることができ、イベントのカテゴリは、タスク、アラート、そしてログ記録されたすべてのイベントのジャーナルの 3 つに分けられます。

特定のマシンの Core のイベントを表示しているかどうかにかかわらず、イベントのデフォルトビューは、**タスク** ページです。ページタイトルの右にあるドロップダウンメニューをクリックすると、イベントの別のビューを選択できます。

イベントを表示し、タスク、重要なアラート、およびすべてのイベントのジャーナル間で移動するには、次の手順を実行します。

アイコンバーから ✦（イベント）をクリックして、Core に関連するイベントを表示できます。

最初に、保護対象のマシンまたはレプリケートされたマシンに移動し、ページ上部のメニューから **イベント** を選択すると、指定したマシンのイベントを表示できます。

特定のマシンの Core のイベントを表示しているかどうかにかかわらず、イベントのデフォルトビューは、**タスク** ページです。ページタイトルの右にあるドロップダウンメニューをクリックすると、イベントの別のビューを選択できます。

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。

   デフォルトのビューに Core のすべてのタスクが表示されます。手順 3 に進みます。
2. 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。

   デフォルトのビューには、選択したマシンのすべてのタスクが表示されます。手順 3 に進みます。
3. **タスク** ペインの上部左側から、▼（タスク タイトルの右側にある下向きの矢印）をクリックします。

   ドロップダウンメニューが表示されます。
4. 次のいずれか 1 つを選択します。

オプション	説明
タスク	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。
警告	アラートとは、エラー、警告、または重要な情報メッセージなど、タスクまたはイベントに関連する優先順位が付けられた通知のことです。

オプション	説明
ジャーナル	ジャーナルでは、記録されたすべてのイベントの完全なリストを示します。このリストは、アラートに含まれるイベントセットよりもさらに包括的な情報が確認できます。

選択したイベントのビューが表示されます。たとえば、**アラート** を選択した場合は、アラート ページが表示されます。

5. 別のビューを見るには、タスク、アラート、または ジャーナル ペインの右側のドロップダウンメニューに戻って、対象のビューのオプションを選択します。

   イベントのリストはフィルタされ、現在のビューには関連するイベントのセットのみを表示します。

関連タスク

See also: タスクの表示
See also: アラートの表示
See also: ログ記録されたすべてのイベントのジャーナルを表示
See also: 任意の Core コンソールページからの実行中タスクの表示

Rapid Recovery のイベント通知について

Rapid Recovery Core では、多くのイベントを追跡し、診断および操作の目的のために情報を ログ記録します。

特定のイベントに対する通知を設定することができます。Rapid Recovery では、通知の方法や、それらのイベントの記録を保持しなければならない期間を選択することができます。繰り返し回数の削減機を使用すると、同じイベントに対する通知の頻度を調整することもできます。

Core で追跡されたジョブおよびイベントは、デフォルトでは 30 日間保存されます。追跡するイベントの保持期間を変更するには、次を参照してください。 イベントの保持の設定

さまざまな方法でイベントが通知されます。サポートされる通知方法を次の表に示します。

表 110. サポートされるイベント通知方法

オプションのタイプ	説明	デフォルト設定
Email	Core の SMTP 設定を使用し、電子メール通知のテンプレートに基づいて、電子メールで指定したユーザーに通知します。	オフ
Windows イベントログ	Windows イベントログ API を使用してイベントを ログ記録します。この ログは、Windows イベントビューア またはカスタムのアプリケーションを使用して読み取ることができます。	オン
syslogd	syslog メッセージのプロトコルもサポートする Linux ログサーバで読み込まれることを意図したイベントを ログ記録します。	オフ
Toast アラート	この通知方法を選択すると、Rapid Recovery Core Console の右下隅に簡単なメッセージがポップアップ表示されます。	オン
SNMP トラップ	Rapid Recovery Core が SNMP エージェントとして設定され、この通知方法が選択された場合は、通知オプション ダイアログボックスで指定したトラップ番号を使用してイベントがログサーバに送信されます。	オン

通知グループを使用すると、通知を受信したいイベントの種類を指定して、通知方法を設定することができます。

Rapid Recovery Core には、少なくとも 1 つの通知グループが必要であり、出荷時には自動的にデフォルトのグループが適用されています。デフォルトの設定を使用するか、またはそれらの設定を編集することができます。

オプションで、他の通知グループを追加して設定することができます。たとえば、デフォルトはそのまま使用し、他のグループで電子メール通知を使用するように設定できます。

他の例としては、1 つのイベントの種類 (たとえば、Microsoft Exchange) のカスタムの通知グループを設定し、関連するすべての通知を Exchange 管理者に送信することができます。

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。

電子メール通知はデフォルトでは無効になっています。電子メールによって通知を送信するには、メールサーバの設定をして、**電子メールで通知 オプション**を有効にした状態で通知グループを編集または追加する必要があります。この設定では、通知の送信先の電子メールアドレスを入力する必要があります。詳細については、「電子メールサーバの設定」を参照してください。

Exchange Server を使用している場合は、サーバに合わせて設定する必要があります。サーバに合わせて設定しない場合、電子メールテストが成功したとしても、電子メールの通知は送信されません。詳細については、Exchange Server 管理者に確認してください。

Core では、電子メールの通知テンプレートを使用します。テンプレートには、件名の行と、メッセージ本文となる特定のコンテンツが含まれます。デフォルトで電子メール通知テンプレートが 1 つ入っています。このテンプレートでは、Core とサーバホスト、イベントの日時、イベントの性質、および該当する場合はエラーの詳細が識別されます。オプションで、デフォルトテンプレートを修正したり、カスタマイズした箇所をデフォルトの状態に復元して戻したりすることができます。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。

繰り返し回数の削減機能を使用すると、イベントの種類とスコープが同じ場合は、Core Console にログ記録されて表示されるイベントの数を減らすことができます。この機能はデフォルトで有効になっています。この機能を無効にしたり、複数のイベントをイベントログで 1 つのエントリにまとめる期間を制御したりできます。詳細については、「繰り返し回数の削減について」を参照してください。

関連概念

See also: 繰り返し回数の削減について

関連タスク

See also: 通知グループの設定
See also: イベントの保持の設定

関連資料

See also: 電子メール通知について

通知グループの設定

NOTE: 電子メールメッセージとして通知を送信する場合は、次の手順に従って、SMTP サーバをはじめに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

Rapid Recovery Core は、Core に対してデフォルトの通知グループが設定された状態で出荷されます。各環境のニーズに応じて、そのグループを編集することができます。異なる通知パラメータを使用して複数の通知グループを任意で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. Core レベルで通知を設定するには、アイコンバーで、 (その他) をクリックしてから、 **通知** を選択します。

   通知 ページが表示されます。手順 3 に進みます。
2. 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。
   a. 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。

   サマリ ページが表示されます。

   b. 保護対象マシンの **サマリ** ページの **その他** 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。
3. 新しい通知グループを追加する場合は、**グループを追加** をクリックします。「手順 5」に進みます。

   通知グループを追加 ダイアログボックスに一般的な説明の領域と 2 つのタブが表示されます。
4. デフォルトの通知グループまたは既存の通知グループを編集する場合は、通知グループ ペインにある適切な通知グループの (その他) ドロップダウンメニューをクリックして **編集** を選択します。

   通知グループを編集 ダイアログボックスに一般的な説明の領域と 2 つのタブが表示されます。
5. 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。 **CAUTION: 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。

6. **アラートを有効化** タブでアラートとなるシステムのイベントセットを設定します。これらの設定は、Core Console でイベントを表示すると **アラート** ページに表示されます。次の表に記載されるとおり、イベントのセットを選択できます。

オプション	説明
すべてのアラート	すべてのイベントにアラートを作成するには、
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。

オプション	説明
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。
デフォルトにリストア	または、Core のデフォルトの通知グループを選択して、**タイプを選択** から **デフォルトにリセット** をクリックして、イベントのセットがデフォルトの通知グループにアラートとして表示されるようにリストアします。 **NOTE:** このオプションは、Core のデフォルトの通知グループを編集する場合にのみ使用できます。Core の新しい通知グループまたは特定の保護対象マシンの設定通知には使用できません。

7. 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。
    a. **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。
    b. 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。

    - 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。
8. **通知オプション**タブをクリックします。
9. **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。 **NOTE:** Exchange Server を使用している場合は、SMTP リレーの設定がされている必要があります。SMTP リレーが設定されていないと、イベント通知は、指定した電子メールアドレスに送信されません。詳細については、Exchange Server の管理者にお問い合わせください。
Windows イベントログで通知	Windows イベントログに通知を表示させたい場合は、このオプションを選択します。

オプション	説明
syslogd で通知	Syslog に通知を表示させたい場合は、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：
Toast アラートで通知	画面の右下隅にポップアップメッセージとして通知を表示させたい場合は、このオプションを選択します。
SNMP トラップによる通知	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、SNMP マネージャによって使用されるトラップ番号を指定する必要があります。

10. **OK** をクリックします。

新しいグループを作成する場合、グループ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。

電子メール通知について

Rapid Recovery Core を設定して、指定した電子メールアドレスに、特定のイベントを通知するメールメッセージを送信することができます。アラートをトリガするイベントとその通知方法は、通知グループで定義されます。

NOTE: 通知グループは、電子メールを通知手段として使用するかどうかに関係なく、設定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。

Rapid Recovery では、電子メール通知テンプレートを使用して各通知に送信する情報を決定します。このテンプレートでは、各アラートの電子メールの件名行と、電子メールのメッセージ本文の内容が定義されます。テンプレートにはデフォルト設定があり、デフォルト設定をそのまま使用することも、目的に合わせてテストして変更を加えることもできます。通知テンプレートのカスタマイズ後は、いつでも デフォルトにリストア オプションを選択して、デフォルトのテンプレートを使用する状態に戻すことができます。電子メールのテンプレートの表示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。

通知オプションの 1 つとして電子メールを選択した場合は、はじめに電子メール用の SMTP サーバを設定する必要があります。Rapid Recovery Core では、通知グループのパラメータに基づいて、定義したサーバがアラートの送信に使用されます。

さらに、電子メールの通知を受信するには、通知グループ内で **電子メールで通知** オプションを有効にする必要があります。このオプションはデフォルトで無効に設定されています。 **電子メールで通知** 設定は、「宛先」ア

ドレスが少なくとも設定されている必要があります (オプションで、必要に応じて Cc や Bcc にアドレスを追加できます) 。

本項は、次のトピックで構成されています。

- 電子メールサーバの設定
- 電子メール通知テンプレートの設定

電子メールサーバの設定

電子メールサーバを設定するには、次の手順を実行します。

NOTE: 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。
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) 。
リストア元	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	電子メールサーバのユーザー名を入力します。
パスワード(A)	電子メールサーバ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(O)	ポート番号を入力します。電子メールサーバ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) (M)	電子メールサーバ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。

オプション	説明
TLS	メールサーバでセキュアな接続（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。

   CAUTION: 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. 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 イベントの電子メールでの通知を有効にすると、デフォルトの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 メールサーバでは、このテンプレートを使用して Rapid Recovery イベントに関する通知が電子メールで送信されます。

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、またはコンテンツのカスタマイズのプロセスについて説明します。デフォルトにリストア オプションを使用して、デフォルトの通知テンプレートへの変更をいつでも復元することができます。

CAUTION: テンプレートは、自己の責任で変更してください。ユーザーにはテンプレートへの変更をテストする責任があります。デフォルトテンプレートのみがサポートされています。

電子メール通知テンプレートを設定するには、次の手順を実行します。

NOTE: また、電子メールアラートメッセージを送信する前に、電子メールサーバおよび通知グループ設定を構成する必要があります（**電子メールで通知** オプションの有効化など）。アラートを送信するための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。

1. Rapid Recovery Core Console に移動します。
2. アイコンバーで、 （その他）をクリックしてから、**通知** を選択します。

   通知 ページが表示されます。

3. 電子メール設定 ペインで、 **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. **電子メール通知を有効にする** を選択します。

   メールテンプレートは有効で表示状態です。デフォルトのメールテンプレートの値は、次の手順で説明されています。

5. 電子メールの通知設定を編集 ダイアログボックスの内容を確認し、デフォルトの内容がニーズに適しているかどうかを確認します。

オプション	説明
電子メール通知を有効にする	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、このオプションをクリアします。
電子メールの件名	このテキストフィールドの内容によって、システムイベントの通知として送信されるメールメッセージの件名が制御されます。デフォルトのメールの件名行は次のとおりです。 <hostName> <level>: <agentName> # <name>
E メール	このテキスト領域の内容によって、システムイベントの通知として送信されるメールメッセージの本文が制御されます。デフォルトのメール本文のメッセージは次のとおりです。 <hostName> ## <shortCompanyName> <coreProductName> # <level> ##### #<name>########## ##/##: <localTimestamp> <message> <if(details.errorDetails)> <details.ErrorDetails.Message> <details.ErrorDetails.Details> <endif> --- ##########: <description> <coreAdminUrl>
テスト E メールの送信(S)	このボタンをクリックすると、表示された **テスト電子メールを送信** ダイアログボックスで指定した電子メールアドレスに、テストメールメッセージが送信されます。
デフォルトにリストア	このボタンをクリックすると、電子メールテンプレートからカスタマイズされた変更が削除され、電子メールの件名と電子メールフィールドがこの表で説明されているデフォルトの内容に復元されます。
OK(O)	このボタンをクリックすると、電子メールの通知設定を編集 ダイアログボックスの設定が保存されます。
キャンセル(C)	このボタンをクリックすると、電子メールの通知設定を編集 ダイアログボックスの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場合は、前の手順で説明されているテキストまたは変数を変更します。デフォルトで使用される変数を、以下の表で説明します。

オプション	説明
hostName	Core のホスト名
details	特定のイベントの詳細オブジェクト
agentName	このイベントに関連付けられている保護されたマシンの名前（イベントに 1 つの保護対象マシンの範囲が設定されている場合）。
repositoryName	このイベントに関連付けられているリポジトリの名前（イベントにリポジトリ範囲がある場合）。
jobSummary	このイベントに関連付けられているジョブの概要（イベントにジョブ範囲がある場合）。
remoteSlaveCoreName	このイベントに関連付けられているリモートターゲット Core の名前（イベントにターゲット Core 範囲がある場合）。
remoteMasterCoreName	このイベントに関連付けられているリモートソース Core の名前（イベントにソース Core 範囲がある場合）。
productName	製品の名前。例：「AppAssure Core」または「Rapid Recovery Core」。この製品名はホワイトラベルを使用したブランド設定に合わせて変更できます。
companyName	製品を販売する会社の名前です。

7. **電子メールの件名** テキストボックスに、電子メールテンプレートの件名を入力します。

   電子メールの件名 は、電子メール通知のテンプレートの件名を定義します（例：<ホスト名> - <レベル>: <名前>）。

8. **電子メール** テキストボックスに、イベント、発生日時、および重要度を示すテンプレートの本文の情報を入力します。
9. **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. テストメッセージに失敗したら、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、**OK** をクリックして現在のメールテンプレートの設定を保存します。次に、メールサーバ設定を手順「電子メールサーバの設定」の説明に従って変更します。メールアカウントのパスワードをもう一度確実に入力します。それらの設定を保存し、この手順に戻ります。
   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。

テスト結果に問題がなければ、電子メールの通知設定を編集 ダイアログボックスに戻り、**OK** をクリックしてダイアログボックスを閉じ、設定を保存します。

イベント設定の構成

イベント固有の特定の設定を構成できます。

たとえば、繰り返される同じイベントに対しての通知の量を減らすために、繰返し回数の削減設定をすることができます。

また、イベントがデータベースに保存される期間を日数で設定することもできます。

イベント設定の構成についての詳細は、以下のトピックを確認してください。

- 繰り返し回数の削減について
- イベントの保持の設定

関連資料

See also: タスク、アラート、およびジャーナルページを使用したイベントの表示
See also: Rapid Recovery のイベント通知について

繰り返し回数の削減について

特定のイベントが発生した時点で管理者が通知を受け取ることは、非常に重要です。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。管理者がすぐに認識すべき環境の問題が原因で通知が 1 つだけ生成される場合も、同じエラー条件に対し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。イベントログの繰り返しを削減し、Core Console の同じイベントに対して Toast アラートや電子メールによる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設定があります。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の経過時間に関係なく、新しいイベントが発生するごとに、その各イベントは イベント ページの 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がしきい値を超えるまで、同じイベントに対してイベントログ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、別の通知が届きます。

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、 (その他) をクリックして、**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. 保存されるイベントの時間しきい値を有効化、無効化、または変更するには、**変更** をクリックします。

繰返し回数の削減の編集 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を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。

   NOTE: 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** 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内容を保存します。

   イベントの保持期間が、指定したとおりに調整されます。

レポート

本項では、Rapid Recovery Core Console で使用できるレポート機能の概要を説明します。

Rapid Recovery レポートについて

次のようなレポートを Rapid Recovery Core Console から生成できます。その他のレポートも Data Protection ポータル から利用できるようになる予定です。

Core Console から使用できるレポートの説明を次の表に示します。

表 111. Rapid Recovery レポート

レポートタイプ	説明
ジョブレポート	成功したジョブ、失敗したジョブ、エラーが検出されたジョブのステータスについて基本的な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。 • デフォルトでは、レポートの時間範囲は過去 31 日間です。これはカスタマイズすることができます。 • Core からを実行すると、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 (データベースサーバ、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
ジョブサマリレポート	成功したジョブ、失敗したジョブ、エラーが検出されたジョブのステータスについてより詳細なレポートを提供します。ジョブタイプごとにレポート内で個別の行が表示され、潜在的な問題をより適切に診断できます。 • デフォルトでは、レポートの時間範囲は過去 31 日間です。これはカスタマイズすることができます。 • ジョブレポートとは異なり、このレポートではパラメータとして Core を選択することができません。 • デフォルトでは、この情報のセットには、すべてのマシン (データベースサーバ、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) のジョブと、マシンに依存するジョブがジョブタイプごとに含まれます。レポートをカスタマイズすることができます。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。マシンに依存しないジョブを選択または除外することもできます。 • 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。 このレポートタイプの詳細については、ジョブサマリ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
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。このレポートには、保護対象マシンの詳細を含めることも除外することもできます。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。 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
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。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。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、すべて Core の視点によるものです。 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
従来のサマリレポート	このレポートには、ジョブ統計情報成功、GB ごとのリポジトリサマリ、スナップショット成功、リポジトリ使用状況トレンドのサマリビュー、および Core 上の保護対象マシンのサマリを表示できます。レポートパラメーターには、日付範囲と関連する Core が含まれます。
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 からの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。

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 からの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、 (その他) 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、サマリレポート、または Core (クラシック) 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
過去 24 時間	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。
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。

オプション	説明
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。

NOTE: 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、失敗レポート、または Core (クラシック) 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
すべて選択	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。 **NOTE:** 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。
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な生成されます。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も、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

オプション	説明
	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。

    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。
13. 次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 メニューの使い方 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 ツールバーの使い方」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。

1. Rapid Recovery Core Console に移動します。
2. 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。

3. 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
過去 24 時間	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。
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。

   NOTE: 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 メニューの使い方 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 ツールバーの使い方」を参照してください。

Core Console からの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。

NOTE: 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。

- 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

関連概念

See also: 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

関連タスク

See also: レポートのスケジュール設定
See also: レポートスケジュールの変更

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、 (その他) 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 112. 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
名前名前(N)	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」は適用できません。
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で 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。
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。

マシン	使用可能なレポート
	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。

     NOTE: 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 113. 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」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 114. 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
毎日	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(W)	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。
毎月	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、（その他）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. 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、（その他のオプション）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し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、 (その他) 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. 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 メニューの使い方

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 115. レポートメニューのコントロール

UI エレメント	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。

See also: ジョブレポートについて
See also: 失敗レポートについて
See also: サマリレポートについて

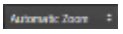
レポート ツールバーの使い方

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 116. 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：サムネイルの表示。**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。

アイコン	説明
	**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。
	**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。

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、レポート対象の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 で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、それらのマシンのボリューム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）、成功したジョブの数、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。

NOTE: 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、レポート対象の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ているかどうか
- 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。

従来のサマリレポートについて

従来のサマリレポートは、Core に関するさまざまな役に立つメトリックスについて選択した期間のサマリを提供します。

上部には、3 つの円グラフがあります。1 つ目はジョブの統計情報 (成功したジョブ、キャンセルされたジョブ、および失敗したジョブ) を示します。2 番目の円グラフは、リポジトリごとの容量を GB 単位で示します。3 番目の円グラフは、スナップショットの統計情報 (成功したジョブ、キャンセルされたジョブ、および失敗したジョブ) を示します。

次に示すのは、リポジトリ使用状況を示すトレンドグラフです。

最後に、レポートには保護対象マシンのサマリが記載されています。

このレポートタイプのレポートパラメーターには、日付範囲および関連する Core が含まれます。

Core からのこの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。

VM のエクスポート

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

Rapid Recovery Core から、Windows または Linux マシンのリカバリポイントをサポート対象のいずれかのフォーマットで仮想マシン（VM）にエクスポートできます。Core で保護される元の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障害が発生したマシンとすばやく置き換えることで、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できます。この仮想エクスポートプロセスでは、結果的に、保護対象マシンのオペレーティングシステムと設定とともに、リカバリポイントから取得したすべてのバックアップ情報を含む VM となります。この VM が起動可能な保護対象マシンのクローンとなります。

NOTE: 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ーファン」のトピックを参照してください。

Core Console の **仮想スタンバイ** ページから、Core に表示される特定のリカバリポイントから、または、ボタンバーの **リストア** ドロップダウンメニューから **VM のエクスポート** を選択して、仮想エクスポートを実行することができます。

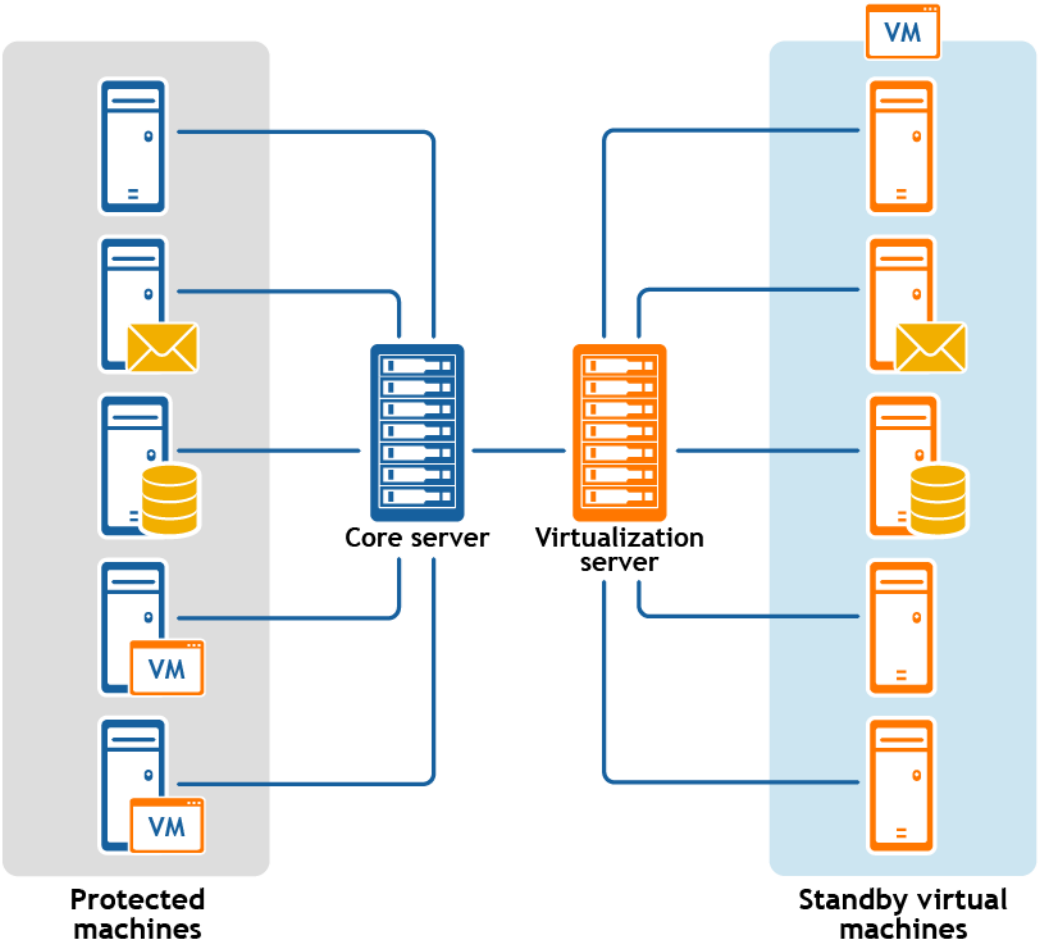
Rapid Recovery Core から仮想エクスポートを実行する場合は、次の 2 つの方法があります。

- **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、選択したリカバリポイントの情報から、所定の時点の単一のスナップショットとなるブータブル VM が作成されます。このエクスポートジョブはすぐにキューに追加され、キューの追加が完了すると、複製された VM が指定した場所にエクスポートされます。1 回限りのエクスポートに使用した設定情報は保存されません。
- **継続エクスポート**をセットアップできます。このプロセスでは、指定した最初のリカバリポイントから起動可能な VM を作成して、VM を指定した場所に保存します。仮想エクスポートを実行するための設定情報については、Core Console の **Virtual Standby** ページに保存されます。その後に、保護対象マシンのスナップショットがキャプチャされるごとに、Core により新しい仮想エクスポートのジョブがキューに登録され、ブータブル VM は最新情報で更新されます。この操作によりデータリカバリのための高可用性のリソースが作成されるため、この機能は**仮想スタンバイ**とも呼ばれます。

仮想エクスポートのジョブがキューに登録されて完了するまでの間に、このジョブは Core Console の Virtual Standby ページの エクスポートキュー ペインの一覧に表示されます。

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 5. 仮想スタンバイの展開



NOTE: 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。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。

互換性のある VM ハイパーバイザーには、vCenter/ESXi、VMware Workstation、Hyper-V、VirtualBox、および Azure が含まれます。これらのハイパーバイザのサポートされているバージョンについては、*Rapid Recovery ## #######* で「ハイパーバイザの要件」のトピックを参照してください。

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。Azure のエクスポートには、Azure アカウントやその他の前提条件が必要です。

NOTE: Azure では、エクスポートや最終的な配置で、新しいリソースマネージャモデルではなく従来の VM 管理を使用して VM を作成します。Azure との連携には、使用するクラウドサービスのプロバイダに固有の要素が含まれます。詳細については、「Azure へ仮想エクスポートする前に」を参照してください。

関連概念

See also: ESXi 仮想マシンへのデータのエクスポート
See also: VMware Workstation 仮想マシンへのデータのエクスポート
See also: VirtualBox 仮想マシンへのデータのエクスポート
See also: Azure 仮想マシンへのデータのエクスポート

関連タスク

See also: エクスポートの管理

関連資料

See also: Hyper-V 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 (仮想スタンバイの場合) 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 仮想マシンへエクスポート 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 117. 仮想マシンパラメータ

オプション(O)	説明
ホスト名	ホストマシンの名を入力します。
ポート(O)	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(A)	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。
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。

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。 • ソースマシンと同容量の RAM を使用します • 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。
ディスクのプロビジョニング	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 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て **次へ** をクリックします。
13. **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。

NOTE: **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。

ESXi への連続エクスポートのセットアップ

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セットアップするには、この説明の各手順を実行します。これは、仮想スタンバイの設定としても知られています。

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** をクリックします。
     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、（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 119. 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(O)	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(A)	ホストマシンのログオン資格情報を入力します。

8. **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 120. 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。 • ソースマシンと同容量の RAM を使用します • 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。

オプション	説明
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。
最初の 1 回限りのエクスポートを実施	スケジュールされた次回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。

NOTE: 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。

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（仮想スタンバイの場合）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 仮想マシンへエクスポート 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。 **NOTE:** 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(A)	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。 **NOTE:** 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
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。 • ソースマシンと同容量の RAM を使用します • 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。

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 **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。

NOTE: 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。

Vmware Workstation への連続エクスポートのセットアップ

Rapid Recovery を使用して VMware Workstation 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。これは、仮想スタンバイの設定としても知られています。

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** をクリックします。
     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、（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. 「**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 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。 **NOTE:** 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(A)	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。 **NOTE:** 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

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。 • ソースマシンと同容量の RAM を使用します • 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。
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。

NOTE: 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。

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（仮想スタンバイの場合）を設定して、データを Hyper-V にエクスポートできます。

第 1 世代および第 2 世代の Hyper-V エクスポートでサポートされるホストオペレーティングシステムについては、『*Rapid Recovery #########*』で「ハイパーバイザの要件」のトピックを参照してください。

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、**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. **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(O)	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(A)	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。

    NOTE: 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。

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

    NOTE: 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。

    NOTE: 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

    NOTE: 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。

    NOTE: 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、**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。

    NOTE: **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。

Hyper-V への連続エクスポートのセットアップ

Rapid Recovery を使用して Hyper-V 仮想マシン（VM）への連続エクスポートをセットアップするには、次の手順を実行します。これは、仮想スタンバイの設定としても知られています。

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** をクリックします。
        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、（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. **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(O)	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(A)	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。

   NOTE: 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

    NOTE: 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。

    NOTE: 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

    NOTE: 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。

    NOTE: 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。
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。

    NOTE: **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。

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（仮想スタンバイの場合）を設定して、データを VirtualBox 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。

NOTE: Windows ホスト上で VirtualBox VM に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。Linux でホストされている VM はこの要件を共有しません。

1 回限りの VirtualBox エクスポートの実行

リモートの Windows ホスト上の VirtualBox VM にエクスポートするには、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。この要件は、Linux でホストされている VM には該当しません。

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** ページで、仮想マシンへエクスポート ドロップダウンメニューから **VirtualBox** を選択してから、**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、**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 125. 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。 **NOTE:** 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。 **NOTE:** 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。 • ソースマシンと同容量の RAM を使用します • 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 **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。

NOTE: **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。

VirtualBox への連続エクスポートのセットアップ

リモートの Windows ホスト上の VirtualBox VM にエクスポートするには、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。この要件は、Linux でホストされている VM には該当しません。

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 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。
     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、（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 126. 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(O)	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。 **NOTE:** 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。 **NOTE:** 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(A)	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。

オプション	説明
パスワード(A)	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。 • ソースマシンと同容量の RAM を使用します • 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。

NOTE: 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。

Azure 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 (仮想スタンバイの場合の場合) を設定して、データを Azure にエクスポートできます。Azure プラットフォームへの 1 回限りのエクスポートには、ワークフローに展開が含まれます。連続エクスポートを使用する場合、エクスポートされたファイルを後でブータブル VM として展開することもできます。

Azure の操作の詳細については、「」を参照してください。

Azure への仮想エクスポートの前提条件については、「Azure へ仮想エクスポートする前に」を参照してください。

Azure への仮想エクスポートに関する固有の側面についての詳細説明については、「Azure への VM のエクスポートと展開」を参照してください。

Azure の設定と価格の詳細については、Azure ウェブサイトの「Virtual Machines の価格」ページを参照してください。

Microsoft ウェブサイトのその他の有用なリファレンスへのリンクについては、 を参照してください。

Azure での VM のエクスポートまたは展開に関連する手順については、次の関連リンクを参照してください。

関連概念

See also: VirtualBox 仮想マシンへのデータのエクスポート

関連タスク

See also: Azure への連続エクスポートの設定
See also: Azure での仮想マシンの展開
See also: 1 回限りの Azure エクスポートの実行

Microsoft Azure での操作

Microsoft Azure は、サブスクリプションベースのクラウドコンピューティングプラットフォームです。弊社の製品で Azure を容易に使用できるように、次の情報が Rapid Recovery のお客様に提供されます。

- Azure インタフェースの免責事項
- Azure ストレージアカウントでのコンテナの作成
- Azure への VM のエクスポートと展開
- Microsoft Azure のマニュアル

Azure インタフェースの免責事項

Microsoft Azure のインタフェースは変更される可能性があります。

この文書に記載された、Azure で必要となる手順に関する情報は、公開日時点で最新の情報です。この情報は、Azure を使用する際の前提条件とともに、お客様をサポートするためのサービスとして提供されます。

ただし、Azure に関する操作を行う場合は、Azure 固有のステップに注意してください。URL だけではなく Azure のインタフェースにも、常時変更が加えられる可能性があります。このような変更は弊社では予期することができません。

Azure のアカウントに関する手順の実行に問題が生じた場合は、Microsoft Azure の担当者にアドバイスを求めてください。

Azure ストレージアカウントでのコンテナの作成

- Azure のアカウントに管理者アクセス権限がある必要があります。
- お使い Azure アカウント内で定義されたストレージアカウントが必要です。

仮想エクスポートを実行すると、その情報は Azure ストレージアカウント内のコンテナに格納されます。仮想エクスポートを実行する前に、下記の手順を使用してお使いの Azure アカウントからコンテナを定義できます。または、ウィザードの **宛先** ページから、エクスポートプロセスの一部としてコンテナを定義できます。

この手順のステップを完了して、Azure ストレージアカウントにコンテナを作成します。

1. Microsoft Azure ダッシュボードを開きます。
2. 左のナビゲーションエリアから、**すべてのリソース** をクリックします。
3. **すべてのリソース** ペインで、Rapid Recovery の仮想エクスポートによるデータを保存するストレージアカウントの名前をクリックします。
4. **設定** ペインで、**BLOB** をクリックします。
5. **BLOB サービス** ペインの上部のヘッダーで、**+ コンテナー** をクリックします。
6. **新しいコンテナー** ペインの **名前** フィールドに、新しいコンテナの名前を入力します。

   NOTE: 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。

7. **新しいコンテナー** ペインの **アクセスの種類** ドロップダウンメニューで適切なコンテナの種類を選択して、コンテナーを公開するかどうかを定義します。次の説明を参考にしてください。

オプション	説明
プライベート	このオプションでは、コンテナはアカウント所有者に制限されます。

オプション	説明
BLOB	このオプションでは、バイナリラージオブジェクト（BLOB）の公開読み取りアクセスを許可します。
コンテナ	このオプションでは、公開読み取りおよびリスト表示アクセスをコンテナ全体に許可します。

たとえば、**コンテナ** を選択します。

8. **Create**をクリックします。

   Toast アラートがアクティブな場合、コンテナが正常に作成されたことを示すメッセージが表示されます。

   BLOB サービス ページが更新され、新しいコンテナの名前がリストに表示されます。

Microsoft Azure のマニュアル

Microsoft では Azure の使用に関する数多くのマニュアルを用意しており、それらはドキュメントセンターで利用することができます。

Azure アカウントの作成、Rapid Recovery または AppAssure Core で使用するための VM のスピンアップ、ストレージアカウントの追加などの詳細については、「https://azure.microsoft.com/en-us/documentation」で Microsoft のマニュアルを参照してください。

たとえば、Windows VM のプロビジョニングや管理の詳細については、「https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/」を参照してください。

Azure の使用に関するオンラインビデオは、「http://azure.microsoft.com/en-us/get-started/」を参照してください。

NOTE: Azure ウェブサイトでは、ウェブアドレスの言語と国コードを使用してコンテンツの表示に反映されます。たとえば、`https://azure.microsoft.com/[####]/[##]/` などです。

NOTE: 本書全体で使用する Azure の URL には、米国における英語の国コードが含まれます。その他の言語の場合、お使いのコンピュータの設定および Microsoft から提供されているコンテンツによって、これらのコードに基づく URL は異なる場合があります。

関連するMicrosoft リンク

Microsoft のウェブサイトにある関連記事の一部は次のとおりです。

- Azure ログインページ（米国）
- Microsoft Azure ホームページ
- Microsoft ドキュメントセンター
- Windows Virtual Machines のドキュメント
- ビデオ：Azure を使ってみる
- Azure 仮想マシンの価格
- 地域別の Azure サービス
- Azure ストレージアカウントについて
- Azure ストレージアカウントの作成
- Azure ポータルで Windows VM にデータディスクを接続する方法
- Microsoft Azure Import/Export サービスを使用した Blob Storage へのデータの転送
- Import/Export の料金
- Storage: Import/Export Hard Disk Drives to Windows Azure（ストレージ：Windows Azure へのハードディスクドライブのインポート / エクスポート）（ブログ投稿）

Azure へ仮想エクスポートする前に

Rapid Recovery では、Microsoft Azure への仮想エクスポート（1 回限り、または仮想スタンバイ）を実行できます。

Rapid Recovery によって保護されるマシンで仮想エクスポートを実行する前には、「クラウドアカウントの追加」のトピックで説明されているように、最初にお使いの Azure クラウドアカウントを Core に関連付ける必要があります。

Azure に適切なストレージアカウントが必要です。Azure でのストレージアカウントの作成についての詳細は、「」のトピックに記載された Azure のサポート情報をご参照ください。

お使いのストレージアカウントで、エクスポートを保存するためのコンテナを動的に作成するか、または既存のコンテナを使用することができます。ストレージコンテナ作成の詳細については、「Azure ストレージアカウントでのコンテナの作成」を参照してください。

Rapid Recovery を使用した他の仮想エクスポートの形態とは異なり、Azure への VM エクスポートには 2 つのプロセスが含まれます。詳細については、「Azure への VM のエクスポートと展開」のトピックで説明されています。

Azure への VM のエクスポートと展開

他のプラットフォームへの仮想エクスポートとは異なり、Azure への仮想エクスポートには、「エクスポート」と「展開」の 2 つのプロセスがあります。

Microsoft Azure の顧客は、料金を負担する必要があることに注意してください。Azure との統合における一部の要素は、この料金構造を念頭に置いて設計されています。たとえば、Microsoft では Azure に VM を展開する場合と、データが Azure から他のソースに転送される場合に、料金が発生します。

NOTE: Microsoft により前提条件、要件、価格などは変更される場合があるため、常にこのような Azure に関する情報を確認してください。詳細については、Azure のウェブサイトを参照するか、Azure の担当者にお問い合わせください。

必要がない可能性がある費用を支払うため、不要な費用請求がないように、Azure への 仮想エクスポートは 2 つの異なるプロセスの構成になっています。

エクスポートプロセスでは、Rapid Recovery から必要なファイルのセットを抽出して検証し、それらのファイルを指定した Azure のコンテナにアップロードします。これらのファイルには以下が含まれています。

- リカバリポイント内の各ボリュームに対して、1 つの仮想ハードディスク (VHD) 。
- 各ディスクのメタ情報が入っている単一の XML ファイル (各ディスクとボリュームがシステムディスクかどうかを示すフラグを表すファイルの一覧です) 。
- バックアップスナップショットを含む 1 つの VHD ファイル。

必要なストレージにかかる費用以外、エクスポート処理自体には Azure の料金は発生しません。

展開プロセスでは、これらのファイルを結合して単一の起動可能な仮想マシンにします。展開では、Azure のクラウド REST API を直接使用します。エクスポートプロセス中 Azure にはじめに配置されたファイルのセットは、Azure では読み取り専用であり、ディスク容量を消費しますが、Azure にそれ以外の費用はかかりません。これらのファイルを展開する場合は、各ファイルを複製したコピーが作成され、定義した別のコンテナに格納されて、動作中の単一の仮想マシンに組み込まれます。Azure アカウントの観点では、展開した後は、そのサーバ上の VM に対して料金が発生します。展開された VM は、エクスポートされたファイルのコピーであるため、展開プロセスでは仮想エクスポートに必要な Azure のストレージ領域の使用容量は倍になります。

1 回限りの仮想エクスポートの場合は、別個のプロセスで展開する仕組みはありません。したがって、このエクスポートを効率的に実行するには、仮想マシンの作成が必要になった時点で Azure を展開する必要があります。結果として、Azure への 1 回限りのエクスポートでは、展開する VM に関する費用が即時発生します。

Azure 上の保護対象マシンに仮想スタンバイを設定する場合、余分なストレージ容量と VM の費用が発生することを避けるためには、エクスポートプロセスをシンプルに定義することが考えられます。シンプルに定義すると、結果的にはじめの仮想エクスポートを定義することになり、それは随時アップデートされることになります。Core でスナップショットがキャプチャされるごとに、エクスポートされたファイルは最新の情報で Azure アカウントを更新します。仮想エクスポートしたファイルを起動 VM として使用するには、起動する前にエクスポートしたファイルを展開する必要があり、その展開では Azure に費用が発生します。保護対象マシンでエクスポートしたファイルを起動可能な VM に変換する必要がない場合は、Azure アカウントに VM を展開する費用は発生しません。

展開を含む、Azure への 1 回限りのエクスポートについての詳細は、「1 回限りの Azure エクスポートの実行」のトピックを参照してください。

Azure への連続エクスポートのセットアップについての詳細は、「Azure への連続エクスポートの設定」のトピックを参照してください。

エクスポートされた最新ファイルの Azure での展開および起動可能な仮想スタンバイ VM の作成についての詳細は、「Azure での仮想マシンの展開」のトピックを参照してください。

1 回限りの Azure エクスポートの実行

1 回限りの Azure エクスポートを実行するには、次の条件が必要です。

- Azure にエクスポートするリカバリポイントが Rapid Recovery Core に少なくとも 1 つ存在する保護対象マシンが必要です。
- 展開された VM が正常に起動するためには、保護対象マシンでリモートアクセスが有効化されている必要があります。
- Azure のアカウントに管理者アクセス権限がある必要があります。
- オプションで、エクスポートする前に、エクスポートするデータが格納されるお使いの Azure ストレージアカウント内に適切なコンテナを作成することができます。詳細については、「Azure ストレージアカウントでのコンテナの作成」のトピックを参照してください。

「Azure への VM のエクスポートと展開」のトピックで説明するように、Azure への仮想エクスポートにはエクスポートと展開の 2 つのプロセスがあります。

エクスポートプロセスでは、Rapid Recovery から必要なファイルのセットを抽出して検証し、それらのファイルを指定した Azure のコンテナにアップロードします。これらのファイルには以下が含まれています。

- リカバリポイント内の各ボリュームに対して、1 つの仮想ハードディスク (VHD)
- 各ディスクのメタ情報が入っている単一の XML ファイル (各ディスクとボリュームがシステムディスクかどうかを示すフラグを表すファイルの一覧です)
- バックアップスナップショットを含む 1 つの VHD ファイル

展開プロセスでは、これらのファイルを結合して単一の起動可能な仮想マシンにします。展開では、Azure のクラウド REST API を直接使用します。エクスポートプロセス中 Azure にはじめに配置されたファイルのセットは、Azure では読み取り専用であり、ディスク容量を消費しますが、Azure に追加費用はかかりません。これらのファイルを展開する場合は、各ファイルを複製したコピーが作成され、定義した別のコンテナに格納されて、動作中の単一の仮想マシンに組み込まれます。Azure アカウントの観点では、展開した後は、そのサーバ上の VM に対して料金が発生します。展開プロセスでは、仮想エクスポートに必要な Azure のストレージ領域の使用容量は倍になります。

1 回限りの仮想エクスポートの場合は、別個のプロセスで展開する仕組みはありません。したがって、このエクスポートを効率的に実行するには、仮想マシンの作成が必要になった時点で Azure を展開する必要があります。

Azure 上の保護対象マシンに仮想スタンバイを設定する場合、余分なストレージ容量と VM の費用が発生することを避けるために、リカバリポイントのエクスポートと継続的なアップデートを行うことで展開する必要性を排除することが考えられます。その後で VM を使用する必要が出てきた時に、Azure に展開できます。Azure での仮想スタンバイを展開して機能する VM にする場合の詳細については、Azure での VM への仮想スタンバイデータの展開に関するトピックを参照してください。

Azure に対して 1 回限りのエクスポートを実行して VM として展開するには、次の手順を実行します。

1. Rapid Recovery Core Console 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。

   仮想マシンのエクスポート ウィザードが表示されます。
2. このウィザードの **VM のエクスポートタイプを選択** ページで、**1 回限りのエクスポート** を選択してから、**次へ** をクリックします。

   ウィザードの **マシン** ページが表示されます。
3. **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、**次へ** をクリックします。
4. **リカバリポイント** ページで、リカバリポイントのリストを必要に応じてスクロールして、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。次に、**次へ** をクリックします。
5. **宛先** ページにある 仮想マシンへエクスポート ドロップダウンメニューで、**Azure** を選択します。
6. 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 127. Azure の認証情報

オプション(O)	説明
公開設定ファイル	公開設定ファイルは、Azure のサブスクリプション情報を管理する認証情報を含む Azure で生成された XML ドキュメントです。 **NOTE:** 公開設定は、Core の UI から Azure アカウントごとに定義する場合にのみ必要です。その後、公開設定はキャッシュされます。 この公開ファイルが必要というプロンプトが表示された場合は、Azure のアカウントにログインし、お使いの VM の「https://manage.windowsazure.com/publishsettings/index?client=powershell」から公開ファイルをダウンロードします。 このファイルは、AzureServiceManagement API と、セキュリティに関わる認証情報を含むお使いの Azure サブスクリプションについての情報を定義します。アカウントにアクセスして仮想エクスポートを実行するには、Rapid Recovery Core でこのファイルを定義する必要があります。 セキュリティを確保するため、ファイルは安全な場所に格納するか、この手順を実行した後で削除します。

オプション(O)	説明
サブスクリプション	公開設定ファイルを追加した直後の場合は、この情報は公開設定ファイルから自動的に入力されます。 **NOTE:** 公開設定は、Core の UI から Azure アカウントごとに定義する場合にのみ必要です。その後、公開設定はキャッシュされます。 以前追加した公開設定ファイルを使用する場合は、ドロップダウンリストからファイルを選択します。 公開設定ファイルを追加する場合は、＋ボタンを使用して **証明書のロード** ウィンドウを開いて、ファイルを参照します。 この公開ファイルが必要というプロンプトが表示された場合は、Azure のアカウントにログインし、お使いの VM の「https://manage.windowsazure.com/publishsettings/index?client=powershell」から公開ファイルをダウンロードします。 セキュリティを確保するため、ファイルは安全な場所に格納するか、この手順を実行した後で削除します。
アカウント	Core に関連付けられている Azure クラウドアカウントです。サブスクリプションファイルから自動的に入力されます。 **NOTE:** 「クラウドアカウントの追加」のトピックに説明されているように、最初に Azure クラウドアカウントを Core に関連付ける必要があります。
コンテナ名	すでにコンテナがある場合は、ドロップダウンメニューから、お使いの Azure のクラウドアカウントに関連付けられた適切なコンテナの名前を選択します。または、新しいコンテナの名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。
フォルダ名	エクスポートした仮想マシンを格納するコンテナ内のフォルダ名を指定します。 **NOTE:** Azure フォルダ名に、「/ \ : * ? " < > I」は使用できません。

7. **展開** ページで、次の表に記載されているように VM を展開する宛先を入力し、**次へ** をクリックします。

表 128. Azure への展開オプション

オプション	説明
クラウドサービス名	Azure のクラウドサービスは、従来の管理モデルを使用した仮想マシン用のコンテナです。すでに利用しているクラウドサービスがある場合は、**クラウドサービス名** ドロップダウンメニューから、適切なクラウドサービス名を選択します。または、**クラウドサービス名** フィールドに一意で、分かりやすいクラウドサービス名を入力します。 **NOTE:** Microsoft Azure サブスクリプションには、利用できるクラウドサービスの数にデフォルトで制限があります (通常は 25 です) 。このサブスクリプションの制限を超えていないことを確認します。
展開名	既存の仮想マシンからクラウドサービスを選択した場合、このフィールドは自動的に入力されます。仮想マシンがないクラウドサービスを選択した場合は、この新しい展開のための名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。
宛先コンテナ	VM を格納するコンテナ名を入力します。

オプション	説明
	NOTE: 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。

8. **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 129. 仮想マシンオプション

オプション	説明
仮想マシン名	仮想マシンの名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 15 文字で入力します。
仮想マシンのサイズ	ドロップダウンリストから、適切な VM のサイズを選択します。 **NOTE:** Azure の設定と価格の詳細については、Azure ウェブサイトの「Virtual Machines の価格」ページを参照してください。Microsoft ウェブサイトのその他の有用なリファレンスへのリンクについては、 を参照してください。
エンドポイント (リモートアクセス設定)	リモートアクセス設定には、次の VM オプションがあります。
名前	**リモートデスクトップ** または **SSH** を選択します。
プロトコル	**TCP** または **UDP** を選択します。
ポート	公開用ポートおよびプライベートポートはデフォルトで 3389 を使用します。必要に応じて変更します。
データ転送サーバポート	公開用ポートおよびプライベートポートはデフォルトで 8009 を使用します。必要に応じて変更します。
エージェントポート	公開用ポートおよびプライベートポートはデフォルトで 8006 を使用します。必要に応じて変更します。

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を選択し、**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。

NOTE: **Virtual Standby** または **イベント** ページで、エクスポートキュー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。

Azure への連続エクスポートの設定

Azure への連続仮想エクスポートを実行する前に、次の条件が必要です。

- Azure にエクスポートする Rapid Recovery Coreのリカバリポイントが少なくとも 1 つある保護対象マシンがある必要があります。
- 展開された VM が正常に起動するためには、保護対象マシンでリモートアクセスが有効化されている必要があります。
- Azure のアカウントに管理者アクセス権限がある必要があります。
- Azure アカウントを Core に関連付けるには、まず Azure 内から公開設定ファイルをダウンロードする必要があります。詳細については、Azure アカウントの公開設定ファイルの取得を参照してください。
- オプションで、エクスポートする前に、エクスポートするデータが格納されるお使いの Azure ストレージアカウント内に適切なコンテナを作成することができます。保護対象マシンで保護するデータが増えるにつれて、ストレージ要件が増大することに注意してください。Azure アカウントでは、指定するコンテナが VM に対応するために十分な容量を備えたストレージの場所に関連付けられている必要があります。詳細については、「Azure ストレージアカウントでのコンテナの作成」のトピックを参照してください。

この手順を完了して、Rapid Recovery を使用して Azure クラウドアカウントの指定されたコンテナへの選択したマシンの連続仮想エクスポートを実行します。

NOTE: このプロセスには、エクスポートされたファイルを展開してブータブル仮想マシンを作成することは含まれていません。導入の手順については、「Azure での仮想マシンの展開」を参照してください。

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** をクリックします。
     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、(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. **宛先** ページにある 仮想マシンへエクスポート ドロップダウンメニューで、**Azure** 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パラメータを入力し、**次へ** をクリックします。

表 130. Azure の認証情報

オプション(O)	説明
公開設定ファイル	このオプションは、Azure サブスクリプションを Core に関連付けていない場合にのみ表示されます。このオプションが表示された場合は、「Azure アカウントの公開設定ファイルの取得」のトピックで説明されているようにファイルをダウンロードし、サブスクリプションを Core に関連付けます。この関連付けは、Core 内から Azure アカウントに接続して仮想エクスポートを実行する前に完了する必要があります。 **NOTE:** 公開設定は、Core の UI から Azure アカウントごとに定義する場合にのみ必要です。その後、公開設定はキャッシュされます。

オプション(O)	説明
	セキュリティを確保するため、ファイルは安全な場所に格納するか、この手順を実行した後で削除します。
サブスクリプション	公開設定ファイルを追加した直後の場合は、この情報は公開設定ファイルから自動的に入力されます。 **NOTE:** 公開設定は、Core の UI から Azure アカウントごとに定義する場合にのみ必要です。その後、公開設定はキャッシュされます。 以前追加した公開設定ファイルを使用する場合は、ドロップダウンリストからファイルを選択します。 公開設定ファイルを追加する場合は、+ボタンを使用して **証明書のロード** ウィンドウを開いて、ファイルを参照します。
アカウント	Core に関連付けられている Azure クラウドアカウントです。サブスクリプションファイルから自動的に入力されます。 **NOTE:** トピックで説明されているように、最初に Azure クラウドアカウントを Core に関連付ける必要があります クラウドアカウントの追加
コンテナ名	すでにコンテナがある場合は、ドロップダウンメニューから、お使いの Azure のクラウドアカウントに関連付けられた適切なコンテナの名前を選択します。または、新しいコンテナの名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。
フォルダ名	エクスポートした仮想マシンを格納するコンテナ内のフォルダ名を指定します。 **NOTE:** Azure フォルダ名に、「/ \ : * ? " < > I」は使用できません。
最初の 1 回限りのエクスポートを実施	仮想スタンバイを定義する場合は、このオプションを選択して、エクスポートジョブをただちにキューに入れます。次回の強制またはスケジュールされたバックアップのスナップショット取得まで Core が待機するようにするには、このオプションをオフにします。

8. **次へ** をクリックします。
9. **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。
10. **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。

NOTE: 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。

この手順で定義する仮想スタンバイパラメータにより、Azure アカウントで VM を作成するために必要なファイルがエクスポートされます。すべてのスナップショット (強制またはスケジュールされた) の取得後は、これらのファイルは Azure で新しいバックアップ情報により更新されます。これらのファイルを VM として起動する前に、Azure で VM を導入する必要があります。導入の手順については、「Azure での仮想マシンの展開」を参照してください。

Azure での仮想マシンの展開

Azure で VM を展開する前に、Rapid Recovery Core 上に 1 つ以上のリカバリポイントを持つ保護対象マシンがあり、Core Console で連続エクスポート (仮想スタンバイ) がセットアップされている必要があります。連続エクスポートのセットアップの詳細については、「Azure への連続エクスポートの設定」を参照してください。ま

たこのプロセスでは、Core に十分なストレージが関連付けられている Azure のアカウントがある必要があります。

保護対象マシンの仮想スタンバイを Azure にセットアップすると、最新のバックアップ情報がバックアップスナップショットの取得のたびに Core から Azure アカウントに連続的にエクスポートされます。このプロセスにより、前のエクスポートファイルセットのバックアップ情報が更新されます。（たとえば、元の保護対象マシンが故障した場合に）仮想エクスポートを VM として起動する前に、まず Core Console から導入する必要があります。このプロセスにより、新しいコンテナで起動可能な VM が生成されます。

この手順を完了すると、最新の仮想スタンバイエクスポートファイルが Azure のブータブル VM に導入されます。

1. Rapid Recovery 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。
2. **Virtual Standby** ペインで、Azure への連続エクスポート用に設定されている Rapid Recovery Core のマシンを特定します。
3. 展開する仮想スタンバイマシンを表す行から （その他のオプション）をクリックし、**仮想マシンを展開** を選択します。

   Azure への展開ウィザード が表示されます。
4. **宛先** ページの **クラウドサービス名** ドロップダウンメニューで、Azure アカウントで使用可能なオプションから適切なクラウドサービスの名前を選択します。
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 仮想マシンへエクスポート 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 131. 仮想マシンパラメータ

オプション(O)	説明
クラウドサービス名	すでに利用しているクラウドサービスがある場合は、**クラウドサービス名** ドロップダウンメニューから、適切なクラウドサービス名を選択します。または、**クラウドサービス名** フィールドに一意で、分かりやすいクラウドサービス名を入力します。 クラウドサービス名は、Azure アカウントのリソースグループに関連付けられます。Azure の管理権限を持っている場合、Azure のマニュアルを参照して適切なアカウントを作成します。適切なクラウドサービスアカウントが表示されない場合、Azure 管理者からのサポートを依頼してください。 **NOTE:** Microsoft Azure サブスクリプションには、利用できるクラウドサービスの数にデフォルトで制限があります（通常は 25 です）。このサブスクリプションの制限を超えていないことを確認します。
展開名	既存の仮想マシンからクラウドサービスを選択した場合、このフィールドは自動的に入力されます。仮想マシンがないクラウドサービスを選択した場合は、この新しい展開のための名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。
宛先コンテナ	VM を格納するコンテナ名を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 63 文字で入力します。

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、**次へ** をクリックします。

表 132. 仮想マシンオプション

オプション	説明
仮想マシン名	仮想マシンの名前を入力します。 **NOTE:** 名前は、小文字、数字、およびハイフンのみを使用して、3 ~ 15 文字で入力します。
仮想マシンのサイズ	ドロップダウンリストから、適切な VM のサイズを選択します。 **NOTE:** Azure の設定と価格の詳細については、Azure ウェブサイトの「Virtual Machines の価格」ページを参照してください。Microsoft ウェブサイトのその他の有用なリファレンスへのリンクについては、 を参照してください。
エンドポイント (リモートアクセス設定)	
名前名前(N)	**リモートデスクトップ** または **SSH** を選択します。
プロトコル	**TCP** または **UDP** を選択します。
ポート	公開用ポートおよびプライベートポートはデフォルトで 3389 を使用します。必要に応じて変更します。
データ転送サーバポート	公開用ポートおよびプライベートポートはデフォルトで 8009 を使用します。必要に応じて変更します。
エージェントポート	公開用ポートおよびプライベートポートはデフォルトで 8006 を使用します。必要に応じて変更します。

11. **ディスク** ページでエクスポートするボリュームを選択し、**終了** をクリックしてウィザードを閉じ、展開を開始します。

NOTE: **イベント** ページでタスクを表示することにより、展開の進行状況を監視できます。

展開が完了したら、Azure アカウントで新規 VM が Azure の **マシンの表示 (クラシック)** ビューに表示されます。VM が利用可能になったら、料金を負担することになります。課金を続行しないためには、必要でない場合、展開された VM を削除します。この手順を繰り返して、最新の仮想エクスポートファイルのセットから VM を展開することができます。

エクスポートの管理

Core に連続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が **Virtual Standby** ページの行として表示されます。ここで、確立されている連続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、Core Console から連続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、1 回限りの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。

NOTE: Rapid Recovery では、Window 8、Window 8.1、Windows 10、Windows Server 2012、Windows Server 2012 R2、および Windows Server 2016 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 133. 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。
エクスポートタイプ	をクリックしてエクスポートのタイプを確認します。これにより、ESXi、VMware Workstation、Hyper-V、VirtualBox、Azure 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が表示されます。
最終エクスポート	をクリックしてエクスポートのタイプを確認します。これにより、最後のエクスポートの日時が表示されます。 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。
ターゲット	データをエクスポートしている仮想マシンとそのパス。

列	説明
設定	(その他のオプション) 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。 • **仮想マシンを展開**。Azure の連続エクスポートに限り、これによって Azure アカウントでエクスポートされたファイルがブータブル VM に変換されます。

表 134. 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。次のオプションが含まれます。 • **キャンセル**。現在の 1 回限りの仮想エクスポートをキャンセルします。 • **設定**。最大同時エクスポート設定を更新することができます。
ステータスインジケータ	現在のエクスポートのステータスが割合で表示されます。1 回限りのエクスポートのキューがない場合、この列には値がありません。
マシン名	ソースマシンの名前。
エクスポートタイプ	をクリックしてエクスポートのタイプを確認します。これにより、ESXi、VMware、Hyper-V、VirtualBox、Azure 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が表示されます。
スケジュールタイプ	をクリックしてスケジュールのタイプを確認します。これにより、エクスポートのタイプが 1 回限り または 連続 のいずれかで表示されます。
ターゲット	データをエクスポートしている仮想マシンとそのパス。

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、仮想スタンバイ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**。次回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. VM を Azure に導入するには、**仮想マシンを展開** を選択し、Azure への展開ウィザードで詳細を入力します。

   お使いの Azure アカウントに保存された最新の仮想エクスポートからのデータは、ブータブル VM として関連 Azure アカウント内に展開されます。
5. 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。
6. 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。
7. 新しい仮想スタンバイ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。表示されるウィザードを完了すると、選択した保護対象マシンの連続エクスポートが実行されます。特定の仮想マシンの仮想スタンバイ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 への連続エクスポートのセットアップ
   - Vmware Workstation への連続エクスポートのセットアップ
   - Hyper-V への連続エクスポートのセットアップ
   - VirtualBox への連続エクスポートのセットアップ
   - Azure への連続エクスポートの設定

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アについて

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アウェアです。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。アプリケーションア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
- 仮想マシンへの必要な時点での 1 回限りのエクスポートおよび連続エクスポート

NOTE: 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」のトピック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。保護対象マシンのバックアップが、Rapid Recovery Core に関連付けられたリポジトリ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、次の方法のいずれかを使用してデータをリストア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リストアして、リストア先マシンのボリュームを置き換えることができます。 詳細については、「データリカバリポイントからのボリュームのリストア」を参照してください。
- また、Linux エージェントでコマンドラインを使用して、Linux マシン上のボリューム全体をリカバリポイントからリストアすることもできます。コマンドラインの local_mount ユーティリティの使用の詳細については、「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。

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 (保護対象マシンの C ドライブなど) をリストアする場合、ベアメタル復元 (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、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ブータブルイメージを作成します。その後で、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。リカバリポイントを 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 マシンでのベアメタル復元の実行」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 マシンでのベアメタル復元の実行」を参照してください。

Rapid Recovery Agent リリース 6.2.1 に保護されている Linux マシンにソフトウェア RAID がある場合、リカバリポイントからソフトウェア RAID を復元できます。

NOTE: この機能は リリース 6.2.1 で導入されたため、それ以前の Agent バージョンで取得したスナップショットとは互換性がありません。Rapid Recovery Agent を リリース 6.2.1 以降にアップグレードしてから Rapid Recovery Core でスナップショットを取得した場合は、新しいスナップショットからソフトウェア RAID を復元できます。

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。リカバリポイント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 のエクスポート」を参照してください。

NOTE: 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、ベアメタル復元、および仮想エクスポートで Windows 8、Windows 8.1、Windows 10、Windows 2012、Windows Server 2012 R2、および Windows Server 2016 がサポートされています。バックアップおよびリカバリのサポート対象およびサポート対象外のボリュームタイプの詳細については、『*Rapid Recovery #########*』のトピック「Dynamic and basic volumes support limitations」(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の制限事項) を参照してください。

ファイルの検索と復元の機能について

Rapid Recovery のファイル検索および復元機能により、保護対象マシンのリカバリポイントにある 1 つまたは複数のファイルを検索できます。その後、ローカルディスクに結果のいずれかまたは複数を復元できます。

検索ガイドライン

Core Console の **ファイル検索** ページで、選択したマシンからのリカバリポイントのセットからファイルを検索できます。検索条件は基本および詳細の 2 つのグループに分かれています。

基本グループには、次のパラメータが含まれます。

- 検索するリカバリポイントを持つ保護対象マシン。
- 検索対象を開始時刻と終了時刻の間に作成されたリカバリポイントのみに制限する時間範囲。
- 検索するファイルの名前またはマスク。ワイルドカードの「?」を使用すると任意の単一文字、「*」を使用すると 0 または複数の文字に置き換えることができます。ただし、より具体的なファイル名を指定すればより具体的な結果が生成されます。
- 検索するディレクトリへのパスのリスト。

NOTE: すべての基本的な条件が必須です。ディレクトリを指定しない場合、Rapid Recovery では指定された保護対象マシンのすべてのボリュームが検索されます。

その他のオプション により詳細グループが表示されます。ここには次のパラメータが含まれます。

- 検索場所のサブディレクトリで再帰的に検索するか、指定された場所のみを検索するかを示すオプション。
- NTFS ボリューム上での検索速度を上げるアルゴリズムを実行する機能。
- 検索結果の数を管理しやすい総数に制限する機能。

NOTE: 特定の検索条件では、より迅速かつ的確な検索結果が生成されます。サブディレクトリを含めると（たとえば `C:\work\documents\accounting` とし `C:` としない）、検索を完了するのにかかる時間を短縮できます。また、制限的なファイルマスク（たとえば `invoice*.pdf` とし `in*.*` としない）を指定すると効果的です。

この機能では、要求したファイルが検出された後でもリカバリポイントや場所での検索が継続されるため、完了する前に検索を一時停止したり、停止することができます。複数の検索を同時に実行できますが、同時にそれらの検索を開始することはできません。たとえば、別のファイルを検索するために、最初の検索の進行中に 2 番目の検索を開始できます。ただし、同時に検索できるのは 1 台の保護対象マシンだけです。

NOTE: 前の例では、最初の検索を一時停止すると 2 番目の検索に使用できるメモリ容量が増えるため、2 番目の検索をより早く完了するのに役立ちます。一度に複数の検索を実行するとメモリが集中的に消費され、検索の完了までにかかる時間が増加します。

各検索は、ページ上にタブとして表示されます。検索が完了したら、タブを個別に閉じるか、すべてを一度に閉じることができます。

復元ガイドライン

ファイルを見つけたら、**ファイル検索** ページから直接復元することができます。

ファイルの検索および復元機能では、Core 上にある場所にのみ復元できるよう制限されています。ファイルを保護対象マシンに復元することはできません。

関連タスク

See also: ファイルの検索および復元

ファイルの検索および復元

ボリュームの代わりにファイルをリストアする場合、Rapid Recovery を使用してそのファイルを保護対象マシンのリカバリポイント間で検索できます。日付範囲やディレクトリなどの検索条件により、検索対象を関連するリカバリポイントの小さいグループに絞り込むことができます。

NOTE: 特定の検索条件では、より迅速かつ的確な検索結果が生成され、メモリの消費量も少なくなります。サブディレクトリを含めると（たとえば `C:\work\documents\accounting` とし `C:` としない）、検索を完了するのにかかる時間を短縮できます。また、制限的なファイルマスク（たとえば `invoice*.pdf` とし `in*.*` としない）を指定すると効果的です。

ファイルを見つけたら、検索結果のリストから直接復元することができます。

1. Rapid Recovery Core Console アイコンバーから **その他** ドロップダウンメニューをクリックして、**ファイル検索** を選択します。

   ファイル検索 ページが開きます。
2. **ファイル検索** ページで、特定の保護対象マシンのリカバリポイント内のファイルを検索するには、次の表に示す情報をすべて入力します。

表 135. ファイルの検索条件

保護対象マシンのリカバリポイント内からファイルを検索するための検索条件。

テキストボックス	説明
マシン	ドロップダウンリストから、検索する保護対象マシンを選択します。 **NOTE:** 一度に 1 つの保護対象マシンでのみリカバリポイントを検索することができます。
リカバリポイントの日付範囲	検索する最も古いリカバリポイントと最新のリカバリポイントの日時を指定します。この時間範囲内に作成されたリカバリポイントのみが検索されます。

テキストボックス	説明
	NOTE: デフォルトの期間は前月です。たとえば、2017 年 8 月 22 日 2:04 PM で検索を実行した場合、デフォルトの日付範囲は 2017 年 7 月 22 日 2:04 PM から 2017 年 8 月 22 日 2:04 PM までです。
ファイル名 (* と ? のワイルドカードを使用できます)	検索および復元するファイルのファイル名またはファイルマスクを入力します。ワイルドカードは不明な文字の代わりとして使用できます。 **NOTE:** ワイルドカードの「?」を使用すると任意の単一文字、「*」を使用すると 0 または複数の文字に置き換えることができます。
検索するディレクトリ	保護対象マシン上の 1 つまたは複数のディレクトリ一覧で、検索対象をこれらの場所のみに制限します。 **NOTE:** ディレクトリを指定しない場合、Rapid Recovery では指定された保護対象マシンのすべてのボリュームが検索されます。

3. 必要に応じて、**その他のオプション** をクリックしてから、次の表で説明する情報を入力します。

表 136. その他のファイル検索オプション

保護対象マシンのリカバリポイント内からファイルを検索するためのその他の検索条件。

テキストボックス	説明
サブディレクトリを含める	手順 3 で一覧表示されたディレクトリのすべてのサブディレクトリを検索します。デフォルトで有効。
NTFS ボリュームに対する高速検索アルゴリズムを使用	NTFS ボリュームをマウントせずにファイルシステムデータ構造の解析により検索します。この方法は高速であり、検索時のメモリ消費が少なくて済みます。デフォルトで有効。 **NOTE:** NTFS ボリュームの検索中に問題が発生した場合は、このオプションを選択せずに再度検索を試行します。
検索結果を制限する	表示する結果の最大数を入力します。デフォルトは 1000 です。

4. **検索を開始** をクリックします。

   検索が開始します。各検索はタブとして **検索結果** の下に表示されます。各タブのボタンを使用して検索を一時停止するか停止することができます。またはタブの **X** をクリックして検索を削除できます。複数の検索を同時に実行できます。
5. 検索結果から、復元するファイルを選択します。
6. **リストア** をクリックします。

   ファイルをリストア ダイアログボックスが開きます。
7. **場所** には、Core がインストールされて実行されているマシン上にある、リストアしたファイルの保存先のパスを入力します。
8. **リストア** をクリックします。

   選択したファイルは指定された宛先パスに、保護対象マシンでそれが表示されていた元のディレクトリツリー構造で復元されます。

関連概念

See also: ファイルの検索と復元の機能について

データリカバリポイントからのボリュームのリストア

マシンのリストア ウィザードを使用して、Rapid Recovery Core に保存されたリカバリポイントから保護対象マシン上のボリュームをリストアできます。

NOTE: 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。

NOTE: Rapid Recovery では、EISA パーティションで設定されたマシンの保護およびリカバリがサポートされています。Windows リカバリ環境 (Windows RE) を使用する Windows 8、Windows 8.1、Windows Server 2012、Windows Server 2012 R2、および Windows Server 2016 マシンもサポートされます。

Rapid Recovery Core Console の任意の場所から、Rapid Recovery ボタンバーの **リストア** アイコンをクリックして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、Core 上で保護されているマシンのうち、どのマシンをリストアするのかを指定し、リストアするボリュームに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 **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て、**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、トピック リカバリポイントからのボリュームのリストア の 手順 5 に従って開始します。

また、コマンドラインを使用して、Linux マシン上のリカバリポイントからリストアすることもできます。詳細については、「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」のトピックを参照してください。

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、またはブート CD を使用してリカバリポイントからリストアする場合、ベアメタル復元 (BMR) を実行する必要があります。BMR については、「Windows マシンのベアメタル復元について」を参照してください。また、Windows の前提条件については「Windows マシンに対してベアメタル復元を実行するための前提条件」を、Linux オペレーティングシステムの前提条件については「Linux マシンに対してベアメタル復元を実行するための前提条件」を参照してください。各オペレーティングシステムのロードマップの説明に従って、Core Console から BMR 機能を使用できます。また、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。この手順では、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ベアメタル復元の実行を実行するよう指示されます。

リカバリポイントからのボリュームのリストア

リカバリポイントからボリュームを復元するには、マシンが Core 上にてボリュームレベルで保護されていて、Core に復元操作を実行するリカバリポイントが含まれている必要があります。

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. 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 **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。
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、保護対象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、このプロセスではベアメタル復元 (BMR) が考慮されます。BMR については、「ベアメタル復元」を参照してください。

     NOTE: BMR を実行する場合、リストアする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 マシンに対してベアメタル復元を実行するための前提条件」および「Linux マシンに対してベアメタル復元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。

     NOTE: 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 マシンでのベアメタル復元の実行に進みます。
     - 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「Windows マシンでのベアメタル復元の実行」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 マシンでのベアメタル復元の実行に進みます。
     - 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 137. 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「Windows マシンでのベアメタル復元の実行」の手順 9 に進みます。

   NOTE: 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 8.1、Windows 10 (Enterprise または Pro のみ) 、Windows Server 2012、Windows Server 2012 R2、または Windows Server 2016 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。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ベアメタル復元はサポートされません。詳細については、「*Rapid Recovery* ####################」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、**Live Recovery** を選択します。

      Rapid Recovery の Live Recovery 即時リカバリテクノロジを使用すると、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。

      CAUTION: 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 Oracle データベース、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自動的に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。それ以外の場合は、このオプションをオフにします。

    NOTE: 適切な VSS ライターは、データベースのスナップショットをバックアップモードで取得できます。自動的にすべてのデータベースを再マウントしないことを選択した場合は (デフォルトのオプション) 、リストア後に手動でデータベースを起動する必要があります。
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。

    WARNING: 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。

一部のファイルには、管理者権限を必要とするファイルアクセス制限があります。特に Windows Server 2012 以降のオペレーティングシステムの場合、リストアを試みるユーザーは、権限付きのリストアを正常に行うための適切な NTFS 権限を持っている必要があります。たとえば、完全な NTFS 権限をマウントポイントからコピーするためには、ユーザーに (NTFS のフル権限を持つ) 管理者権限が必要です。

NOTE: 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。

   NOTE: 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復元

リストアは、マシン上のボリュームをリカバリポイントからリストアするプロセスです。サーバークラスタの場合、ノードレベルまたはマシンレベルでリストアを実行します。本項では、クラスタボリュームのリストアを実行するためのガイドラインを示します。

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、次の手順を実行します。

1. 1 つを除くすべてのノードの電源をオフにします。
2. 「データリカバリポイントからのボリュームのリストア」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」の説明に従って、マシンの標準 Rapid Recovery 手順でリストアを実行します。
3. リストアが完了したら、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、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、次の手順を実行します。

1. 1 つを除くすべてのノードの電源をオフにします。
2. 「データリカバリポイントからのボリュームのリストア」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」の説明に従って、マシンの標準 Rapid Recovery 手順でリストアを実行します。
3. リストアが完了したら、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。

   NOTE: 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。自動的に、またはクラスタサービス機能を使用して、これを再生成できます。

接続されているアーカイブからの復元

アーカイブからデータを復元するには、次の 2 つの方法があります。ベアメタル復元 (BMR) のソースとしてアーカイブを使用することができます。またはアーカイブを接続し、アーカイブからリカバリポイントをマウントし、アーカイブされたデータを復元することができます。

アーカイブを接続する場合は、Core Console の アーカイブ ページにある 接続されているアーカイブ の下に表示され、アーカイブの内容は左のナビゲーション領域からアクセス可能になります。内容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。このため、リカバリポイントをマウントし、リカバリするアイテムの場所を確認し、Windows エクスプローラを使用して宛先にアイテムをコピーして貼り付けることによって、現在保護されているマシンと同じようにリカバリポイントにアクセスできます。

リポジトリへのアーカイブのインポートではなく、接続されているアーカイブからの復元には利点があります。

- 接続されているアーカイブからの復元では、アーカイブ全体をリポジトリにインポートする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、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内の最も古いアイテムである可能性が高いため、保持ポリシーに基づいて、次回の夜間ジョブ中にロールアップされる可能性があります。（ただしこのアクションではリカバリポイントがアーカイブから削除されることはありません。翌日リカバリポイントの再インポートができます。）
- 最後に、Core は、アーカイブを分離した後でも、アーカイブとの接続の関連付けを記憶し、後でアーカイブをもう一度接続する場合、簡単にすばやく接続できます。

  接続を削除することにより、関連付けを削除することができます。

接続されているアーカイブからデータを復元するには、関連リンクを使用して、次のステップを実行します。

NOTE: 接続されているアーカイブからの復元手順では、ロールアップされたリカバリポイントのアーカイブがすでに存在することを前提としています。

1. アーカイブを接続します。
2. 復元するデータを含むリカバリポイントをマウントします。
3. 以下のいずれかの方法を使用してデータを復元します。
   - リカバリポイントからファイルまたはフォルダなどのデータを復元します。
   - リカバリポイント全体を復元します。
   - 仮想マシンにリカバリポイントをエクスポートします。

See also: アーカイブについて
See also: アーカイブのアタッチ
See also: アーカイブのインポート
See also: リカバリポイントのマウント
See also: 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
See also: リカバリポイントからのボリュームのリストア
See also: Rapid Recovery を使用した仮想マシンへのエクスポート
See also: アーカイブからの BMR の実行

Rapid Recovery によるメールのリストア

Rapid Recovery のメールのリストア機能を使用すると、保護対象の Exchange Server マシンのデータストアから、メールボックス、フォルダ、アイテム（メッセージ、カレンダーイベント、連絡先など）をリストアできます。選択した内容を、リカバリフォルダ、元のソース、または 1 つ以上の PST ファイルにリストアできます。

メールのリストア ページには、Rapid Recovery Core Console の **その他**（...）メニューからアクセスできます。そのページから次のアクションを実行できます。

- Exchange データベースを開く
- 開いたデータベースからアイテムをリストアする
- データベースを閉じる
- 開いたデータベースでアイテムを検索する

詳細については、次を参照してください。Rapid Recovery で Exchange データベースを開くおよび「Rapid Recovery によるメールアイテムのリストア」を参照してください。

メールのリストアの前提条件

メールアイテムをリストアするには、次の前提条件が満たされている必要があります。

- Outlook 2007 以降が Core マシンにインストールされている。
- 少なくとも 1 つのプロファイルが Microsoft Outlook で設定さています。
- Outlook プロファイルにフルコントロール権限 (「Send As」および「Receive As」権限を含む) が付与されている。詳細については、次を参照してください。。
- Rapid Recovery に関連付けられた Outlook プロファイルの Outlook Exchange キャッシュモードオプションが無効になっている。
- Core マシンが Exchange データベースと同じドメインに属している。
- 必要な Exchange データベースが開かれていて、Rapid Recovery Core Console の **メールのリストア** ページを表示している。詳細については、次を参照してください。Rapid Recovery で Exchange データベースを開く。

適切な権限と Core マシンにインストールされた Outlook のインスタンスがないと、Exchange Server が Rapid Recovery Core によって保護されていても、Exchange アイテムのリカバリを実行できません。

Rapid Recovery で Exchange データベースを開く

このタスクを開始する前に、次の前提条件が満たされていることを確認してください。

- Outlook 2007 以降が Core マシンにインストールされている。
- Core マシンが Exchange データベースと同じドメインに属している。
- 適切な権限が、Exchange で設定されている。詳細については、を参照してください。

Rapid Recovery では、インタフェースを離れることなく、メールアイテムをリストアできます。メールアイテムは、保護対象 Exchange Server マシンのリカバリポイント内の Exchange データベースに存在します。メールアイテムは、Exchange データベースを開くウィザードを使用して開くことができます。

1. ★Rapid Recovery Core Console から。 で、その他 (**...**) メニューをクリックし、**メールのリストア** をクリックします。
2. **メールのリストア** ページで、メールアイテムが格納されている Exchange データベースにアクセスするには、**データベースを開く** をクリックします。

Exchange データベースを開くウィザードが開きます。

3. ウィザードの**場所** ページでは、保護対象マシンから、または現在のマシンやファイル共有などのローカルパスからデータベースを開くことができます。
   - **保護対象マシンから開く**：**次へ** をクリックし、このタスクの次の手順に進みます。
   - **ローカルパスから開く**：場所に関する次の情報を入力し、**終了** をクリックします。
     - データベースファイルのパス
     - ログのパス
     - システムのパス
4. **マシン** ページで、Exchange データベースを格納している保護対象マシンを選択し、**次へ** をクリックします。
5. **リカバリポイント** ページで、データベースを開く時点のリカバリポイントを選択し、**次へ** をクリックします。
6. **データベース** ページで、開く Exchange データベースを選択し、**終了** をクリックします。

   Rapid Recovery は、選択したデータベースを開き、**メールのリストア** ページに表示します。メールボックスとフォルダは、左側の展開可能なナビゲーションツリーにリストされます。フォルダ内のアイテムは右側に表示されます。

   NOTE: Rapid Recovery が Exchange データベースを開くのにかかる時間は、データベースのサイズによって異なります。

開いているデータベースからアイテムをリストアする方法については、「Rapid Recovery によるメールアイテムのリストア」を参照してください。

Rapid Recovery によるメールアイテムのリストア

このタスクを開始する前に、メールのリストアを完了するための前提条件を満たされていることを確認してください。詳細については、次を参照してください。メールのリストアの前提条件。

Rapid Recovery のメールのリストア機能を使用すると、保護対象 Exchange Server マシンのデータストアから、メールボックス、フォルダ、アイテム (メッセージ、カレンダーイベント、連絡先など) をリストアできます。選択した内容を、リカバリフォルダ、元のソース、または 1 つ以上の PST ファイルにリストアできます。Rapid Recovery Core Console からメールアイテムをリストアするには、次の手順を実行します。

1. **メールのリストア** ページの Exchange データベースを開く から、リストアするアイテムを選択し、**メールのリストア** アクションバーで **リストア** をクリックします。

   電子メールのリストアウィザード が開きます。
2. **リストアセッション** ページで、次のいずれかのオプションを入力し、**次へ** をクリックします。
   - 初めてメールアイテムをリストアする場合は、リストアセッションの表示名と Outlook 認証情報を入力します。今後のリストアでは、このセッションを選択できます。
   - 以前にリストアセッションを作成している場合は、次のいずれかのオプションを選択します。
     - **既存のリストアセッションを使用** を選択して、ドロップダウンリストからセッションを選択します。
     - **新しいリストアセッションを作成** を選択して、リストアセッションの表示名と Outlook 認証情報を入力します。
3. **宛先** ページで、次のオプションからリストアされるアイテムのターゲットの場所を選択し、**次へ** をクリックします。

表 138. メールのリストア先

オプション	説明
リカバリフォルダにリストアする	選択したアイテム（フォルダ階層を含む）を、任意のオンラインメールボックス内のリカバリフォルダにリカバリします。手順 4 に進みます。
元の場所にリストアする	選択したアイテム（フォルダ階層を含む）を、元のオンラインデータストア内のメールボックスに送信します。手順 5 に進みます。
PST ファイルにリストアする	Personal Storage Table（PST）ファイルを作成するか、既存の PST ファイルに書き込むことで、選択したアイテム（フォルダ階層を含む）を保存します。手順 6 に進みます。
PST ファイルにリストアする（メールボックスごとに異なるファイル）	各メールボックスを Personal Storage Table（PST）ファイルとして個別に保存します。手順 6 に進みます。

4. **リカバリフォルダにリストアする** を選択した場合は、**設定** ページで、ドロップダウンリストから **プロファイル** を選択し、Outlook アドレス帳を参照し選択してから、手順 7 に進みます。

   必要に応じて、**詳細設定オプションを表示** を選択して、次のオプションを使用してリストアをさらにカスタマイズします。

表 139. 詳細メールリストアオプション

オプション	説明
エラー処理	リストアプロセス中に発生するすべてのエラーを特定し、管理する方法を決定します。次のいずれかのオプションを選択します。 • **ログと続行**。ログにエラーメッセージを収集し、リストアプロセスを続行します。 • **ユーザーに通知**。エラーが発生すると、リストアを一時停止し、リストアを続行するか中止するかを選択するメッセージが アクティブなタスクをモニタ ダイアログに表示されます。 • **リストアを中止**。エラーが発生するとリストアプロセスが終了します。
削除済みオブジェクトをリストア	Exchange 2010、2013、および 2016 のデータベースの場合は、完全に削除されたアイテムをリストアします。 Exchange 2007 データベースの場合は、現在のフォルダから取り消したアイテムをリストアします。

オプション	説明
電子メールルールをリストア	データがバックアップされた時点でユーザーが所定の位置の持っていたルールをリストアします。

5. **元の場所にリストアする** を選択した場合は、**設定** ページで、ターゲットの Outlook **プロファイル** を選択し、次のオプションから **リストアタイプ** を選択してから、手順 7 に進みます。
   - **差分のみをリストア**。リストアされるアイテムが宛先フォルダに既に存在するかどうかを確認し、重複するアイテムが存在しない場合にのみリストアを行います。差分リストアとしても知られています。
   - **重複エントリの作成**。既存のアイテムに上書きせずに、選択したすべてのアイテムをリストアします。その結果、既存のアイテムは重複することになります。
   - **より最新である場合は上書きする**。オンラインデータストア内に存在しない、日付が新しいアイテムをリストアします。オンラインのデータストア内に存在するアイテムもリストアしますが、これらのアイテムは Exchange データベースのコピー内のアイテムよりも古くなります。

   必要に応じて、**詳細設定オプションを表示** を選択して、次のオプションを使用してリストアをさらにカスタマイズします。

表 140. 詳細メールリストアオプション

オプション	説明
エラー処理	リストアプロセス中に発生するすべてのエラーを特定し、管理する方法を決定します。次のいずれかのオプションを選択します。 • **ログと続行**。ログにエラーメッセージを収集し、リストアプロセスを続行します。 • **ユーザーに通知**。エラーが発生すると、リストアを一時停止し、リストアを続行するか中止するかを選択するメッセージが アクティブなタスクをモニタ ダイアログに表示されます。 • **リストアを中止**。エラーが発生するとリストアプロセスが終了します。
削除済みオブジェクトをリストア	Exchange 2010、2013、および 2016 のデータベースの場合は、完全に削除されたアイテムをリストアします。 Exchange 2007 データベースの場合は、現在のフォルダから取り消したアイテムをリストアします。
電子メールルールをリストア	データがバックアップされた時点でユーザーが所定の位置の持っていたルールをリストアします。
ユーザー権限をリストア	パブリックフォルダ用のカスタム権限をリストアします。 **NOTE:** このオプションは、パブリックフォルダを元の場所にリストアする場合にのみ使用できます。権限のリストアを選択しない場合は、デフォルトのフォルダ権限がコンテンツにリストアされます。

6. **PST ファイルにリストアする** または **PST ファイルにリストアする (メールボックスごとに異なるファイル)** を選択した場合、**設定** ページで、次の選択を完了してから、手順 7 に進みます。
   a. **プロファイル**。ドロップダウンリストから Outlook プロファイルを選択します。
   b. **プライマリ PST ストレージ**。パスを入力するか、既存のファイルを選択して、PST ファイルの最初の宛先フォルダを特定して選択します。
   c. **オーバーフロー PST ストレージ (オプション)**。プライマリの宛先で PST ファイル用の容量が不足している場合、PST ファイルのセカンダリの宛先を選択します。

NOTE: オーバーフローの場所として、最初の場所と同じディスクを割り当てないでください。

必要に応じて、**詳細設定オプションを表示** を選択して、次のオプションを使用してリストアをさらにカスタマイズします。

表 141. 詳細メールリストアオプション

オプション	説明
エラー処理	リストアプロセス中に発生するすべてのエラーを特定し、管理する方法を決定します。次のいずれかのオプションを選択します。 • **ログと続行**。ログにエラーメッセージを収集し、リストアプロセスを続行します。 • **ユーザーに通知**。エラーが発生すると、リストアを一時停止し、リストアを続行するか中止するかを選択するメッセージが アクティブなタスクをモニタ ダイアログに表示されます。 • **リストアを中止**。エラーが発生するとリストアプロセスが終了します。
削除済みオブジェクトをリストア	Exchange 2010、2013、および 2016 のデータベースの場合は、完全に削除されたアイテムをリストアします。 Exchange 2007 データベースの場合は、現在のフォルダから取り消したアイテムをリストアします。

7. **終了** をクリックします。

アイテムは、選択した宛先にリストアされます。イベント ページでジョブの進行状況を監視できます。

ベアメタル復元

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 マシンにベアメタル復元（BMR）を実行する機能が備わっています。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。ベアメタル復元は、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。

NOTE: 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ベアメタル復元（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、および SUSE Linux Enterprise Server（SLES）です。詳細については、「*Rapid Recovery ##########*」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 で BMR を実行すると、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、高い移植性が得られます。

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。ベアメタル復元が完了したら、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。

ベアメタル復元は、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。

仮想マシンの復元

ベアメタル復元（BMR）は仮想マシン（VM）でサポートされますが、物理マシンで BMR を実行するより、仮想マシンに VM エクスポートを実行したほうが簡単です。仮想マシン用の VM エクスポートの実行の詳細については、「Rapid Recovery を使用した仮想マシンへのエクスポート」を参照してください。

BMR を Windows マシンで実行する場合は、前提条件を含め、Windows に固有のトピックを参照してください。詳細については、「Windows マシンでのベアメタル復元の実行」を参照してください。

また、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。これを実行するには、手順 データリカバリポイントからのボリュームのリストア から始め、手順に従って、Windows マシンでのベアメタル復元の実行 に進みます。

Linux マシンで BMR を実行するには、Linux マシンでのベアメタル復元の実行を参照してください。local_mount コマンドラインユーティリティを使用した BMR の実行に加え、Core Console UI からでも BMR を実行できるようになりました。ロードマップでは、両方の方法が考慮されています。

Windows マシンでのベアメタル復元の実行

Windows マシンに対してベアメタル復元を実行するには、次のタスクを実行します。

- Windows ブートイメージの作成。このブート CD 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。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。
  - 宛先ドライブの起動に物理メディアが必要な場合は、ブート CD の ISO イメージをメディアに転送する必要があります。詳細については、「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。
  - どの場合にも、宛先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を起動する必要があります。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。

    NOTE: この処理では、ブート CD を作成 ダイアログボックスからブート CD イメージを管理する方法について説明します。マシンのリストア ウィザードからも、ウィザードの ブート CD ページから開始して、これらの手順を実行できます。この機能には、ウィザードの 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」を指定するとアクセスできます。
- Windows 用のベアメタル復元の起動。ブート CD から宛先マシンを起動したら、BMR を起動できます。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。次のタスクが含まれます。
  - Core のリカバリポイントからリストアを開始します。詳細については、「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。
  - ボリュームをマップします。詳細については、「ベアメタル復元のためのディスクのマップについて」を参照してください。
  - 異種のハードウェアにリストアするときに、必要なストレージドライバとネットワークドライブがブート CD に存在しない場合は、ポータブルメディアデバイスからドライバをロードする必要があることがあります。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。
- マシンのリストア ウィザードから BMR の実行。必要に応じて、すべてのサブタスクを含め、Windows ブートイメージを管理するプロセスや BMR を起動するプロセスを マシンのリストア ウィザードから実行

できます。ウィザードの開始については、「データリカバリポイントからのボリュームのリストア」の手順 1 ～ 5 を参照してください。

- ベアメタル復元の確認。ベアメタル復元の開始後、進捗状況を確認および監視できます。詳細については、「ベアメタル復元の確認」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。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。
  - 処理が完了したら、リストアされたサーバを起動できます。詳細については、次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
  - 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と起動の問題の修復を参照してください。

Windows マシンに対してベアメタル復元を実行するための前提条件

Windows マシンに対してベアメタル復元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。

  NOTE: 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、『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ベアメタル復元の実行

リストアウィザードを使用して、ブート CD を作成し、ベアメタル復元 (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 マシンに対してベアメタル復元を実行するための前提条件またはLinux マシンに対してベアメタル復元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 マシンでのベアメタル復元の実行」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。

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ベアメタル復元を開始します。

NOTE: 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。

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に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。

   NOTE: 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) 。

NOTE: 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 142. 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 143. UltraVNC 接続資格情報

オプション	説明
パスワード(A)	UltraVNC アカウントのパスワード。
ポート(O)	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 144. UltraVNC 接続

オプション	説明
パスワード(A)	この UltraVNC 接続のパスワードを指定します。
ポート(O)	この UltraVNC 接続のポートを指定します。

オプション	説明
	デフォルトポートは 5900 です。

10. 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。
11. 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。
    a. 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。
    b. 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。
    c. 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。
    d. 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。
    e. 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。

    NOTE: 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。
12. **次へ** をクリックします。
13. 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。

      NOTE: 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。
14. 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 145. 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。

15. **次へ** をクリックします。
16. 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。
    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、**自動** を選択します。
    b. 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。

NOTE: 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。

NOTE: 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。

CAUTION: 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 Oracle、SQL Server、または Microsoft Exchange の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、およびジャーナルページ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 のベアメタル復元には、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 でパラメータ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 マシンに対してベアメタル復元（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 ファイルを作成します。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環境である 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

ブート CD イメージには、サーバのドライブを認識するためのストレージドライバと、ネットワークを介して Rapid Recovery Core と通信するためのネットワークアダプタドライバが必要です。

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の導入が必要となる場合があります。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、ターゲットサーバ上のリカバリコンソール、ネットワークアダプタ、およびストレージ間の相互運用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ベアメタル復元を実行する場合は、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、ベアメタル復元（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。

NOTE: 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

NOTE: 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り、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。

NOTE: 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。

NOTE: 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。

NOTE: 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。

   a. 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。
   b. 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。
   c. 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。
   d. 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。

   e. 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。
   f. 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、およびジャーナルページ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、ベアメタル復元を実行するサーバで、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。

NOTE: 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。

1. 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 Quest 画面が表示されます。
2. Rapid Recovery Universal Recovery Console (URC) ユーザーインタフェースを開くには、画面上部にある Quest 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。

   NOTE: 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。

   NOTE: 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。

   NOTE: 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ら、リカバリポイントを選択し、ベアメタル復元プロセスを続行します。

BMR への Universal Recovery Console の使用

Windows 用のベアメタル復元（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 マシンに対してベアメタル復元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
- ベアメタル復元のためのディスクのマップについて
- Universal Recovery Console を使用したドライバのロード

この処理は、Windows マシンでのベアメタル復元の実行の手順です。

Universal Recovery Console ツールについて

Universal Recovery Console（URC）には、ベアメタル復元（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 Quest 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**：このオープンソースブラウザでは、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にアクセスできます。
- **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になることがあります。
- **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、ベアメタル復元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 マシンでのベアメタル復元の実行の手順です。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。

   Quest スプラッシュ画面が表示されます。
6. URC を起動するには、**Quest 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ケットを探します (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。

   Quest スプラッシュ画面が表示されます。
2. URC を起動するには、**Quest 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ケットを探します (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）がベアメタル復元（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。

NOTE: 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 マシンでのベアメタル復元の実行の手順です。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 マシンでのベアメタル復元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 マシンに対してベアメタル復元を起動する 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 146. 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ベアメタル復元のためのディスクのマップについてに進みます。

ベアメタル復元のためのディスクのマップについて

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

CAUTION: 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 8.1、Windows 10 (Enterprise または Pro のみ) 、Windows Server 2012、Windows Server 2012 R2、または Windows Server 2016 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。**

CAUTION: ストレージスペースのディスク構成のベアメタル復元はサポートされません。詳細については、「」を参照してください。 *Rapid Recovery* ####################

このタスクは、Windows マシンでのベアメタル復元の実行の手順です。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 マシンでのベアメタル復元の実行の手順でもあります。これは、Linux 用のベアメタル復元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ベアメタル復元 (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。

   NOTE: 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。

   CAUTION: 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 SP 1)」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。

   NOTE: ベアメタル復元 (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** 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. リストアを開始するには、**リストアを開始** をクリックします。

   CAUTION: リストアを開始 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リストアできます。

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、リストア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 147. 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(U)	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 • Powered by OpenStack • Rackspace クラウドファイル • Google クラウド

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。
        - 領域
        - ユーザー(U)
     2. 次のいずれかのオプションを選択します。
        - パスワード(A)
        - 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

◦ Google クラウドアカウントの場合は、次の手順を実行します。

1. 次の資格情報を入力します。
   - 証明書ファイル
   - プライベートキー
2. 次の情報を入力します。
   - プロジェクト ID
   - サービスアカウントの電子メール
3. コンテナ名 フィールドで、ドロップダウンリストから適切なコンテナを選択します。
   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。

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。

   NOTE: 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。

NOTE: 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。

NOTE: ベアメタル復元 (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。

   NOTE: 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、ベアメタル復元（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ベアメタル復元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、ベアメタル復元（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 マシンでのベアメタル復元の実行

Rapid Recovery では、システムボリュームのリストアを含め、Linux マシンのベアメタル復元（BMR）を実行できます。`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。

CAUTION: Rapid Recovery **では、カーネルが 3.10 以上の場合にのみ、ext2 パーティションタイプがサポートされます。それ以前のカーネルを使用している場合は、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 ext3、ext4、または XFS に変換してください。**

CAUTION: BMR の実行後初めてリストアされた Linux マシンを起動する際に、Rapid Recovery がリストア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 マシンに対してベアメタル復元を実行するには、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。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。
  - BMR のブートイメージを取得する場合は、LiveDVD バージョンが使用している Core のバージョンに一致していることを確認してください。詳細については、「Linux 用のブート ISO イメージについて」および「Linux 用のブート ISO イメージのダウンロード」を順に参照してください。
  - 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。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。
  - どの場合にも、宛先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を起動する必要があります。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。
  - 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。詳細については、「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。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。
  - 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。詳細については、「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。詳細については、「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。詳細については、「コマンドラインを使用して Linux マシンに対してベアメタル復元を起動する」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、リストア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リストアされます。
- Linux 用のベアメタル復元の起動。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 ユーザーインタフェースからこの操作を実行するか、コマンドラインから local_mount ユーティリティを使用して行うかによって、必要なタスクが異なります。詳細については、「Linux 用のベアメタル復元の開始」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。詳細については、「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。
  - 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。詳細については、「ベアメタル復元のためのディスクのマップについて」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 マシンに対してベアメタル復元を起動する」を参照してください。

- ベアメタル復元の確認。ベアメタル復元の開始後、進捗状況を確認および監視できます。詳細については、「コマンドラインからのベアメタル復元の確認」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。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。
  - 処理が完了したら、リストアされたサーバを起動できます。詳細については、「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と起動の問題の修復を参照してください。

Linux マシンに対してベアメタル復元を実行するための前提条件

Linux マシンに対してベアメタル復元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 ##########*』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。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、Quest Data Protection 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 用のベアメタル復元には、Live DVD ブートイメージが必要です。これは、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 サーバを起動する必要があります。

NOTE: 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 マシンでのベアメタル復元の実行 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
- メディアへの Live DVD の ISO イメージの保存
- Live DVD のロードおよびターゲットマシンの起動
- Rapid Recovery Core から BMR ターゲットへの接続

Linux 用のブート ISO イメージについて

Linux マシンに対してベアメタル復元（BMR）を実行するときの最初の手順として、Rapid Recovery ライセンスポータルから Linux 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、Screen 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全体をリストアするために使用される環境です。

NOTE: 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

Linux マシンの Bare-Metal Restore を完了するには、現在の Rapid Recovery のバージョンと一致する Live DVD の ISO イメージが必要です。現在の Live DVD のバージョンは、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、Quest Data Protection サポート にお問い合わせください。

NOTE: Rapid Recovery ライセンスポータル の詳細は、『*Rapid Recovery ##################*』を参照してください。

このタスクは、Linux マシンでのベアメタル復元の実行の手順です。これは、Linux ブートイメージの管理の処理の一部です。

Live DVD ISO イメージをダウンロードするには、この手順のステップを実行します。

1. Rapid Recovery ライセンスポータル（https://licenseportal.com）にログインします。
2. 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。

   ダウンロード ページが表示されます。
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。

   NOTE: 仮想マシンからリストアする場合、イメージをネットワークの場所に保存し、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します。
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 マシンでのベアメタル復元の実行の手順です。これは、Linux ブートイメージの管理の処理の一部です。

1. 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 のエクスポート」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 マシンでのベアメタル復元の実行の手順です。これは、Linux ブートイメージの管理の処理の一部です。

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。

   NOTE: 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、ベアメタル復元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 用のベアメタル復元の開始」を参照してください。
- 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 マシンに対してベアメタル復元を起動する」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。

リストアの起動は、local_mount 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 マシンでのベアメタル復元の実行 のステップです。

次のタスクを実行できます。

関連タスク

See also: 宛先ドライブでのパーティションの作成
See also: 宛先ドライブでのパーティションのフォーマット
See also: 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、ベアメタル復元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。

CAUTION: 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 マシンでのベアメタル復元の実行の手順です。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。

   NOTE: 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

ベアメタル復元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 マシンでのベアメタル復元の実行の手順です。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。

   NOTE: 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 マシンでのベアメタル復元の実行の手順です。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 マシンに対してリストアを実行できます。詳細については、Linux 用のベアメタル復元の開始を参照してください。

Linux 用のベアメタル復元の開始

Linux 用のベアメタル復元（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 マシンに対してベアメタル復元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 からリストアするか、または local_mount を使用してコマンドライン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 マシンでのベアメタル復元の実行の手順です。

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
- ベアメタル復元のためのディスクのマップについて

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 マシンに対してベアメタル復元を起動する

Screen ユーティリティの開始

Live DVD には、Live DVD から Universal Recovery Consol 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。

NOTE: 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。

1. 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 マシンに対してベアメタル復元を起動する

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。

NOTE: 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。

NOTE: 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 マシンでのベアメタル復元の実行の手順です。これは、コマンドラインを使用して Linux マシンに対してベアメタル復元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 148. Rapid Recovery Core 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。	可
ドメイン(D)	Rapid Recovery Core のドメイン。これは任意です。	不可
ユーザー	Core の管理ユーザーのユーザー名です。	可

テキストボックス	説明	必須
パスワード(A)	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。	可

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>
```

NOTE: 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>
```

CAUTION: 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。

NOTE: 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。

NOTE: 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 (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。

NOTE: 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ベアメタル復元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

コマンドラインを使用してリカバリポイントからリストアする前に、データのリストア先となるディスクをマウント解除する必要があります。

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。

NOTE: 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、データリカバリポイントからのボリュームのリストアを参照してください。

CAUTION: 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 マシンでのベアメタル復元の実行」を参照してください。

1. 次のように、ルートとして Rapid 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。

   ```
   lm
   ```

3. プロンプトが表示されたら、Rapid Recovery Core 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。

   この Rapid Recovery Core 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>
   ```

   NOTE: 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されて、保護対象マシン番号 `2` に対して `lr` 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
     ```

NOTE: 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、ベアメタル復元を実行する場合は、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 用のベアメタル復元の開始」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)。

ベアメタル復元の確認

ベアメタル復元 (BMR) の実行後、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。

- 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 (ベアメタル復元を含む) 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、およびジャーナルページを使用したイベントの表示」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。

NOTE: 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 マシンでのベアメタル復元の実行の手順です。これは、ベアメタル復元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ーからブート CD を取り出すか、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 で識別できる必要があります。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、ターゲットサーバー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。ターゲットサーバー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。

   ターゲットサーバー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ベアメタル復元の確認

Quest では、次の手順を実行して、コマンドラインから完了したベアメタル復元を確認することをお勧めします。

このタスクは、Linux マシンでのベアメタル復元の実行の手順です。

- 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ベアメタル復元を実行したら、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 マシンでのベアメタル復元の実行の手順です。これは、コマンドラインからのベアメタル復元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。

NOTE: 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。

CAUTION: BMR の実行後初めてリストアされた Linux マシンを起動する際に、Rapid Recovery がリストア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 マシンでのベアメタル復元の実行の手順です。これは、コマンドラインからのベアメタル復元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。

   NOTE: 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]
   ```
   NOTE: `ls -l /dev/disk/by-uuid` コマンドを使用することもできます。
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
      ```

      NOTE: 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
      ```

      NOTE: 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。

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 Quest 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機能について説明します。

本項では、ロールアップを制御する保持ポリシーを管理する方法、および必要に応じてロールアップを強制実行する方法についても説明します。

データの保持、セカンダリストレージの階層化、およびアーカイブ

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。夜間ジョブの実行時 (特にロールアッププロセス中) 、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。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 はその後で古いリカバリポイントをロールアップ (結合) します。時間が経過するごとに、最も古いリカバリポイントが最終的に保持期間で定義された最長保持期間に達するにしたがい、リポジトリ内の古いリカバリポイントは、より新しいリカバリポイントに置き換えられます。

Rapid Recovery リリース 6.1.1 の時点では、リカバリポイントをプライマリ DVM リポジトリから、Quest の DR バックアップおよび重複排除のアプライアンスにある階層化リポジトリに再配置することもできます。これにより、プライマリリポジトリ内のストレージに空き領域が作られます。

この方法を使用して、リカバリポイントをセカンダリストレージに階層化するには、最初に Rapid Recovery Core に DR アプライアンスをリポジトリとして追加する必要があります。DR 上に新規セカンダリ階層化リポジトリを作成する詳細については、「階層化リポジトリの作成」を参照してください。次に、保護対象マシンレベルで、リカバリポイントをプライマリリポジトリからセカンダリリポジトリに移動する経過時間を、保持ポリシーで指定します。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」(特に手順 7 および 10) を参照してください。

NOTE: リカバリポイントが配置される場所 (ローカル DVM リポジトリか、 または DR バックアップアプライアンス上のセカンダリ階層化リポジトリか) に関係なく、リカバリポイントは保持ポリシーの適用対象であり、ロールアップされます。保持期間よりも古いリカバリポイントを保持する必要がある場合の方法の 1 つは、アーカイブすることです。もう 1 つの方法は、ロールアップを無効にするか、または関連する保護対象マシンの保持期間を延長します。

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でのリカバリポイントの完全なセットを含む単一ファイルです。Core Console からアーカイブされた情報に後でアクセスすることができます。リポジトリ内のリカバリポイントとは異なり、アーカイブ内のリカバリポイントはロールアップされません。

アーカイブは、Core のバックアップ、レプリケーションデータのリモートレプリカ Core へのシーディングなどのコンプライアンスデータを保持することや、より長い期間バックアップを保持しながらも、最近のビジネスクリティカルなトランザクションを保有するために Core 内のスペースを節約することに役立ちます。

アーカイブの詳細については、「アーカイブあーかいぶ」を参照してください。

保持ポリシーの管理

保持ポリシーは、ロールアップを開始するまでにリカバリポイントを保持しておく Core の期間を決定するルールのセットです。保持ポリシーは、時間、日、週、月、年単位でロールアップするように設定できます。最大 6 つのルールを設定できます (デフォルトポリシーは 5 つのルールを設定) 。

5 分ごとの頻度 (DL1000 の場合は 1 時間に 1 回の頻度) でバックアップできるため、保持ポリシーの最初のルールは通常、すべてのリカバリポイントを保持する時間の長さを設定します。たとえば、25 分ごとにマシンをバックアップする場合、ロールアップが開始するまでにそのマシンのリポジトリには毎日 96 のリカバリポイントが保存されます。保持ポリシーを管理しないと、データ量によってリポジトリがすぐにいっぱいになる可能性があります。

NOTE: 管理者は、頻繁なバックアップがネットワークトラフィックに与える影響に留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する他の要因には、その他の転送 (レプリケーションなど) 、データの変更レート、ネットワークハードウェア、ケーブル、スイッチなどがあります。

Core はデフォルトの保持ポリシーでプリセットされています。デフォルトポリシーでは次のように保持されます。

- すべてのリカバリポイントを 3 日間
- 1 時間あたり 1 つのリカバリポイントを 2 日間
- 1 日あたり 1 つのリカバリポイントを 4 日間
- 1 週間あたり 1 つのリカバリポイントを 3 週間
- 1 か月あたり 1 つのリカバリポイントを 2 か月間
- 1 年あたり 1 つのリカバリポイントを X 年間 (デフォルトポリシーでは無効)

このデフォルトポリシーに基づく最も古いリカバリポイントは通常、92 日前のものです。デフォルトポリシーの実行日を経過したデータは削除されます。

Core レベルでの保持ポリシーの設定は、Core で保護されるすべてのマシンに自動的に適用されます。デフォルトポリシーは必要に応じて変更できます。

任意のマシンに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、「Core のデフォルト保持ポリシー設定の指定」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。

Core のデフォルト保持ポリシー設定の指定

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をレジストリに保存する期間を指定します。

Core の保持ポリシーは、夜間ジョブの 1 つのコンポーネントとして実行されるロールアッププロセスによって適用されます。その後、保持ポリシーで指定した期間を超えるリカバリポイントは、より長い期間をカバーするリカバリポイントに「ロールアップ」 (結合) されて、リカバリポイントの数が削減されます。保持ポリシーを夜間ベースで適用すると、古くなったバックアップが継続的にロールアップされます。最終的にその保持ポリシーで指定した要件に基づいて、最も古いリカバリポイントが削除されます。

ソース Core とターゲット Core で異なる保持設定を設定することができます。

NOTE: このトピックでは、Rapid Recovery Core 上の保持ポリシー設定のカスタマイズについてのみ説明しています。カスタマイズされた保持ポリシー設定を Core に保存する場合、この Core で保護されているすべてのマシンに適用できるデフォルト保持ポリシー設定を構成します。個々の保護対象マシンの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 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 設定のリストで **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** 見出しが表示されるまで下にスクロールします。

   夜間ジョブの Core 設定が表示されます。
3. **夜間ジョブ** で、 **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. 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、夜間ジョブ ペインで **ロールアップ** を選択し、**設定** をクリックします。

   Core のデフォルト保持ポリシーの **設定** ダイアログボックスが表示されます。
5. Core の保持ポリシーの設定は、いつでもデフォルト値にリストアできます。リストアするには、設定 ダイアログボックスの一番下にある **デフォルトにリストア** をクリックし、**はい** をクリックして確認します。

   すべての設定が、手順 6 の表に記載されているデフォルト値にリストアされます。
6. 次の表の説明に従って、リカバリポイントを保持するデフォルトスケジュールを入力します。最初の設定で、リポジトリに保存されたすべてのリカバリポイントのプライマリ保持期間を指定します。各追加設定を有効にすると、リカバリポイントがロールアップされる間隔を指定することで、より詳細なレベルの保持を指定できます。これらの設定は、リカバリポイントを維持する期間を定義します。

   保持ポリシーの各オプションを次の表に示します。

表 149. デフォルト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
すべてのリカバリポイントを n [保持期間] 保持…	リポジトリに保存されたすべてのリカバリポイントのプライマリ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。 次から選択できます。日、週、月、および 年
…さらに、1 時間あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 時間ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 2 日間です。日、週、月、および 年 から選択できます。 1 時間ごとのリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 日あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1日ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 4 日間です。日、週、月、および 年 から選択できます。 毎日のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 週間あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 週間ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 3 週間です。週、月、および 年 から選択できます。

テキストボックス	説明
	1 週間ごとのリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
...さらに、1 か月あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、 1 か月ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 2 か月です。月 および 年 から選択できます。 毎月のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
...さらに、1 年あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 年ごとに 1 つのリカバリポイントがこの設定により指定した年数保持されます。デフォルトの値 (1 年間) は無効になっています。 毎年少なくとも 1 つのリカバリポイントを保存する場合、このオプションを選択して年数を指定します。毎年のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。

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決定されます。

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

...さらに、1 時間あたり 1 つのリカバリポイントを 3 日間保持

...さらに、1 日あたり 1 つのリカバリポイントを 4 日間保持

...さらに、1 週間あたり 1 つのリカバリポイントを 3 週間保持

...さらに、1 か月あたり 1 つのリカバリポイントを 2 か月間保持

...さらに、1 か月あたり 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 か月前のものになります。

7. 保存ポリシーの設定が完了したら、**保存** をクリックします。

   設定 ダイアログボックスが閉じます。

8. **夜間ジョブ** ダイアログボックスで **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ます。定義した保持ポリシーが夜間ロールアップ時に適用されます。

   これらの設定は、個々の保護対象マシンの保持ポリシーを指定するときに適用することもできます。保護対象マシンの保持ポリシーの設定の詳細については、「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。

保護対象マシンの保持ポリシー設定のカスタマイズ

特定の保護対象マシンのリカバリポイントをプライマリ DVM リポジトリから階層化リポジトリに再配置する場合、階層化リポジトリがすでに存在している必要があります。階層化リポジトリを定義するには、「階層化リポジトリの作成」を参照してください。

保護対象マシンの保持ポリシーは、リカバリポイントをリポジトリに保存する期間を指定します。デフォルトでは、各保護対象マシンは、この手順で説明するようにカスタム保持ポリシーを指定しない限り、Core に設定された保持ポリシーを使用します。

Rapid Recovery バージョン 5.4.1 から、AppAssure には、ソース Core 上の保護対象マシンとターゲット Core 上のレプリケートされた対応するマシンに、異なる保持ポリシーを設定できる機能が含まれています。

この手順を使用して、保護対象マシンのカスタム保持ポリシーを定義します。これには、レプリケートされたマシンも含まれます。

NOTE: 次の記述は、Rapid Recovery Core リリース 5.3.x からリリース 5.4.1 またはすべてのバージョンの AppAssure にアップグレードする環境に適用されます。レプリケートされたマシンの保持ポリシーをカスタマイズする場合は、まずソース Core および ターゲット Core を AppAssure Core リリース 5.4.1 にアップグレードしてから、そのターゲット Core の各リポジトリでリポジトリチェックジョブを実行してください。リポジトリのサイズや基になるストレージシステムによっては、このジョブの完了に長時間かかる場合があります。このジョブに関する基礎的な情報については、「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。このジョブの実行方法については、「DVM リポジトリでの整合性チェックの実行」を参照してください。

1. Rapid Recovery Core Console の マシン メニューで、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 **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. 必要に応じて、設定 ページで **夜間ジョブ** リンクをクリックし、スクロールダウンして、夜間ジョブの設定を表示します。

4. 夜間ジョブ の見出しの下で、 **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。

5. 必要に応じてバックアップデータを保持する間隔を指定するには、**ロールアップ** を選択し、**設定** をクリックします。

   保持ポリシーの **設定** ダイアログボックスが表示されます。

6. レプリケートされたマシンの保持ポリシー設定のカスタマイズ中に、リポジトリで整合性チェックを実行するように通知する注意が表示された場合は、この手順を実行します。それ以外の場合は、手順 7 に進みます。

   a. このジョブを実行する準備ができている場合は、**整合性チェック** をクリックします。

   b. **はい** をクリックして整合性チェックジョブを確認します。

   NOTE: リポジトリのサイズによっては、このジョブにかなりの時間がかかる場合があります。この間、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。

   - リポジトリチェックジョブの子ジョブがすべて正常に完了したら、この手順に戻って次のステップに進みます。

7. **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。

   - 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、**Core のデフォルトの保持ポリシーを使用する** を選択し、**保存** をクリックします。この保護対象マシンにデフォルトのポリシーが適用されます。
   - このエージェントのカスタム保持ポリシーを定義する場合は、**カスタム保持ポリシーを使用する** を選択し、次のステップに進みます。

   設定 ダイアログボックスが展開され、カスタム保持ポリシーの情報が表示されます。

8. 次の表の説明に従って、リカバリポイントを保持するカスタムスケジュールを入力します。最初の設定で、リポジトリに保存されたすべてのリカバリポイントのプライマリ保持期間を指定します。各追加設定を有効にすると、リカバリポイントがロールアップされる間隔を指定することで、より詳細なレベルの保持を指定できます。これらの設定は、リカバリポイントを維持する期間を定義します。

表 150. 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
すべてのリカバリポイントを n [保持期間] 保持…	リポジトリに保存されたすべてのリカバリポイントのプライマリ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。 次から選択できます。日、週、月、および 年
…さらに、1 時間あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 時間ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 2 日間です。日、週、月、および 年 から選択できます。 1 時間ごとのリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 日あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1日ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 4 日間です。日、週、月、および 年 から選択できます。 毎日のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 週間あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 週間ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 3 週間です。週、月、および 年 から選択できます。 1 週間ごとのリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 か月あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、 1 か月ごとに 1 つのリカバリポイントがこの設定により指定した期間保持されます。デフォルトは 2 か月です。月 および 年 から選択できます。 毎月のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。
…さらに、1 年あたり 1 つのリカバリポイントを n [保持期間] 保持	選択した場合、1 年ごとに 1 つのリカバリポイントがこの設定により指定した年数保持されます。デフォルトの値 (1 年間) は無効になっています。 毎年少なくとも 1 つのリカバリポイントを保存する場合、このオプションを選択して年数を指定します。毎年のリカバリポイントを 1 つも保存しない場合、このオプションを選択解除します。

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

…さらに、1 時間あたり 1 つのリカバリポイントを 3 日間保持

…さらに、1 日あたり 1 つのリカバリポイントを 4 日間保持

…さらに、1 週間あたり 1 つのリカバリポイントを 3 週間保持

…さらに、1 か月あたり 1 つのリカバリポイントを 2 か月間保持

…さらに、1 か月あたり 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 か月前のものになります。

9. リカバリポイントをプライマリ DVM リポジトリで保持する場合は、手順 11 にスキップします。
10. リカバリポイントをプライマリ DVM リポジトリからQuest DR シリーズバックアップアプライアンスに保存されたセカンダリ階層化リポジトリに再配置する場合、次の手順を実行します。

a. **期限切れのリカバリポイントを階層化リポジトリに再配置する** オプションを選択します。

b. プライマリリポジトリから階層化リポジトリにリカバリポイントを移動するには、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。設定可能な最短期間は 1 週間です。

c. **リポジトリを選択** ドロップダウンメニューで、指定したマシンのすべてのリカバリポイントを再配置する階層化リポジトリを選択します。

NOTE: リカバリポイントが配置される場所 (ローカル DVM リポジトリ または DR バックアップアプライアンス上のセカンダリ階層化リポジトリか) に関係なく、リカバリポイントは保持ポリシーの適用対象であり、ロールアップされます。保持期間よりも古いリカバリポイントを保持する必要がある場合の方法の 1 つは、アーカイブすることです。もう 1 つの方法は、ロールアップを無効にするか、または関連する保護対象マシンの保持期間を延長します。

11. **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。

アーカイブあーかいぶ

本項では、Rapid Recovery アーカイブの概念について説明します。これには、アーカイブ作成のビジネスケース、ストレージオプション、および使用に関する情報が含まれます。また、1 回限りのアーカイブの作成方法や、スケジュールに従って継続的に更新されるアーカイブの作成方法についても説明します。スケジュール設定されたアーカイブを一時停止または編集する方法、アーカイブを強制的に実行またはチェックする方法、およびアーカイブをアタッチまたはインポートする方法を説明しているトピックも含まれています。

アーカイブについて

Rapid Recovery Core ではスナップショットデータをリポジトリに保存します。リポジトリはさまざまなストレージテクノロジ（SAN、DAS、NAS など）上に存在することができますが、最も重要なパフォーマンス要素は速度です。リポジトリでは短期（高速でより高価な）メディアを使用します。リポジトリがすぐに一杯になることを防止するために、Core では保持ポリシーを実施して時間の経過とともにリカバリポイントをロールアップし、最終的に新しいバックアップデータに置き換えます。

履歴保存の意味や法令遵守、あるいはオフサイトのデータストレージポリシーを満たすためなどの理由で、リカバリポイントを保持する必要がある場合、アーカイブを作成できます。アーカイブは、指定した日付範囲上にある、指定マシンのリポジトリからのリカバリポイントのコピーです。リカバリポイントのセットをアーカイブしても、リポジトリ内の元のリカバリポイントは削除されません。代わりに、アーカイブを行うと、リカバリポイントの集合はアーカイブ作成時点の状態に留まり、指定した保存場所に別のコピーとして格納されます。リポジトリ内にあるリカバリポイントとは異なり、アーカイブ内のデータは、ロールアップの対象になりません。

アーカイブを作成、インポート、およびアタッチするには、ボタンバーの  **アーカイブ** オプション、または Core Console の ••• （その他）アイコンからアクセス可能な**アーカイブ** ページを使用できます。

See also: アーカイブの作成およびストレージオプション
See also: Amazon のストレージオプションとアーカイブ
See also: アーカイブ用のリカバリポイントチェーンのオプション
See also: アーカイブにアクセスする方法
See also: アーカイブの使用
See also: アーカイブの作成

アーカイブの作成およびストレージオプション

任意の時点にオンデマンドで、1 回限りのアーカイブを作成できます。

継続的にスケジュール設定されたアーカイブの要件を定義することもできます。このアクションでは、選択したマシンのリカバリポイントのアーカイブが指定した場所に作成されます。これらのマシンへの追加のリカバリポイントは、その後定義済みスケジュール（毎日、毎週、または毎月）に従ってアーカイブに継続的に追加されます。

アーカイブを作成する場合は、保存する場所を指定します。アーカイブはファイルシステム（ローカルまたはネットワーク上）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。

NOTE: クラウドアカウントをアーカイブする前に、まず資格情報を Rapid Recovery Core のストレージアカウントに追加する必要があります。Core でのクラウドアカウントの定義の詳細については、「クラウドアカウントの追加」を参照してください。

アーカイブを Amazon クラウドストレージアカウントにアーカイブする場合、アカウントの作成時にストレージクラスを定義する必要があります。Amazon Glacier に直接アーカイブする場合は、アーカイブウィザードで場所

を定義するときに Glacier ストレージを指定できます。Amazon ストレージクラスの詳細については、「Amazon のストレージオプションとアーカイブ」を参照してください。

- 1 回限りのアーカイブは、読み取り専用です。1 回限りのアーカイブを作成するときは、指定する宛先の場所を空にする必要があります。
- スケジュール済みアーカイブを使用すると、Core は既存のアーカイブに追加のリカバリポイントを付加します。
- 選択したストレージメディアで容量が不足した場合には、Rapid Recovery でアーカイブジョブが一時停止し、別の場所を指定できます。次にアーカイブはセグメントに分割されます。スペースがある場合は、セグメントを異なる場所に配置できます。

See also: クラウドアカウントの追加

Amazon のストレージオプションとアーカイブ

Amazon Simple Storage Service（S3）アカウントにデータをアーカイブする場合、さまざまなストレージクラスから選択することができます。ストレージクラスごとに異なるコスト、メリット、アクセス制限が設定されています。価格はリージョンによって異なる場合があります。Rapid Recoveryリリース 6.2.1 では、Amazon ストレージアカウントのサポート対象がすべてのストレージクラスに拡張されています。これは、Rapid Recovery のアーカイブを Amazon クラウドに保存することを計画している場合に役立ちます。

ストレージのコストを効果的に管理しつつ、許容される時間範囲内にアーカイブにアクセスできるようにするには、利用可能なストレージクラス、およびこれらのクラスにアクセスするためのリードタイムの差を把握しておくことが極めて重要です。

NOTE: Quest では、Rapid Recovery のお客様がストレージの価格に関する認識を高めることができるように、この情報を提供しています。これらの考え方を計画と予算を策定する際に利用して、役立てることができます。Amazon や他のクラウドサービスプロバイダのすべてのストレージコストは、ユーザーが確認する必要があります。Amazon は前提条件、要件、コスト、ストレージ階層の定義などを変更することがあるため、それらの情報については、Amazon ウェブサイトを最も重要な高信頼ソースとして使用してください。

Amazon では現在のところ、おおむね次のようなストレージクラスを提供しています。

標準。このストレージクラスは、頻繁に、または迅速にアクセスする予定のデータに使用します。このクラスは、Rapid Recovery のすべてのウィザード、ウィンドウ、およびダイアログボックスで、デフォルトのストレージオプションとして使用されます。標準ストレージクラスでは、情報の取得に料金は別途発生しません。

標準 - 低頻度アクセス（IA）。これは標準クラスよりも経済的なストレージクラスで、頻繁にアクセスする予定ではないデータ向けです。このストレージクラスのデータにアクセスするには取得料金がかかります。ただし、データはただちに取得できます。Amazon では、30 日を経過せずに低頻度アクセスストレージから削除されたオブジェクトに対して料金を課しています。

Glacier。このストレージは、リアルタイムのアクセスを必要としないデータの長期ストレージ用です。ほとんど取得されないデータの長期ストレージ用としては最も経済的です。このストレージクラスのデータにアクセスするには取得料金がかかります。Amazon では、90 日を経過せずに Glacier から削除されたオブジェクトに対して料金を課しています。Glacier に保存されたデータは、ただちに取得することはできません。通常の取り出し（Standard）に必要な時間は 3 ～ 5 時間です。大量データの一括取り出し（Bulk）には、最大で 12 時間かかります。急速取り出し（Expedited）の場合は、最大 5 分で取得できます。取得オプションごとに料金が適用されます。

NOTE: 他の Amazon ストレージクラスとは異なり、Rapid Recovery では、Glacier 固有のクラウドアカウントの作成をサポートしていません。Glacier にデータをアーカイブするには、Amazon クラウドアカウントを選択し、アーカイブウィザードの **場所** ページで **Glacier ストレージを使用** オプションを選択します。

低冗長化ストレージ（RRS） このカテゴリは、標準ストレージクラスよりも冗長性レベルを下げた、重要性の低い再作成可能なデータ向けに提供された低コストのストレージクラスです。このストレージクラスのデータにアクセスするには、最低限の取得料金がかかります。このクラスに保存されたオブジェクトのうち、ごくわずかな割合（Amazon によると最大 0.01%）は、回復不可能であると予測されています。

最新の情報については、必ず Amazon ウェブサイトの資料を確認してください。

一般的には、次のガイドラインが適用されます。

- Rapid Recovery アーカイブから定期的にデータをリストアすることが予想される場合は、標準が最適なオプションと考えられます。
- データをリストアする頻度が低いと予想される場合は、コストの観点から標準 - 低頻度アクセスを検討します。
- Glacier は、リストアに使用する可能性が低いと想定されるアーカイブリカバリポイントのコールドストレージに使用します。Glacier ストレージを使用する良い例として、コンプライアンス標準のためにデータを保存するケースが挙げられます。Glacier は、アーカイブウィザードからアーカイブオプションとして利用できます。
- 重要性の低い再作成可能なデータのストレージには、RRS を検討してください。

アーカイブ用のリカバリポイントチェーンのオプション

アーカイブを作成する前に、リカバリポイントチェーンに対して、適切な手段を決定する必要があります。次の情報を使用して、アーカイブウィザード の **オプション** ページでどのオプションを選択するかを決定します。

- **日付範囲外の参照されたベースイメージを含めた、完全なリカバリポイントチェーンを構築します。**完全なリカバリポイントチェーンを構築するオプションを選択すると、アーカイブ内のすべてのリカバリポイントについて全範囲の復元アクションを実行できます。この範囲には、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。このオプションを選択すると、完全なリカバリポイントチェーンがアーカイブとともに保存されます。データは、選択したリカバリポイントに対応するベースイメージがアーカイブの日付範囲よりも前である場合にも、復元することができます。ただし、フルリカバリポイントチェーン内のデータへのアクセスがあることを確認するため、このアーカイブのファイルサイズは大きくなります。
- **日付範囲内のリカバリポイントのみが含まれます。スペースは節約できますが、必要なベースイメージのアーカイブの責任を負うことになります。**アーカイブ内に指定した日付範囲内のリカバリポイントのみを含める場合には、アーカイブのファイルサイズが小さくなります。ベースイメージが指定した日付範囲に含まれているデータについては、リストアオプションの全範囲にアクセスできます。ただし、指定した日付範囲より前の日付からのベースイメージにキャプチャされたデータを復元する場合は、ファイルレベルのリカバリのみに制限されます。アーカイブの範囲外のデータは孤立します。

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」のトピックを参照してください。

関連概念

See also: リカバリポイントチェーンとオーファン

関連タスク

See also: アーカイブの作成
See also: スケジュール設定されたアーカイブの編集

アーカイブにアクセスする方法

アーカイブされた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、2 つのオプションがあります。

- Rapid Recovery バージョン 6.0.1 以降で作成されたアーカイブの場合、アーカイブを接続することができます。接続されたアーカイブは、Core Console の左のナビゲーションメニューに表示されます。アーカイ

ブ内のリカバリポイントを参照し、データをリポジトリにインポートせずに、リポジトリに存在するその他のリカバリポイントと同様に、そのデータに同じアクションをとることができます。

- アーカイブをインポートし、それらのリカバリポイントをリポジトリに復元することができます。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。Rapid Recovery Core は下位互換性をサポートし、AppAssure と Rapid Recovery のすべてのバージョンからのアーカイブのインポートをサポートしています。

CAUTION: Core はアーカイブ内のリカバリポイントについて元の日付を認識しているため、アーカイブからインポートされたリカバリポイントは次の夜間ジョブの期間中にロールアップされるか、または保持期間が超えている場合は削除されます。アーカイブからインポートした古いリカバリポイントを保持する場合は、ロールアップを無効にするか、または関連する保護対象マシンの保持期間を延長することができます。

アーカイブ済みの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、アーカイブを接続 (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。

関連タスク

See also: アーカイブのアタッチ
See also: アーカイブのインポート

アーカイブの使用

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。

- アーカイブはリポジトリ間でデータを移動するために使用されます。
- アーカイブは Core Console に接続し、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ことができます。いくつかの制限が適用されます。
- リポジトリにインポートする。アーカイブのリカバリポイントがリポジトリからロールアップまたは削除されている場合、このアクションによりリカバリポイントがリストアされます。
- アーカイブは、ベアメタル復元または仮想マシンへのエクスポートのソースとして使用されます。

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。定期アーカイブをスケジュールすると、1 回限りのアーカイブを繰り返し定義することなく、保護対象マシンからのデータを頻繁にアーカイブするニーズに対応できます。

アーカイブを作成する場合は、アーカイブにフルリカバリポイントチェーンを含めるかどうかを決定する必要があります。詳細については、アーカイブ用のリカバリポイントチェーンのオプションを参照してください。

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
   - 継続的なアーカイブ (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 151. 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	`d:\work\archive` などアーカイブを格納する場所のローカルパスを入力します。
ネットワーク	場所	`\\servername\sharename` などアーカイブを格納するネットワークパスを入力します。
	ユーザー名	ネットワーク共有にアクセスできるユーザーのユーザー名を入力します。
	パスワード (A)	ネットワーク共有にアクセスできるユーザー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。 **NOTE:** 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	アーカイブデータが保存されるフォルダの名前を入力します。
	Glacier ストレージを使用	Amazon Glacier ストレージにアーカイブを保存するには、このオプションを使用します。このオプションはアーカイブを長期間保存することを目的にしていま

オプション	テキストボックス	説明
		す。詳細については、「Amazon のストレージオプションとアーカイブ」を参照してください。

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、**次へ** をクリックします。
7. 次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 14 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 8 に進みます。
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(D)
   - 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 152. 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
毎日	時間	日次アーカイブを作成する時間を選択します。
週次(W)	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。
毎月	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。

10. 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。

    NOTE: 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. 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 153. 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
この Core を置換	この Core に関連する既存のアーカイブ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	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(I)	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、アーカイブに存在するデータの重複を回避します。

13. 継続アーカイブの **オプション** ページで、アーカイブにフルリカバリポイントチェーンを含めるかどうかを決定します。リカバリポイントチェーンのオプションの詳細については、「アーカイブ用のリカバリポイントチェーンのオプション」を参照してください。次のいずれかを実行します。
    - **日付範囲外の参照されたベースイメージを含めた、完全なリカバリポイントチェーンを構築します。** を選択してから、手順 17 に進みます。
    - **日付範囲内のリカバリポイントのみを含めます。このオプションではスペースは節約できますが、必要なベースイメージのアーカイブの責任を負うことになります** を選択してから、手順 17 に進みます。
14. 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 154. 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、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) 。 • テキストボックスを選択して、領域の容量を入力し、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。 **NOTE:** 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**。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。 • **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。
日付範囲外の参照されたベースイメージを含めた、完全なリカバリポイント	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。

テキストボックス	説明
チェーンを構築します。	
日付範囲内のリカバリポイントのみが含まれます。スペースは節約できますが、必要なベースイメージのアーカイブの責任を負うことになります。	増分リカバリポイントのみをアーカイブし、ベースイメージを含めない場合は、このオプションを選択します。 **NOTE:** このオプションを使用すると、孤立したリカバリポイントがアーカイブされます。関連するベースイメージもアーカイブするまでは、これをリカバリ用に使用することはできません。 リカバリポイントチェーンのオプションの詳細については、「アーカイブ用のリカバリポイントチェーンのオプション」を参照してください。

15. 日付範囲内のリカバリポイントのみを含めるオプションを選択した場合、**次へ** をクリックします。それ以外の場合は、**終了** をクリックします。
16. **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。
17. **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 S3、OpenStack ベースのプロバイダ、Rackspace Cloud Files、Google Cloud などがあります。

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。
- アーカイブをアタッチするか、クラウドの場所からインポートして、アーカイブされたデータを取得します。詳細については、「アーカイブのアタッチ」または「アーカイブのインポート」をそれぞれ参照してください。

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 **その他** 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** ページの スケジュールされたアーカイブ 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 155. 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	`d:\work\archive` などアーカイブを格納する場所のローカルパスを入力します。
ネットワーク	場所	`\\servername\sharename` などアーカイブを格納するネットワークパスを入力します。
	ユーザー名	ネットワーク共有にアクセスできるユーザーのユーザー名を入力します。
	パスワード (A)	ネットワーク共有にアクセスできるユーザー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。 **NOTE:** 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	アーカイブデータが保存されるフォルダの名前を入力します。
	Glacier ストレージを使用	Amazon Glacier ストレージにアーカイブを保存するには、このオプションを使用します。このオプションはアーカイブを長期間保存することを目的にしています。詳細については、「Amazon のストレージオプションとアーカイブ」を参照してください。

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(D)
   - 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 156. 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
毎日	時間	日次アーカイブを作成する時間を選択します。
週次(W)	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。
毎月	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。

> **NOTE:** 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 157. 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
増分(I)	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. ウィザードの **オプション** ページで、アーカイブにフルリカバリポイントチェーンを含めるかどうかを決定します。リカバリポイントチェーンのオプションの詳細については、「アーカイブ用のリカバリポイントチェーンのオプション」を参照してください。次のいずれかを実行します。
    - **日付範囲外の参照されたベースイメージを含めた、完全なリカバリポイントチェーンを構築します。** を選択します。
    - **日付範囲内のリカバリポイントのみを含めます。スペースは節約できますが、必要なベースイメージのアーカイブの責任を負うことになります。**
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」の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 **その他** 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。
     - 一時停止
     - 再開
   - 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。
     - 一時停止
     - 再開

   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 で、アイコンバーの **その他** 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、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。

1. Rapid Recovery Core Console で、アイコンバーの **その他** 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。
3. **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
4. 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 158. 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	アーカイブのローカルパスを入力します。
ネットワーク	場所	アーカイブのネットワークパスを入力します。
	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 (A)	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。 **NOTE:** 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 -7-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。

   NOTE: 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

オプション	説明
	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 リリース 6.0.1 以降で作成されたアーカイブが存在している必要があります。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の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と禁止されている語句は、使用できません。
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 159. 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。

オプション	テキストボックス	説明
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(A)	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。 **NOTE:** 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	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

次の手順を使用して、アーカイブを 1 回のみインポートしたり、アーカイブを定期的にインポートするスケジュールを設定したりすることができます。

アーカイブデータをリカバリする場合は、指定の場所にアーカイブ全体をインポートします。

CAUTION: この手順は、十分に検討してから実行してください。アーカイブをインポートすると、アーカイブの内容がリポジトリに再入力され、アーカイブのキャプチャ以降のリポジトリ内の新しいデータがすべて置き換えられます。

アーカイブをインポートするには、次の手順を実行します。

1. Rapid Recovery Core Console のメニューバーで **アーカイブ** ドロップダウンメニューをクリックし、**アーカイブのインポート** を選択します。

   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**インポートタイプ** ページで、次のいずれかのオプションを選択します。
   - 1 回限りのインポート
   - 継続インポート（スケジュール使用）
3. **次へ** をクリックします。
4. **場所**ページでドロップダウンリストから、インポート元の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 160. インポートされ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	`d:\work\archive` などアーカイブを格納する場所のローカルパスを入力します。
ネットワーク	場所	`\\servername\sharename` などアーカイブを格納するネットワークパスを入力します。
	ユーザー名	ネットワーク共有にアクセスできるユーザーのユーザー名を入力します。
	パスワード (A)	ネットワーク共有にアクセスできるユーザー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。 **NOTE:** 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	アーカイブデータが保存され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. アーカイブに含まれているすべてのマシンをインポートする場合は、ウィザードの **アーカイブの情報** ページで **すべてのマシンをインポート** を選択します。
7. 選択に基づいて、次のオプションのいずれかを実行します。
   - **手順 2** で 1 回限りのインポート を選択し、**手順 6** で すべてのマシンをインポート を選択した場合で、すべてのマシンが Core 上に (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として) 存在する場合は、手順 12 に進みます。
   - **手順 2** で 継続インポート (スケジュール使用) を、**手順 6** で すべてのマシンをインポート を選択しており、少なくとも 1 台のマシンが Core 上に (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として) 存在していない場合は、**次へ** をクリックし、手順 9 に進みます。
   - 手順 6 でインポートしていないマシンがある場合は、**次へ** をクリックし、手順 8 に進みます。
8. **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 1 回限りのインポート を選択しており、少なくとも 1 台のマシンが Core 上に (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として) 存在していない場合は、ドロップダウンリストを使用して、インポートする各マシンのリポジトリを選択し、手順 12 に進みます。
   - すべてのマシンが Core 上に (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として) すでに存在する場合は、手順 12 に進みます。
9. **次へ** をクリックします。
10. **リポジトリ** ページで、次のいずれかを行います。
    - リポジトリが Core に関連付けられている場合は、次の表にあるオプションのいずれかを選択します。

表 161. リポジトリオプション

オプション	説明
既存のリポジトリを使用	ドロップダウンメニューから、Core に現在関連付けられているリポジトリを選択します。
リポジトリを作成	サーバ テキストボックスに、新しいリポジトリの保存先となるサーバの名前を、servername または localhost のように入力し、「DVM レポジトリの作成」を参照してください。

- Core にリポジトリが関連付けられていない場合は、新しいリポジトリの保存先となるサーバの名前を、servername または localhost のように入力し、「DVM レポジトリの作成」を参照してください。

11. **手順 2** で 継続インポート (スケジュール使用) を選択した場合は、**スケジュール** ページで、次の表に説明されているオプションを選択します。

表 162. 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	時計アイコンをクリックし、上下の矢印を使用して、アーカイブジョブを開始する時刻を選択します。 12 時間形式の時刻を使用する場合は、AM または PM ボタンをクリックして時刻を指定します。
週次(W)	曜日を選択し、アーカイブジョブを開始する時刻を選択します。 12 時間形式の時刻を使用する場合は、AM または PM ボタンをクリックして時刻を指定します。
毎月	日付を選択し、アーカイブジョブを開始する時刻を選択します。 12 時間形式の時刻を使用する場合は、AM または PM ボタンをクリックして時刻を指定します。
最初のインポートを一時停止	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、このオプションを選択します。 **NOTE:** 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、スケジュールされた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刻にインポートが開始されます。

12. **終了** をクリックします。

クラウドアカウント

Rapid Recovery では、既存のクラウドストレージやクラウドサービスプロバイダと、Rapid Recovery Core の間の接続を定義できます。互換性のあるクラウドサービスには、Microsoft Azure、Amazon Web Services（AWS）、OpenStack ベースのプロバイダ（Rackspace を含む）、Google Cloud などがあります。米国政府固有のプラットフォームには、AWS GovCloud（US）および Azure Government などがあります。任意の数のクラウドアカウント（同じプロバイダの複数のアカウントを含む）を Core Console に追加できます。

クラウドアカウントを Core Console に追加する目的は、「クラウドアカウントについて」のトピックに説明されているようにそれらのアカウントで操作を行うことです。

アカウントを追加したら、Core とクラウドアカウントの間の接続を管理できます。具体的には、表示名や資格情報の編集、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。Core Console でクラウドアカウントを編集または削除する場合、クラウドアカウント自体は変更せず、それらのアカウント間のリンクと、Core Console からのそれらのアカウントへのアクセス可能性のみを変更します。

本項では、既存のクラウドストレージプロバイダやクラウドサービスプロバイダのアカウントと、Rapid Recovery Core Console の間のリンクを定義する方法について説明します。また、これらのクラウドアカウントを Rapid Recovery で管理する方法についても説明します。

次のトピックで構成されています。

- クラウドアカウントについて
- クラウドストレージオプションの検討
- クラウドアカウントの追加
- クラウドアカウントの編集
- クラウドアカウントの削除

クラウドアカウントについて

Rapid Recovery では、次のような方法でクラウドアカウントを利用できます。

- **アーカイブ**。1 回限りのアーカイブまたは継続的にスケジュール設定されたアーカイブをクラウドに保存できます。この機能は、サポートされているすべてのクラウドアカウントのタイプで利用できます。クラウドにアーカイブした場合、アーカイブをアタッチすることで、アーカイブされたリカバリポイントの情報に後からアクセスすることができます（リリース 6.0.1 以降で作成されたアーカイブの場合）。すべてのアーカイブは、インポートすることも可能です。また、アーカイブからベアメタル復元も実行できます。
- **仮想エクスポート**。仮想エクスポートを Azure クラウドアカウントに対して実行できます。これには、仮想マシンの 1 回限りのエクスポートや、仮想スタンバイ VM の連続エクスポートが含まれます。

さまざまなクラウドアカウントの概念については、「クラウドストレージオプションの検討」を参照してください。

Core とクラウドアカウントの間のタイムアウト設定を構成する詳細については、「クラウドアカウント接続設定の構成」を参照してください。

Azure クラウドへの仮想エクスポートを実行する詳細については、「Azure 仮想マシンへのデータのエクスポート」を参照してください。

クラウドストレージオプションの検討

このトピックでは、米国政府向けクラウドストレージアカウントのサポートについて説明します。また、アーカイブ用のクラウドアカウントを選択する際のコストと他の要素のトレードオフについても説明します。

米国政府向けの安全なクラウドアカウント

米国連邦政府、州政府、地方自治体の各機関およびそのパートナーがアクセスできるクラウドアカウントのオプションはますます増加しています。Rapid Recovery では、政府機関向けの次のサービスおよび関連するクラウドアカウントをサポートしています。

- **AWS GovCloud (US)** 。Amazon Web Services が AWS GovCloud (US) というサービスを提供しています。これは、特定の規制やコンプライアンス要件を満たすように設計された独自の AWS リージョンです。このサービスを使用して、米国政府機関と顧客はクラウドアカウントを活用して民間企業と連携することができます。Rapid Recovery では、AWS GovCloud 内の Amazon S3 ストレージアカウントへのアーカイブをサポートしています。
- **Azure Government**。Azure Government は米国連邦政府、州政府、地方自治体、先住民族政府の各機関およびそのパートナー向けの、米国政府専用のクラウドプラットフォームです。Rapid Recovery では、標準の Azure サポートと同じように、Azure Government のサポートを提供しています。たとえば、次のとおりです。
  - Rapid Recovery では、Azure Government および Azure 標準ストレージアカウントへのアーカイブをサポートしています。
  - Rapid Recovery では、パブリックプラットフォームおよび Azure Government プラットフォーム上の Azure 仮想マシンへの仮想エクスポート (1 回限り、または仮想スタンバイ) をサポートしています。
  - Rapid Recovery では、パブリッククラウドプラットフォームまたは Azure Government クラウドプラットフォームのレプリケーションターゲットに対するオンプレミス Core のレプリケートをサポートしています。いずれのプラットフォームの場合でも、Azure Marketplace にログインすると、Azure Government Marketplace から「Rapid Recovery Replication Target」を選択できます。この VM、Azure コンピューティングサービス、およびリポジトリ用に VM に追加するストレージを使用して、オンプレミスのバックアップデータを Azure Government クラウドにレプリケートするターゲット Core を迅速かつ簡単に設定できます。

クラウドアカウントにアーカイブする場合のアクセス時間、コスト、および利便性の間でバランスを取る

コストパフォーマンスに優れたクラウドアーカイブと仮想エクスポートのオプションを提供するために、Rapid Recovery では引き続き、クラウドストレージプロバイダ (およびストレージを提供する主要なプロバイダのストレージクラス) のサポートを拡大しています。知識のあるユーザーはポリシーを利用して、データアーカイブの利便性、データアクセス時間、およびコストのバランスを取ることができます。

クラウドにアーカイブするかエクスポートするかの戦略を検討する場合、Rapid Recovery ユーザーは、データを格納する初期コスト、想定されるデータの使用頻度、所定の期間内にそれらのデータにアクセスする必要性、およびデータの取得に伴うコストの間のトレードオフを理解することが推奨されます。

一部のプロバイダ (Amazon S3 など) は、さまざまなストレージクラスを提供しています。上記の要因に関する想定が正確であれば、適切なストレージクラスを選択することで費用を削減できます。Quest では、Rapid Recovery ユーザーが少なくとも年に 1 回はデータストレージのポリシーを見直して、リソースを効果的に利用していることを確認することをお勧めします。同様に、ユーザーが計画で使用する想定に最新の状況を反映して、それに応じてデータを移行できるように、管理者はクラウドアカウントにアーカイブまたはエクスポートされているデータを再調査することが求められます。

一部のベンダーでは、データを格納する費用は非常に安価であるか、無料の場合もあります。ただし、多くのクラウドサービスプロバイダでは、それらのデータへのアクセスや取得に対しては費用が課されます。多くの場合、どの程度迅速にデータにアクセスする必要があるかに基づいてさまざまな料金が設定されています。Glacier にデータを保存してリストアを行うよりも、コストの高いストレージ (Amazon S3 標準) を使用してリカバリポイントからリストアするほうがコストパフォーマンスが向上することもあります。

Amazon では、時間の経過に伴って Amazon S3 ストレージクラス間でデータを移動するデータのライフサイクルポリシーを定義できます。たとえば、新しくアップロードしたデータは「標準」ストレージクラスを使用して保存し、30 日後には「標準 – 低頻度アクセス」に移動して、さらに 60 日が経過した後は「低冗長化ストレージ」に移動することができます。また、アーカイブウィザードを使用して、任意のタイプの Amazon S3 クラウドアカウントのデータを、明示的に Glacier にアーカイブすることもできます。これは、データのリカバリ頻度が非常に低いと想定される場合に推奨されます。このオプションを選択する前に、アクセスやストレージ期間などに関する料金をよく把握しておきます。「Amazon のストレージオプションとアーカイブ」のトピックを参照してください。

Rapid Recovery の一部の機能は、特にクラウド向けに設計されています。Azure を使用してクラウドへの仮想エクスポートを行う場合は、仮想スタンバイについて検討します。このプロセスを使用すると、完全に起動可能な仮想マシンを Azure クラウド内に作成できます。VM ファイルは、新しくキャプチャされたリカバリポイントを使用して継続的に更新されます。オンプレミスで実行される仮想スタンバイとは異なり、VM ファイルが必要になるまで、または必要にならない限り、それらのファイルは起動可能な VM に展開されません。Azure で行う仮想スタンバイの初期コストは、ストレージに関するものだけです。コンピューティングコスト (Azure では長期的に多大なコストとなる) は、VM の起動とリストアの実行に必要な、VM の展開が行われた場合にのみ発生します。

また、Rapid Recovery Replication Target を使用して、オンプレミスの Core を Azure クラウドにレプリケートすることもできます。Azure Marketplace で「Rapid Recovery Replication Target」を選択して、ターゲットの Core を迅速かつ簡単に設定することができます。ターゲットの Core にはコンピューティングコストが発生します。Azure 内のリポジトリストレージについても計画する必要があります。リリース 6.2.1 の新機能として、Government クラウドでもレプリケーションターゲットを使用できます。Azure へのレプリケーションの詳細については、『*Rapid Recovery Replication Target for Microsoft Azure #########*』を参照してください。

これらのクラウドストレージオプションを利用する Rapid Recovery ユーザーは、データを格納する初期コスト、所定の期間内にそれらのデータにアクセスする必要性、およびデータの取得に伴うコストの間のトレードオフを理解することが推奨されます。

たとえば、一部のベンダーでは、データを格納する費用は非常に安価であるか、無料の場合もあります。ただし、多くのクラウドサービスプロバイダでは、それらのデータへのアクセスや取得に対しては費用が課されます。多くの場合、どの程度迅速にデータにアクセスする必要があるかに基づいてさまざまな料金が設定されています。Glacier にデータを保存してリストアを行うよりも、コストの高いストレージ (Amazon S3 標準) を使用してリカバリポイントからリストアするほうがコストパフォーマンスが向上することもあります。

Amazon では、時間の経過に伴って Amazon S3 ストレージクラス間でデータを移動するデータのライフサイクルポリシーを定義できます。たとえば、新しくアップロードしたデータは「標準」ストレージクラスを使用して保存し、30 日後には「標準 – IA」に移動して、さらに 60 日が経過した後は「Amazon Glacier」に移動することができます。

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 アイコンバーで、 **その他** 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 163. 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	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、Azure Cloud Account 1 などとします。
	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。 **NOTE:** 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。 **NOTE:** 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。
Amazon S3	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、Amazon S3 Cloud Account 1 などとします。
	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。
	サービスエンドポイント	標準の Amazon S3 ストレージアカウント以外の S3 互換のストレージアカウントを使用している場合、必要に応じてそのストレージアカウントの完全修飾 http または https URL を入力します。
	ストレージクラス	S3 アカウントのストレージクラスを選択します。次から選択できます。 • 標準 • 標準 - 低頻度アクセス • 削減された冗長ストレージ Glacier にアーカイブする場合、リストされたストレージクラスを使用して Amazon クラウドアカウントを定義できます。Glacier ストレージを選択するオプションは、アーカイブウィザードからアクセスできます。 **NOTE:** ストレージクラスの詳細については、「クラウドストレージオプションの検討」を参照してください。
Powered by OpenStack	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 Cloud Account 1 などとします。
	領域	クラウドアカウントの領域を入力します。

クラウドタイプ	テキストボックス	説明
	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。これは、クラウドインスタンスのベース URL です。指定されない場合、Rapid Recovery Core ではデフォルトの URL、https://identity.api.rackspacecloud.com が使用されます。
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、Rackspace Cloud Account 1 などとします。
	領域	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。これは、クラウドインスタンスのベース URL です。指定されない場合、Rapid Recovery Core ではデフォルトの URL、https://identity.api.rackspacecloud.com が使用されます。
Google クラウド	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、Google Cloud Account 1 などとします。
	証明書ファイル	Google 証明書を参照して選択し、このクラウドアカウントを認証します。
	プライベートキー	このアカウントのプライベートキーを入力します。
	プロジェクト ID	このアカウントに関連付けられたプロジェクト ID を入力します。
	サービスアカウントの電子メール	このクラウドサービスアカウントの所有者として Google Cloud に登録した電子メールアドレスを入力します。

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 アイコンバーで、**その他** 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. 必要に応じて詳細情報を編集してから、クラウドアカウントに接続するために必要なパスワード (または API キー、秘密キー、プライベートキー、など) を再入力します。次に、**保存** をクリックします。

   NOTE: クラウドタイプは編集できません。

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 のアイコンバーで、**その他** アイコンをクリックし、**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定します。
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** をクリックして確定します。

   NOTE: 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。

   ダイアログボックスが閉じ、指定したクラウドアカウントにアクセスするための認証情報が Core から削除されます。

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

Local Mount Utility (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、互換性のある任意の 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。この負荷のかからないユーティリティは、Rapid Recovery Agent ソフトウェアと同じ 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できますが、Agent と同じマシン上にインストールすべきではありません。LMU に rapidrecovery-vdisk (以前の aavdisk) と aavstor ドライバが含まれていますが、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、マシンのデスクトップにショートカットが表示されます。

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 Quest 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、「*Mailbox Restore for Exchange #######*」を参照してください。

NOTE: 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、「*Rapid Recovery #######*」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 サーバにインストールする場合、そのマシンはローカルホストとして自動的に LMU に表示されます。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。

- 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

関連タスク

See also: Local Mount Utility への Core マシンの追加
See also: Local Mount Utility オプションの変更
See also: Local Mount Utility での Core の接続設定の編集
See also: Core への再接続
See also: 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 164. Rapid Recovery **Core の認証情報**

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。 **NOTE:** 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(O)	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 ユーザー認証情報を使用する	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。
特定の認証情報を使用する	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。

オプション	説明
	NOTE: 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(A)	Core マシンにアクセスするために使用するパスワード。 **NOTE:** 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 165. Core 設定

オプション	説明
場所	**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フォルダへのパスを入力します。
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
言語(L)	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 • 韓国語
自動更新	最新情報を取得するために LMU と Core の接続を更新する時間を選択して入力します。
ローカル Core の表示	LMU が Core マシンにインストールされている場合、選択するとこの Core が表示されます。

オプション	説明
ポップアップ通知を表示	選択すると、LMU によりデスクトップにポップアップでイベントやアラートが通知されます。
マウントが成功した場合、Windows エクスプローラでマウントフォルダを開きます	マウントされたリカバリポイントのコンテンツを参照できるようにするには、このオプションを選択します。

3. **保存** をクリックします。

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。

NOTE: 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 166. 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。 **NOTE:** 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(O)	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 ユーザー認証情報を使用する	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。
特定の認証情報を使用する	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。 **NOTE:** 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(A)	Core マシンにアクセスするために使用するパスワード。 **NOTE:** 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 マシンへの接続が失われた場合は、LMU ホーム画面で **更新** をクリックして接続を再確立できます。

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。

NOTE: 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。

1. Local Mount Utility のユーザーインタフェースで、削除する Core を右クリックし、**Core の削除** をクリックします。
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。

   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 に口グインせずに、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 での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。

1. LMU 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。
2. マウントするリカバリポイントを選択して、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、LMU オプションのデフォルトの選択を使用して、リカバリポイントをマウントできます。詳細については、次を参照してください。Local Mount Utility オプションの変更。
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。

3. **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 167.「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	リカバリポイントのマウントに使用する場所を入力するか、または参照します。
マウントタイプ	次のいずれかのオプションを選択します。 • 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。LMU の リカバリポイント ページにあるローカルマウント 列に、リカバリポイントがマウントされた方法が表示されます。

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。

NOTE: 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

このオプションが有効になっている場合、Local Mount Utility (LMU) は、Core および保護対象マシンからリアルタイム更新を受信します。このオプションが無効になっている場合、マシンの最新リカバリポイントを表示するには、LMU のホーム画面で定期的に**更新** をクリックする必要があります。

Local Mount Utility でのリカバリポイントのマウント解除

Local Mount Utility (LMU) 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. LMU ユーザーインタフェースから、マウントリカバリポイント (1 つまたは複数) と関連付けられた Core または保護対象マシンをクリックします。
2. 次のいずれかのアクションを実行します。
   - Core または保護対象マシンからマウントされたすべてのリカバリポイントを一度にマウント解除するには、**すべてをマウント解除** をクリックしてから、ダイアログボックスで **はい** をクリックします。
   - 単一のリカバリポイントをマウント解除するには、リストからリカバリポイントを選択し、**マウント解除** をクリックします。

   リカバリポイント (1 つまたは複数) がマウント解除されます。

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『*Rapid Recovery #######*』の「Core Console」の章を補完するものです。

Core Console ユーザーインタフェースの表示

Core Console は、ユーザーが Rapid Recovery を操作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 168. Core Console の UI エレメント

Core Console に表示されるメニューと情報の説明。

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 Quest の口ゴなど、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 169」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**。Quest ウェブサイトの Rapid Recovery の技術マニュアルにリンクします。 • **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 Quest Data Protection サポート ウェブ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。『クイックスタートガイド』は ヘルプ メニューからいつでも開くことができま

UI エレメント	説明
	す。この機能の詳細については、「クイックスタートガイドについて」を参照してください。 • **アイデアを送信**。機能や拡張機能について提案がある場合、このオプションを選択して、Quest 提案ポータルを開きます。ここでアイデアの簡単な説明を入力し、プロダクトマネージャーに Rapid Recovery の将来のリリースに含めるかどうかを検討してもらうことができます。 • **バージョン情報**：Rapid Recovery のバージョン情報 ダイアログボックスが開きます。ここには、Rapid Recovery コンポーネント、バージョン情報、Core ID、本製品に使用されているサードパーティ製品へのハイパーリンク、およびソフトウェアの説明が表示されます。
サーバの日時	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 170」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 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 エレメント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エレメントについては、さらに「表 172」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。左側のフレームには、*Rapid Recovery #######* のトピックを示しているナビゲーションツリーが表示されます。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

UI エレメント	説明
	ンテキスト依存のヘルプの機能を使用すると、すべての#######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 169. ボタンバーのボタンとメニュー

Core Console のボタンバーの各メニューとボタンで使用可能なアクションの説明。

UI エレメント	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。

UI エレメント	説明
	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：レプリケートボタン 	**レプリケート** 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 170. アイコンバー

Core Console のアイコンバーの各メニューで使用可能なアクションの説明。

UI エレメント	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**：入力方向または出力方向の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：仮想スタンバイアイコン 	**仮想スタンバイ**：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、仮想スタンバイ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。

UI エレメント	説明	
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、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：詳細アイコン	システム情報 	**システム情報**。システム情報 をクリックして、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：詳細アイコン	アーカイブ 	**アーカイブ**。Rapid Recovery では、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：詳細アイコン	マウント 	**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。
アイコンバー：詳細アイコン	ブート CD 	**ブート CD**。通常、ベアメタル復元 (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。

UI エレメント	説明		
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	ファイル検索		**ファイル検索**。リカバリポイントで特定のファイルを検索し、これをローカルディスクにリストアできます。
アイコンバー：詳細アイコン	リテンションポリシー		**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	メールのリストア		**メールのリストア**。Exchange Server のデータベースを検索して、メールサービスを特定しリストアできます。
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 171. 左側のナビゲーションメニューオプション

左のナビゲーション領域にリストされたマシンのタイプに使用可能なオプションの説明です。

UI エレメント	説明
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 マシン メニュー (以前の 保護対象マシン 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	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

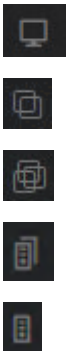
UI エレメント	説明
シン メニュー	ら命名され、その下にリストされる各マシンは、このターゲット上でレプリケートされるそのソース Core からのマシンを表します。 このターゲット Core が複数のソース Core からのリカバリポイントをレプリケートする場合、各ソース Core は左側のナビゲーションエリアで独自の移動可能なメニューとして表示されます。 レプリケートされたマシン メニューに表示される特定のマシン名をクリックすると、サマリページが表示され、選択したレプリケートされたマシンのサマリ情報が表示されます。 レプリケーションの詳細については、「レプリケーション」を参照してください。
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、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。
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 172. 左のナビゲーション領域およびメニュー

左のナビゲーション領域にリストされたマシンのタイプに使用可能なメニューの説明です。

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、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、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。

UI エレメント	説明
マシン メニュー	 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。 **NOTE:** vSphere/ESXi ハイパーバイザ上に保護対象マシンが存在する場合、ホストが保護されていない場合でもこのメニューにホストが表示され、VM がその子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 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。同じアイコンがリカバリポイントのみのマシンを表示するためにも使用されます。 • 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。 • 白抜きの 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。 • 白抜きの 3 台のマシンのアイコンは、VMware vCenter ホストを表します。 • 2 台のサーバが重なっているアイコンは、Hyper-V ホストを示します。 • 1 台のサーバを示すアイコンは、エージェントレス保護された Hyper-V の VM を表します。 マシン メニューラベルをクリックすると、マシン ページが表示されます。このページの 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 の名前が別のメニューとして 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。メニューアイコンはありません。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。リカバリポイントのみのマシンには、標準の保護対象マシンアイコンが表示されます。 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。

UI エレメント		説明
		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。

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。

NOTE: 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。このページでは、各マシンのサマリ情報を確認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。

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 で実行する必要のあるジョブ。
- **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 173. イベント ページの要素

UI エレメント	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。
リストア元	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

UI エレメント	説明
	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
 (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 174. イベントのサマリ表の詳細情報

UI エレメント	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(N)	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。
終了時間	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。
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 詳細 タブの表示

詳細 メニューには、選択した保護対象マシンの管理に役立つ追加のオプションが用意されています。これらのツールにアクセスするには、詳細 ドロップダウンメニューをクリックし、次の表に記載されているいずれかのオプションを選択します。

表 175. 保護対象マシンの 詳細 オプションからアクセスできるツール

UI エレメント	説明
 システム情報	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、このマシンの IP アドレスが表示されます。 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。
 マウント	ローカルマウント ペインから、ローカルにマウントされたボリュームを表示またはマウント解除できます。リモートマウント ペインから、Local Mount Utility を使用してマウントされたボリュームを表示またはマウント解除できます。 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。 リカバリポイントをローカルにマウントする方法については、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。
 リテンションポリシー	選択したマシンの保持ポリシーを指定できます。Core のデフォルトポリシーを使用するように選択できます。または、マシン固有の保持ポリシーを区別することができます。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。
 通知	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。既に Core に設定されている通知は、これによって変更されません。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。
 Agent ログ	Rapid Recovery Agent ソフトウェアを使用して、保護対象マシンのログファイルをダウンロードし、表示することができます。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。

Third-party contributions

This product contains the third-party components listed below. For third-party license information, go to http://quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

Table 176. List of third-party contributions

Component	License or acknowledgment	Notes
AlphaFS 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AlphaVSS 1.2.4000	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 3.3.3	BSD ANTLR 3	Copyright (c) 2003-2007, Terence Parr A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ANTLR 4.0.2	BSD ANTLR 4	Copyright (c) 2012 Terence Parr and Sam Harwell A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
AWS SDK for .NET 3.3.37	Apache 2.0	A copy of this license can be found at Apache 2.0.
Azure SDK for .NET 2.4	Apache 2.0	A copy of this license can be found at Apache 2.0
Bootstrap 3.0.0	Apache 2.0	Bootstrap.js by @fat & @mdo Copyright 2012 Twitter, Inc. A copy of this license can be found at Apache 2.0
Bundletransformer 1.9.138	Apache 2.0	Copyright (c) 2012-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0
Caliburn.Micro 2.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Castle Windsor 2.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Chromium 43.0.2312	Chromium BSD License N/A	Copyright 2014 The Chromium Authors. All rights reserved. A copy of this license can be found at Chromium BSD License N/A.

Component	License or acknowledgment	Notes
CLAP 4.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Common Library for Hyak Code Generator 1.0.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
curlpp 0.7.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
EcmaScript.Net 1.0.1	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Far Manager 3.0.4242	Far Manager BSD License N/A	Copyright (c) 1996 Eugene Roshal Copyright (c) 2000 Far Group All rights reserved. A copy of this licenses can be found at Far Manager BSD License N/A.
fio 2.18*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at GPL (GNU General Public License) 2.0.
FlotCharts 0.8.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Google APIs Client Library for .NET 1.9.2	Apache 2.0	Copyright 2011 Google Inc A copy of this license can be found at Apache 2.0.
HTML Renderer 1.5.0.6	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
html5-placeholder-shim.jquery.js 1.0.58	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ISOLINUX 4.05 20120131*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
JavaScriptEngineSwitcher 1.2.4	Apache 2.0	Copyright (c) 2013-2015 Andrey Taritsyn A copy of this license can be found at Apache 2.0.
jqGrid 4.4.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jqrowl 1.2.6	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
JQuery 1.8.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery File Upload Plugin 5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery knob 1.2.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Templates 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
JQuery UI 1.9.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Validation 1.9.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jQuery Viewport 1.0.0.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.fileDownload 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.hotkeys 0.7.9	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.mCustomScrollbar 3.0.7	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquerey.mousewheel 3.1.12	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.splitter 0.14.0	GNU LGPL Version 3, 29 June 2007	Copyright (C) 2010-2013 Jakub Jankiewicz A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
jquery.tagsinput 1.3.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Json.NET 4.5	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
jsTree 1.0-rc3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.11.3*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.12*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.15*	GNU LGPL Version 3, 29 June 2007	Copyright © 2015 Canonical Ltd. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.17*	GNU LGPL Version 3, 29 June 2007	Copyright © 2002 Red Hat, Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
libc 2.19*	GNU LGPL Version 3, 29 June 2007	Copyright © 2006–2015 SUSE LLC and contributors. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Libc.so.6 2.7*	LGPL (GNU Lesser General Public License) 2.1	A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libext2fs 1.42.12*	GNU Lesser General Public License 2.1	Copyright (C) 1993, 1994, 1995, 1996 Theodore Ts'o. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
libssh2 1.4.3	BSD-style N/A	Portions Copyright 2002-2010 Atsuhiko Yamanaka, JCraft,Inc. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Log4Net 1.2.10	Apache 2.0	A copy of this license can be found at Apache 2.0.
MarkdownSharp 1.13	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
matchMedia 2.72	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
memtest86+ 4.20*	GPL (GNU General Public License) 2.0	A copy of this license can be found at GPL (GNU General Public License) 2.0.
Microsoft Azure Compute	Apache 2.0	A copy of this license can be found at Apache 2.0.

Component	License or acknowledgment	Notes
Management Library 12.0.0		
Microsoft Reactive Extensions for .NET 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Moment.js 2.6.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
MongoDB 2.0.6*	GNU Affero GPL 3.0	A copy of this license can be found at GNU AFFERO GENERAL PUBLIC LICENSE
MongoDB 10gen driver 2.4.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Mono 5.2*	LGPL (GNU Lesser General Public License) 2.1	Copyright (C) 1991, 1999 Free Software Foundation, Inc. A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
MsieJavaScriptEngine 1.4.3*	Mozilla Public License (MPL) 1.1	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NBD various*	GPL (GNU General Public License) 2.0	This component is not used in the application. It is provided with the product for customer convenience. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NDesk.Options 0.2.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Newtonsoft.Json.dll 6.0.8	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
NLog 4.4.12	BSD - Kowalski 2011	Copyright (c) 2004-2011 Jaroslaw Kowalski <jaak@jkowwalski.net>. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
OpenSSL 1.1.0e	OpenSSL 1.0	This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved. A copy of this license can be found at OpenSSL 1.0.
OpenStack.NET 1.4.0.2	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
PowerCollections 2007*	Eclipse Public License 1.0	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Prism 4.0	Microsoft patterns & practices license N/A	Contains software or other content adapted from Microsoft patterns & practices ObjectBuilder, © 2006 Microsoft Corporation. All rights reserved. A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
ProductionStackTrace 1.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Protobuf-net 2.0.0.627	Apache 2.0	A copy of this license can be found at Apache 2.0.
PuTTY 0.63	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Quartz.NET 2.1.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Raphaël—JavaScript Library 2.1.1	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
RazorGenerator 2.1	Apache 2.0	A copy of this license can be found at Apache 2.0.
Resize Floating Popup Control Revision 3	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
respond.js 1.3.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SignalR 1.2.2	Apache 2.0	Copyright (c) .NET Foundation. All rights reserved. A copy of this license can be found at Apache 2.0.
SimpleRestServices 1.2.0.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SimpleRestServices 1.3.0.3	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Sparsehash 1.11	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
SSH.Net 2013.4.7	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Component	License or acknowledgment	Notes
TextFileEncodingDetector 1.0	BSD TextFileEncodingDetector 1.0	Copyright 2002-2008 Xiph.org Foundation Copyright 2002-2008 Jean-Marc Valin Copyright 2005-2007 Analog Devices Inc. Copyright 2005-2008 Commonwealth Scientific and Industrial Research Organisation (CSIRO) Copyright 1993, 2002, 2006 David Rowe Copyright 2003 EpicGames Copyright 1992-1994 Jutta Degener, Carsten Bormann A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
trip 2.1.0	MIT N/A	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
Tri-state tree view Revision 9 (30-May-2011)	Code Project Open License (CPOL) 1.02	A copy of this license can be found at Code Project Open License (CPOL) 1.02 .
Virtual Box SDK 4.2.14*	LGPL (GNU Lesser General Public License) 2.1	c 2004-2015 Oracle Corporation A copy of this license can be found at LGPL (GNU Lesser General Public License) 2.1.
WebGrease 1.5.2	Apache 2.0	A copy of this license can be found at Apache 2.0.
Yahoo! UI Library: YUI Compressor .Net 2.7.0	BSD CodePlex	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.
zlib 1.2.5	zlib 1.2.5	A copy of this license can be found at http://quest.com/legal/third-party-licenses.aspx.

Apache 2.0

License Text

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places:

within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions.

Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Chromium BSD License N/A

License Text

Copyright 2014 The Chromium Authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code Project Open License (CPOL) 1.02

License Text

Preamble

This License governs Your use of the Work. This License is intended to allow developers to use the Source Code and Executable Files provided as part of the Work in any application in any form.

The main points subject to the terms of the License are:

Source Code and Executable Files can be used in commercial applications;

Source Code and Executable Files can be redistributed; and

Source Code can be modified to create derivative works.

No claim of suitability, guarantee, or any warranty whatsoever is provided. The software is provided "as-is".

The Article(s) accompanying the Work may not be distributed or republished without the Author's consent

This License is entered between You, the individual or other entity reading or otherwise making use of the Work licensed pursuant to this License and the individual or other entity which offers the Work under the terms of this License ("Author").

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CODE PROJECT OPEN LICENSE ("LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HEREIN, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. THE AUTHOR GRANTS YOU THE RIGHTS CONTAINED HEREIN IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS. IF YOU DO NOT AGREE TO ACCEPT AND BE BOUND BY THE TERMS OF THIS LICENSE, YOU CANNOT MAKE ANY USE OF THE WORK.

Definitions.

"Articles" means, collectively, all articles written by Author which describes how the Source Code and Executable Files for the Work may be used by a user.

"Author" means the individual or entity that offers the Work under the terms of this License.

"Derivative Work" means a work based upon the Work or upon the Work and other pre-existing works.

"Executable Files" refer to the executables, binary files, configuration and any required data files included in the Work.

"Publisher" means the provider of the website, magazine, CD-ROM, DVD or other medium from or by which the Work is obtained by You.

"Source Code" refers to the collection of source code and configuration files used to create the Executable Files.

"Standard Version" refers to such a Work if it has not been modified, or has been modified in accordance with the consent of the Author, such consent being in the full discretion of the Author.

"Work" refers to the collection of files distributed by the Publisher, including the Source Code, Executable Files, binaries, data files, documentation, whitepapers and the Articles.

"You" is you, an individual or entity wishing to use the Work and exercise your rights under this License.

Fair Use/Fair Use Rights. Nothing in this License is intended to reduce, limit, or restrict any rights arising from fair use, fair dealing, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

License Grant. Subject to the terms and conditions of this License, the Author hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

You may use the standard version of the Source Code or Executable Files in Your own applications.

You may apply bug fixes, portability fixes and other modifications obtained from the Public Domain or from the Author. A Work modified in such a way shall still be considered the standard version and will be subject to this License.

You may otherwise modify Your copy of this Work (excluding the Articles) in any way to create a Derivative Work, provided that You insert a prominent notice in each changed file stating how, when and where You changed that file.

You may distribute the standard version of the Executable Files and Source Code or Derivative Work in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution.

The Articles discussing the Work published in any form by the author may not be distributed or republished without the Author's consent. The author retains copyright to any such Articles. You may use the Executable Files and Source Code pursuant to this License but you may not repost or republish or otherwise distribute or make available the Articles, without the prior written consent of the Author.

Any subroutines or modules supplied by You and linked into the Source Code or Executable Files this Work shall not be considered part of this Work and will not be subject to the terms of this License.

Patent License. Subject to the terms and conditions of this License, each Author hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, import, and otherwise transfer the Work.

Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

You agree not to remove any of the original copyright, patent, trademark, and attribution notices and associated disclaimers that may appear in the Source Code or Executable Files.

You agree not to advertise or in any way imply that this Work is a product of Your own.

The name of the Author may not be used to endorse or promote products derived from the Work without the prior written consent of the Author.

You agree not to sell, lease, or rent any part of the Work. This does not restrict you from including the Work or any part of the Work inside a larger software distribution that itself is being sold. The Work by itself, though, cannot be sold, leased or rented.

You may distribute the Executable Files and Source Code only under the terms of this License, and You must include a copy of, or the Uniform Resource Identifier for, this License with every copy of the Executable Files or Source Code You distribute and ensure that anyone receiving such Executable Files and Source Code agrees that the terms of this License apply to such Executable Files and/or Source Code. You may not offer or impose any terms on the Work that alter or restrict the terms of this License or the recipients' exercise of the rights granted hereunder. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties. You may not distribute the Executable Files or Source Code with any

technological measures that control access or use of the Work in a manner inconsistent with the terms of this License.

You agree not to use the Work for illegal, immoral or improper purposes, or on pages containing illegal, immoral or improper material. The Work is subject to applicable export laws. You agree to comply with all such laws and regulations that may apply to the Work after Your receipt of the Work.

Representations, Warranties and Disclaimer. THIS WORK IS PROVIDED "AS IS", "WHERE IS" AND "AS AVAILABLE", WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OR GUARANTEES. YOU, THE USER, ASSUME ALL RISK IN ITS USE, INCLUDING COPYRIGHT INFRINGEMENT, PATENT INFRINGEMENT, SUITABILITY, ETC. AUTHOR EXPRESSLY DISCLAIMS ALL EXPRESS, IMPLIED OR STATUTORY WARRANTIES OR CONDITIONS, INCLUDING WITHOUT LIMITATION, WARRANTIES OR CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY OF TITLE OR NON-INFRINGEMENT, OR THAT THE WORK (OR ANY PORTION THEREOF) IS CORRECT, USEFUL, BUG-FREE OR FREE OF VIRUSES. YOU MUST PASS THIS DISCLAIMER ON WHENEVER YOU DISTRIBUTE THE WORK OR DERIVATIVE WORKS.

Indemnity. You agree to defend, indemnify and hold harmless the Author and the Publisher from and against any claims, suits, losses, damages, liabilities, costs, and expenses (including reasonable legal or attorneys' fees) resulting from or relating to any use of the Work by You.

Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL THE AUTHOR OR THE PUBLISHER BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK OR OTHERWISE, EVEN IF THE AUTHOR OR THE PUBLISHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Termination.

This License and the rights granted hereunder will terminate automatically upon any breach by You of any term of this License. Individuals or entities who have received Derivative Works from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 6, 7, 8, 9, 10 and 11 will survive any termination of this License.

If You bring a copyright, trademark, patent or any other infringement claim against any contributor over infringements You claim are made by the Work, your License from such contributor to the Work ends automatically.

Subject to the above terms and conditions, this License is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, the Author reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

Publisher. The parties hereby confirm that the Publisher shall not, under any circumstances, be responsible for and shall not have any liability in respect of the subject matter of this License. The Publisher makes no warranty whatsoever in connection with the Work and shall not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. The Publisher reserves the right to cease making the Work available to You at any time without notice

Miscellaneous

This License shall be governed by the laws of the location of the head office of the Author or if the Author is an individual, the laws of location of the principal place of residence of the Author.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this License, and without further action by the parties to this License, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed herein. There are no understandings, agreements or representations with respect to the Work not specified herein. The Author

shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of the Author and You.

Far Manager BSD License N/A

License Text

Copyright (c) 1996 Eugene Roshal

Copyright (c) 2000 Far Group

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

EXCEPTION:

Far Manager plugins that use only the following header files from this distribution (none or any): farcolor.hpp, farkeys.hpp, plugin.hpp, farcolorW.pas, farkeysW.pas and pluginW.pas; can be distributed under any other possible license with no implications from the above license on them.

GNU AFFERO GENERAL PUBLIC LICENSE

Version 3, 19 November 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

Developers that use our General Public Licenses protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License which gives you legal permission to copy, distribute and/or modify the software.

A secondary benefit of defending all users' freedom is that improvements made in alternate versions of the program, if they receive widespread use, become available for other developers to incorporate. Many developers of free software are heartened and encouraged by the resulting cooperation. However, in the case of software used on network servers, this result may fail to come about. The GNU General Public License permits making a modified version and letting the public access it on a server without ever releasing its source code to the public.

The GNU Affero General Public License is designed specifically to ensure that, in such cases, the modified source code becomes available to the community. It requires the operator of a network server to provide the source code of the modified version running there to the users of that server. Therefore, public use of a modified version, on a publicly accessible server, gives the public access to the source code of the modified version.

An older license, called the Affero General Public License and published by Affero, was designed to accomplish similar goals. This is a different license, not a version of the Affero GPL, but Affero has released a new version of the Affero GPL which permits relicensing under this license.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU Affero General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component,

and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from

a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms. "Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available

network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Remote Network Interaction; Use with the GNU General Public License.

Notwithstanding any other provision of this License, if you modify the Program, your modified version must prominently offer all users interacting with it remotely through a computer network (if your version supports such interaction) an opportunity to receive the Corresponding Source of your version by providing access to the Corresponding Source from a network server at no charge, through some standard or customary means of facilitating copying of software. This Corresponding Source shall include the Corresponding Source for any work covered by version 3 of the GNU General Public License that is incorporated pursuant to the following paragraph.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the work with which it is combined will remain governed by version 3 of the GNU General Public License.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU Affero General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU Affero General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU Affero General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU Affero General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software: you can redistribute it and/or modify it under the terms of the GNU Affero General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Affero General Public License for more details.

You should have received a copy of the GNU Affero General Public License along with this program. If not, see <http://www.gnu.org/licenses/>.

Also add information on how to contact you by electronic and paper mail.

If your software can interact with users remotely through a computer network, you should also make sure that it provides a way for users to get its source. For example, if your program is a web application, its interface could display a "Source" link that leads users to an archive of the code. There are many ways you could offer source, and different solutions will be better for different programs; see section 13 for the specific requirements.

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU AGPL, see <http://www.gnu.org/licenses/>.

GPL (GNU General Public License) 2.0

License Text

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its

contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS"

WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LGPL (GNU Lesser General Public License) 2.1

License Text

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is

especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will

automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990
Ty Coon, President of Vice

That's all there is to it!

OpenSSL 1.0

License Text

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

==========

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

/

Quest について

Quest は名前以上の存在です

Quest ではお客様のために IT をより強力にするための方法を追求しています。そのために、IT 管理に費やす時間を短縮し、ビジネス革新のためにより多くの時間をかけるためのコミュニティ主導のソフトウェアソリューションを構築しています。データセンターをモダナイゼーションしてクラウドに素早くアクセスできるようにし、データ駆動型ビジネスを成長させるために必要な専門知識、セキュリティ、アクセシビリティを提供します。革新の一部である Quest のグローバルコミュニティへの招待と、顧客満足度を確実にするため確固たるコミットメントを組み合わせることで、現在のお客様に真のインパクトを与え、Quest が誇るレガシーを残すソリューションを提供し続けています。Quest は新しいソフトウェア企業に変わることで現在の状況に挑みます。お客様のパートナーとして、お客様の情報技術がお客様のために、お客様によって確実に構築されるようにするために、たゆまぬ努力を続けます。これが Quest のミッションです。このミッションに一丸となって取り組んでいます。新しくなった Quest にようこそ。Join the Innovation™ にご招待します。

私たちのブランド、ビジョンとともに。

Quest の口ゴは、Quest の物語、革新、コミュニティ、サポートを表しています。この物語の重要な部分は、Q で始まります。この文字は完璧な円であり、技術の精度と強さへのコミットメントを表しています。Q の中の空間は、新たな Quest のコミュニティに加わる必要のある重要な部分、つまりお客様を象徴しています。

Quest へのお問い合わせ

営業窓口またはその他のお問い合わせについては、https://www.quest.com/contactを参照してください。

テクニカルサポートのリソース

テクニカルサポートは、有効な保守契約と試用版を保有している Quest のお客様を対象としています。https://support.quest.com/ja-jp から Quest サポートポータルにアクセスできます。

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。サポートポータルでは次のことを行うことができます。

- サービスリクエストの送信と管理
- サポート技術情報記事の参照
- 製品通知へのサインアップ
- ソフトウェアと技術マニュアルのダウンロード
- ハウツービデオの表示
- コミュニティディスカッションへの参加
- サポートエンジニアとのオンラインチャット
- 製品のサポートサービスの表示

用語集

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。

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。

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 つのクラスタ化メールボックスサーバ（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レプリケートされる、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、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 サーバは、お互いの不具合を監視します。Mailbox サーバが DAG に追加されると、DAG 内の他のサーバと連携して、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、パス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。この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、Rapid Recovery ライセンスポータルでアカウントを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

Rapid Recovery ライセンスポータルはウェブインタフェースです。ここで、ユーザーおよびパートナーは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、『*Rapid Recovery License Portal User Guide*』（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 およびサーバの即時リカバリを行うテクノロジです。このテクノロジにより、仮想または物理サーバ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 上の空き容量が簡単に特定されます。Oracle データベースサーバの場合、ログを（スケジュールにより、または必要に応じて手動で）切り捨てるとき、アーカイブログが削除され、領域が解放されます。同様に、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。

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 177. 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	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を使用できます (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` または `\\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 178. 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。

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。

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、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。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。

シーディングしーでぃんぐ

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ぷしょっと

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。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 データベースの前回のフルバックアップ以降に行われたデータ変更の累積コピーのことです。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（レプリカ Core 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。このテクノロジは、さまざまなファイルシステムおよびサーバをサポートします。

仮想スタンバイ

仮想スタンバイは、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。仮想スタンバイは、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 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特定のプロバイダが、各社の口ゴで 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市販することができます。

Rapid Recovery をホワイトラベル化するオプションは、Quest Software ライセンス契約により明示的にブランド変更権限を付与されている組織のみが利用できます。このソフトウェアをライセンス、サブライセンスおよび / または再配布するオプションは、これらの権限を付与する特定のライセンス契約が有効である組織にのみ付与されます。Quest Software は、Rapid Recovery に対するすべての権利を有します。ホワイトラベル化オプションは、何人に対しても Rapid Recovery に対する何らの知的財産権も付与しません。組織のためにこの機能を依頼するには、Quest Software の担当者にお問い合わせください。

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（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。