Rapid Recovery 6.11

Commands and Scripting Reference Guide

© 2026 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Rapid Recovery Commands and Scripting Reference Guide
Updated - May 2026
Version - 6.11

Contents

Introduction to Rapid Recovery **22**

Command Line Management utility **24**

Commands 25

ApplyLicense 25

Usage 25

Command Options 25

Examples: 26

Archive 26

Usage 26

Command Options 26

Examples: 29

CancelActiveJobs 31

Usage 31

Command Options 31

Example: 32

CheckRepository 32

Usage 32

Command Options 32

Example: 34

ConfigureAgentMigration 34

Usage 34

Command Options 34

Example: 35

CreateArchiveRepository 35

Usage 35

Command Options 35

Examples: 36

CreateBootCD 36

Usage 36

Command Options 37

Example: 37

CreateEncryptionKey 37

Usage 37

Command Options 37

Example: 38

CreateNASRepository 38

Usage 38

Command Options 38

Examples: 39

CreateRepository 39

Usage 39

Command Options 40
Examples: 40
DedupCacheConfig 41
Usage 41
Command Options 41
Examples: 41
DeleteReplication 42
Usage 42
Command Options 42
Example: 43
DeleteRepository 43
Usage 43
Command Options 43
Example: 44
DeleteTieredRepository 44
Usage 44
Command Options 44
Example: 44
DeployToAzure 45
Usage 45
Command Options 45
Example: 46
Dismount 47
Usage 47
Command Options 47
Example: 48
Dismount-Repository 48
Usage 48
Command Options 48
Example: 49
DismountArchiveRepository 49
Usage 49
Command Options 49
Examples: 49
DismountRemote 49
Usage 50
Command Options 50
Example: 50
EditEsxServer 51
Usage 51
Command Options 51
Examples: 51
EditHyperVCluster 52
Usage 52
Command Options 52
Example: 53
EditHyperVServer 53

Usage 53
Command Options 53
Example: 54
EditOracleDBVerifyNightlyJob 54
Usage 54
Command Options 54
Example: 55
EditOracleLogTruncationNightlyJob 55
Usage 55
Command Options 55
Examples: 56
EnableOracleArchiveLogMode 56
Usage 56
Command Options 57
Example: 57
FileSearch 57
Usage 57
Command Options 57
Examples: 58
Force 59
Usage 59
Command Options 59
Example: 59
ForceAttach 60
Usage 60
Command Options 60
Example: 60
ForceChecksum 61
Usage 61
Command Options 61
Example: 61
ForceLogTruncation 62
Usage 62
Command Options 62
Example: 62
ForceMount 62
Usage 63
Command Options 63
Example: 63
ForceOptimizationJob 63
Usage 63
Command Options 64
Example: 64
ForceReplication 64
Usage 64
Command Options 64
Example: 65

ForceRollup 65
Usage 65
Command Options 65
Example: 66
ForceScheduledArchive 66
Usage 66
Command Options 66
Examples: 67
ForceVirtualStandby 67
Usage 67
Command Options 67
Examples: 67
GetOracleInstanceMetadata 68
Usage 68
Command Options 68
Example: 68
Help 69
Usage 69
Example: 69
List 69
Usage 69
Command Options 69
Examples: 71
ListAzureVMSizes 71
Usage 71
Command Options 71
Examples: 72
ListOracleInstances 72
Usage 72
Command Options 72
Example: 73
ManagementCertificates 73
Usage 73
Command Options 73
Examples: 74
MigrateAgent 74
Usage 74
Command Options 74
Examples: 75
Mount 75
Usage 75
Command Options 75
Examples: 76
Mount-Repository 76
Usage 77
Command Options 77
Examples: 77

MountArchiveRepository 77
Usage 77
Command Options 77
Examples: 78
NewCloudAccount 78
Usage 78
Command Options 78
Examples: 79
OpenDvmRepository 80
Usage 80
Command Options 80
Example: 80
Pause 80
Usage 81
Command Options 81
Examples: 82
Protect 83
Usage 83
Command Options 83
Example: 84
ProtectCluster 84
Usage 84
Command Options 84
Example: 85
ProtectEsxServer 85
Usage 85
Command Options 85
Example: 86
ProtectHyperVCluster 86
Usage 86
Command Options 87
Example: 87
ProtectHyperVServer 87
Usage 88
Command Options 88
Example: 88
RemoveAgent 89
Usage 89
Command Options 89
Example: 89
RemoveArchiveRepository 89
Usage 89
Command Options 90
Examples: 90
RemovePoints 90
Usage 90
Command Options 90

Example: 91
RemoveScheduledArchive 91
Usage 91
Command Options 91
Examples: 92
RemoveVirtualStandby 92
Usage 92
Command Options 92
Examples: 93
Replicate 93
Usage 93
Command Options 93
Example: 94
Replication 94
Usage 94
Command Options 95
Examples: 96
ResizeDedupeCache 97
Usage 97
Command Options 97
Examples: 97
RestartCoreService 97
Usage 98
Command Options 98
Example: 98
RestoreAgent 98
Usage 98
Command Options 99
Example: 99
RestoreArchive 99
Usage 99
Command Options 100
Examples: 100
RestoreUrc 100
Usage 101
Command Options 101
Example: 101
Resume 101
Usage 102
Command Options 102
Examples: 102
ResumeScheduler 103
Usage 103
Command Options 103
Example: 103
SeedDrive 104
Usage 104

Command Options ... 104
Examples: ... 105
SetAgentMetadataCredentials ... 105
Usage ... 105
Command Options ... 105
Example: ... 106
SetOracleMetadataCredentials ... 106
Usage ... 106
Command Options ... 107
Examples: ... 107
StartExport ... 108
Usage ... 108
Command Options ... 108
Examples: ... 110
StartExportAzure ... 110
Usage ... 110
Command Options ... 111
Examples: ... 112
StartOracleDBVerifyJob ... 113
Usage ... 113
Command Options ... 113
Example: ... 114
StartOracleLogTruncationJob ... 114
Usage ... 114
Command Options ... 114
Examples: ... 115
StopCoreService ... 115
Usage ... 115
Command Options ... 116
Example: ... 116
SuspendScheduler ... 116
Usage ... 116
Command Options ... 116
Example: ... 117
UpdateRepository ... 117
Usage ... 117
Command Options ... 117
Examples: ... 118
Version ... 118
Usage ... 118
Command Options ... 119
Example: ... 119
VirtualStandby ... 119
Usage ... 119
Command Options ... 119
Examples: ... 121
Localization ... 122

PowerShell module **123**
Prerequisites for using PowerShell 124
powershell.exe.config 124
Working with commands and cmdlets 124
Getting cmdlet help and examples 124
Rapid Recovery PowerShell module cmdlets 125
Add-EsxAutoProtectObjects 125
Usage 125
Command Options 125
Example: 126
Add-EsxVirtualMachines 126
Usage 126
Command Options 126
Example: 127
Add-HyperVClusterSharedVirtualDisks 127
Usage 127
Command Options 127
Example: 128
Add-HyperVClusterVirtualMachines 128
Usage 128
Command Options 128
Example: 129
Add-HyperVVirtualMachines 129
Usage 129
Command Options 129
Example: 130
Disable-HyperVAutoProtection 130
Usage 130
Command Options 130
Example: 131
Edit-AzureVirtualStandby 131
Usage 131
Command Options 131
Example: 132
Edit-EsxiVirtualStandby 132
Usage 132
Command Options 133
Example: 133
Edit-HyperVVirtualStandby 134
Usage 134
Command Options 134
Example: 135
Edit-OracleDBVerifyNightlyJob 135
Usage 135
Command Options 135
Examples: 136

Edit-OracleLogTruncationNightlyJob ... 136
Usage ... 136
Command Options ... 137
Examples: ... 138
Edit-Replication ... 138
Usage ... 138
Command Options ... 138
Examples: ... 139
Edit-ScheduledArchive ... 139
Usage ... 139
Command Options ... 140
Example: ... 141
Edit-VBVirtualStandby ... 141
Usage ... 141
Command Options ... 142
Example: ... 143
Edit-VMVirtualStandby ... 143
Usage ... 143
Command Options ... 143
Example: ... 144
Enable-HyperVAutoProtection ... 144
Usage ... 144
Command Options ... 144
Example: ... 145
Enable-OracleArchiveLogMode ... 145
Usage ... 145
Command Options ... 145
Example: ... 146
Get-ActiveJobs ... 146
Usage ... 146
Command Options ... 146
Example: ... 147
Get-CloudAccounts ... 147
Usage ... 147
Command Options ... 147
Example: ... 148
Get-Clusters ... 148
Usage ... 148
Command Options ... 148
Example: ... 149
Get-CompletedJobs ... 149
Usage ... 149
Command Options ... 149
Example: ... 150
Get-ExchangeMailStores ... 150
Usage ... 150
Command Options ... 150

Example: 151
Get-Failed 151
Usage 151
Command Options 151
Example: 152
Get-FailedJobs 152
Usage 152
Command Options 152
Example: 153
Get-HyperVClusterSharedVirtualDisks 153
Usage 153
Command Options 153
Example: 154
Get-ListAzureVMSizes 154
Usage 154
Command Options 154
Example: 155
Get-Mounts 155
Usage 155
Command Options 155
Example: 156
Get-OracleInstances 156
Usage 156
Command Options 156
Example: 157
Get-Passed 157
Usage 157
Command Options 157
Example: 158
Get-ProtectedServers 158
Usage 158
Command Options 158
Example: 158
Get-ProtectionGroups 158
Usage 159
Command Options 159
Example: 159
Get-QueuedJobs 159
Usage 159
Command Options 159
Example: 160
Get-RecoveryPoints 160
Usage 161
Command Options 161
Example: 161
Get-ReplicatedServers 161
Usage 161

Command Options ... 162
Example: ... 162
Get-Repositories ... 162
Usage ... 162
Command Options ... 162
Example: ... 163
Get-ScheduledArchives ... 163
Usage ... 163
Command Options ... 163
Example: ... 164
Get-SqlDatabases ... 164
Usage ... 164
Command Options ... 164
Example: ... 164
Get-TransferQueueEntries ... 165
Usage ... 165
Command Options ... 165
Example: ... 165
Get-UnprotectedVolumes ... 165
Usage ... 165
Command Options ... 166
Example: ... 167
Get-Version ... 167
Usage ... 167
Command Options ... 167
Example: ... 168
Get-VirtualizedServers ... 168
Usage ... 168
Command Options ... 168
Example: ... 169
Get-Volumes ... 169
Usage ... 169
Command Options ... 170
Example: ... 170
New-AzureVirtualStandby ... 170
Usage ... 170
Command Options ... 170
Example: ... 171
New-Base ... 171
Usage ... 172
Command Options ... 172
Example: ... 172
New-BootCD ... 172
Usage ... 172
Command Options ... 173
Example: ... 173
New-CloudAccount ... 173

Usage ... 174
Command Options ... 174
Example: ... 175
New-EncryptionKey ... 175
Usage ... 175
Command Options ... 175
Example: ... 176
New-EsxiVirtualStandby ... 176
Usage ... 176
Command Options ... 176
Example: ... 177
New-FileSearch ... 178
Usage ... 178
Command Options ... 178
Examples: ... 179
New-HyperVVirtualStandby ... 179
Usage ... 179
Command Options ... 179
Example: ... 181
New-Mount ... 181
Usage ... 181
Command Options ... 181
Example: ... 182
New-Replication ... 182
Usage ... 182
Command Options ... 182
Example: ... 183
New-Repository ... 183
Usage ... 183
Command Options ... 183
Example: ... 184
New-ScheduledArchive ... 184
Usage ... 184
Command Options ... 185
Examples: ... 186
New-Snapshot ... 187
Usage ... 187
Command Options ... 187
Example: ... 188
New-VBVirtualStandby ... 188
Usage ... 188
Command Options ... 188
Example: ... 189
New-VMVirtualStandby ... 189
Usage ... 189
Command Options ... 189
Example: ... 190

Push-Replication ... 190
Usage ... 191
Command Options ... 191
Example: ... 191
Push-Rollup ... 191
Usage ... 191
Command Options ... 192
Example: ... 192
Remove-Agent ... 192
Usage ... 192
Command Options ... 192
Example: ... 193
Remove-EsxAutoProtectObjects ... 193
Usage ... 193
Command Options ... 193
Example: ... 194
Remove-HyperVClusterSharedVirtualDisks ... 194
Usage ... 194
Command Options ... 194
Example: ... 195
Remove-HyperVClusterVirtualMachines ... 195
Usage ... 195
Command Options ... 195
Example: ... 196
Remove-HyperVVirtualMachines ... 196
Usage ... 196
Command Options ... 196
Example: ... 197
Remove-Mount ... 197
Usage ... 197
Command Options ... 197
Example: ... 198
Remove-Mounts ... 198
Usage ... 198
Command Options ... 198
Example: ... 199
Remove-RecoveryPoints ... 199
Usage ... 199
Command Options ... 199
Example: ... 200
Remove-RemoteMount ... 200
Usage ... 200
Command Options ... 200
Examples: ... 201
Remove-RemoteMounts ... 201
Usage ... 201
Command Options ... 201

Example: 202
Remove-Replication 202
Usage 202
Command Options 202
Example: 203
Remove-Repository 203
Usage 203
Command Options 203
Example: 204
Remove-ScheduledArchive 204
Usage 204
Command Options 204
Example: 205
Remove-VirtualStandby 205
Usage 205
Command Options 205
Example: 205
Restart-CoreService 206
Usage 206
Command Options 206
Example: 206
Resume-Replication 206
Usage 206
Command Options 207
Example: 207
Resume-ScheduledArchive 208
Usage 208
Command Options 208
Examples: 208
Resume-Snapshot 209
Usage 209
Command Options 209
Example: 209
Resume-VirtualStandby 209
Usage 210
Command Options 210
Example: 210
Set-AgentMetadataCredentials 210
Usage 210
Command Options 211
Example: 211
Set-DedupCacheConfiguration 211
Usage 211
Command Options 212
Examples: 212
Set-License 212
Usage 213

Command Options 213
Examples: 213
Set-OracleMetadataCredentials 214
Usage 214
Command Options 214
Examples: 215
Start-Archive 215
Usage 215
Command Options 216
Example: 220
Set-ReplicationResponse 220
Usage 221
Command Options 221
Examples: 221
Start-AttachabilityCheck 221
Usage 222
Command Options 222
Example: 222
Start-AzureDeploy 223
Usage 223
Command Options 223
Examples: 224
Start-AzureExport 225
Usage 225
Command Options 225
Examples: 227
Start-ChecksumCheck 228
Usage 228
Command Options 228
Example: 229
Start-ConsumeSeedDrive 229
Usage 229
Command Options 229
Examples: 230
Start-CopySeedDrive 230
Usage 230
Command Options 230
Examples: 231
Start-EsxiExport 231
Usage 232
Command Options 232
Start-HypervExport 233
Usage 233
Command Options 233
Example: 235
Start-LogTruncation 235
Usage 235

Command Options 235
Example: 236
Start-MountabilityCheck 236
Usage 236
Command Options 236
Example: 237
Start-MigrateAgent 237
Usage 237
Command Options 237
Example: 237
Start-OptimizationJob 238
Usage 238
Command Options 238
Example: 238
Start-OracleDBVerifyJob 238
Usage 239
Command Options 239
Example: 239
Start-OracleLogTruncationJob 239
Usage 239
Command Options 240
Examples: 240
Start-Protect 241
Usage 241
Command Options 241
Example: 242
Start-ProtectCluster 242
Usage 242
Command Options 242
Example: 243
Start-ProtectEsxServer 243
Usage 243
Command Options 243
Example: 244
Start-ProtectHyperVCluster 244
Usage 244
Command Options 244
Example: 245
Start-ProtectHyperVServer 245
Usage 245
Command Options 246
Example: 246
Start-RepositoryCheck 246
Usage 246
Command Options 247
Example: 247
Start-RestoreAgent 247

Usage 247
Command Options 247
Example: 248
Start-RestoreArchive 248
Usage 248
Command Options 249
Example: 249
Start-ScheduledArchive 250
Usage 250
Command Options 250
Example: 250
Start-VBExport 250
Usage 251
Command Options 251
Example: 252
Start-VirtualStandby 252
Usage 252
Command Options 252
Example: 254
Start-VMExport 254
Usage 254
Command Options 254
Example: 255
Stop-ActiveJobs 255
Usage 256
Command Options 256
Example: 256
Stop-CoreService 257
Usage 257
Command Options 257
Example: 257
Suspend-Replication 257
Command Options 258
Example: 258
Suspend-ScheduledArchive 259
Usage 259
Command Options 259
Example: 259
Suspend-Scheduler 260
Usage 260
Command Options 260
Example: 260
Suspend-Snapshot 260
Usage 260
Command Options 261
Example: 261
Suspend-VirtualStandby 261

Usage 261
Command Options 261
Example: 262
Suspend-VMExport 262
Usage 262
Command Options 262
Example: 263
Update-Repository 263
Usage 263
Command Options 263
Example: 264
Localization 264
Qualifiers 264

Scripting 266
Using PowerShell scripting with Rapid Recovery 266
Prerequisites for PowerShell scripting 266
powershell.exe.config 267
Testing PowerShell Scripts 267
Localization 267
Qualifiers 267
Input Parameters for PowerShell Scripting 268
AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents) 268
AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer) 269
BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs) 270
ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks) 271
DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange) 271
ExportJobRequest (namespace Replay.Core.Contracts.Export) 271
NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql) 271
RollupJobRequest (namespace Replay.Core.Contracts.Rollup) 272
TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer) 272
TransferJobRequest (namespace Replay.Core.Contracts.Transfer) 272
TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution) 274
TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution) 274
TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution) 277
VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization) 277
VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints) 278
VolumeName (namespace Replay.Common.Contracts.Metadata.Storage) 278
VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage) 278
VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer) 279
VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer) 279
Sample PowerShell scripts 279
PreTransferScript.ps1 279

PostTransferScript.ps1 280
PreExportScript.ps1 280
PostExportScript.ps1 281
PreNightlyJobScript.ps1 282
PostNightlyJobScript.ps1 283
Using Bourne shell and Bash scripting with Rapid Recovery 286
Prerequisites for shell scripting 286
Execution timing for pre and post scripts 287
Supported transfer and post-transfer script parameters 287
Testing shell scripting 288
Input parameters for shell scripting 288
TransferPrescriptParameters_VolumeNames 288
TransferPostscriptParameter 289
Sample shell scripts 290
PreTransferScript.sh 291
PostTransferScript.sh 291
PreSnapshotScript.sh 292
PostSnapshotScript.sh 292
PostExportScript.sh 292

About us **294**
Technical support resources 294

Introduction to Rapid Recovery

Rapid Recovery is a backup, replication, and recovery solution that offers near-zero recovery time objectives and recovery point objectives. Rapid Recovery offers data protection, disaster recovery, data migration and data management. You have the flexibility of performing bare-metal restore (to similar or dissimilar hardware), and you can restore backups to physical or virtual machines (VMs), regardless of origin. Rapid Recovery lets you create backup archives to a wide range of supported systems including archiving to the cloud. With Rapid Recovery, you can replicate to one or more targets for added redundancy and security.

Rapid Recovery offers:

- **Flexibility**. You can perform universal recovery to multiple platforms, including restoring from physical to virtual, virtual to physical, virtual to virtual, and physical to physical.
- **Cloud integration**. You can export a VM, archive and replicate to the cloud, and perform bare metal restore from archives in the cloud. Compatible cloud services include Microsoft Azure, Amazon Web Services (AWS), any OpenStack-based provider (including Rackspace), and Google Cloud. US government-specific platforms include AWS GovCloud (US) and Azure Government. Pruning from cloud storage also supports scheduled ones to reduce storage costs.
- Pruning from cloud storage also supported for scheduled one to reduce storage cost.
- **Intelligent deduplication**. You can reduce storage requirements by storing data once, and referencing it thereafter (once per repository or encryption domain).
- **Live Recovery**. Using the Live Recovery feature of Rapid Recovery Agent, you have instant access to critical data first, while remaining restore operations complete in parallel. You can use Live Recovery to restore data from a recovery point of any non-system volume of a Windows machine, physical or virtual. Live Recovery is not supported for agentlessly protected machines, Linux machines, or cluster-shared volumes.
- **File-level recovery**. You can recover data at the file level on-premises, from a remote location, or from the cloud.
- **File-level search**. Using criteria you specify, you can search a range of recovery points for one or more files. From the search results, you can then select and restore the files you want to the local Core machine directly from the Rapid Recovery Core Console.
- **Virtual machine export**. Rapid Recovery supports one-time virtual export, letting you generate a VM from a recovery point; and virtual standby, in which the VM you generate is continually updated after each backup. Compatible VM hypervisors include VMware vCenter/ESXi, VMware Workstation, Microsoft Hyper-V, Oracle VM VirtualBox, and Microsoft Azure. You can even perform virtual export to Hyper-V cluster-shared volumes.
- **Rapid Snap for Virtual support**. Enhanced support for virtualization includes agentless protection for vCenter/ESXi VMs and for Hyper-V VMs. Rapid Snap for Virtual includes protection and autodiscovery for VMware ESXi 6.0 and higher with no software agent installed. Host-based protection supports installing Rapid Recovery Agent on a Microsoft Hyper-V host only, letting you agentlessly protect all its guest VMs.
- **Application support**. Rapid Recovery is built with application support. When you protect SQL Server or Microsoft Exchange machines (whether using Rapid Recovery Agent or agentless protection), the backup snapshots captured are automatically application-aware; open transactions and rolling transaction logs are completed and caches are flushed to disk before creating snapshots. Specific application features are supported, including SQL attachability checks (for SQL Server) and database checksum and mountability checks (for Exchange Server). If you protect Oracle 12c or 18c servers with Rapid Recovery Agent, you can also perform DBVERIFY database integrity checks.

See the following resources for more information about Rapid Recovery.

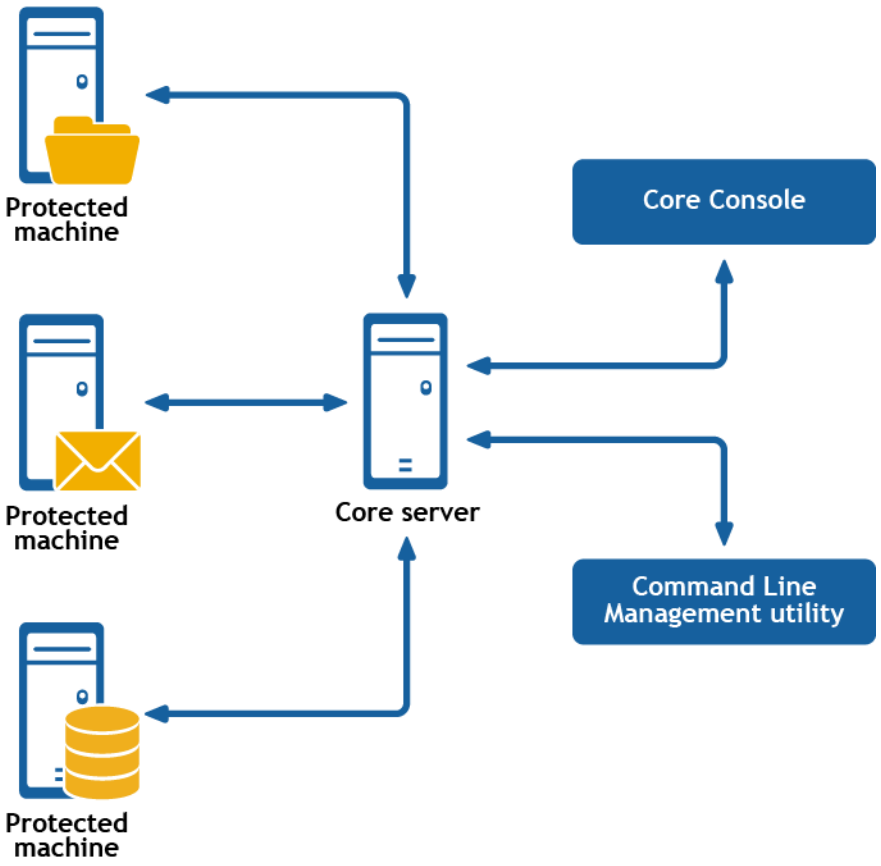
- The Rapid Recovery product support website at https://support.quest.com/rapid-recovery/.
- The documentation website at https://support.quest.com/rapid-recovery/technical-documents/.

Command Line Management utility

Rapid Recovery consists of several software components. Key components relevant to this topic include the following:

- The Rapid Recovery Core manages authentication for protected machines, schedules for transferring data for backup and replication, export to virtual machines, reporting, and bare metal restore (BMR) to similar or dissimilar hardware.
- The Rapid Recovery Agent is responsible for volume snapshots and fast transfer of the data to the repository managed by the Core.
- The Rapid Recovery Command Line Management utility, cmdutil.exe, provides third-party access to manage system functionality. This tool permits scripting of the Rapid Recovery Core management functions.

Rapid Recovery Command Line Management provides command-line functions



Rapid Recovery Command Line Management is a Windows command line utility that lets users interact with the Rapid Recovery Core server. It offers some of the same functions that the Rapid Recovery Core Console graphic user interface provides. For example, Rapid Recovery Command Line Management utility can mount recovery points or force a snapshot.

The Rapid Recovery Command Line Management utility is embedded in every installation of the Rapid Recovery Core. To open the Command Line Management utility for a default installation, open the Command Prompt with Run as Administrator, and change the directory to the path C:\Program Files\AppRecovery\Core\CoreService\, which is the location of the `cmdutil.exe` file. From this directory, you can pass action flags to the Rapid Recovery

Command Line Management utility through a selection of command options and qualifiers to perform limited management functions.

Commands

This section describes the commands and options available for the Rapid Recovery Command Line Management utility.

ApplyLicense

There may be times when you need to change the Rapid Recovery license applied to a machine, such as when moving from a trial license to a subscription or perpetual license. In such instances, you can change the license in the Command Prompt by using the `applylicense` command.

Usage

The usage for the command is as follows:

```
/applylicense -core [host name] -user [user name] -password [password] -licensekey [license key] -licensepath [license file path] -licensenumber [license number] -email [email address]
```

Command Options

The following table describes the options available for the `applylicense` command:

Table 1: ApplyLicense command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-licensekey`	Optional. A 30-character key comprising six groups of five alphanumeric characters, each separate by a hyphen. Use this key when a license file is not available.
`-licensepath`	Optional. The path to the file that ends with the .lic extension. If a license file is available, you can use this option instead of the `-licensekey`.
`-licensenumber`	Optional. You may have received this nine-digit license number in an order confirmation

Option	Description
	email. If you provide this number, use the email address that received it for verification.
`-email`	Optional. If you use the `-licensenumber`, you must include the email address that received it for verification.

Examples:

Change the license key associated with this Core to JL09F-89FSD-6THFS-DSE34-KS3D5-65DF2:

```
>cmdutil /applylicense -core 10.10.10.10 -user admin -password 676df#df -licensekey
JL09F-89FSD-6THFS-DSE34-KS3D5-65DF2
```

Change the license key associated with this Core to the key contained in the license file:

```
>cmdutil /applylicense -core 10.10.10.10 -user admin -password 676df#df -licensepath
C:\MyLicenseFile.lic
```

Change the license number associated with this Core to 111-111-111 using john.doe@example.com to verify the license:

```
>cmdutil /applylicense -core 10.10.10.10 -user admin -password 676df#df -
licensenumber 111-111-111 -email john.doe@example.com
```

Archive

Businesses often use long-term storage to archive both compliant and non-compliant data. The archive feature in Rapid Recovery supports extended retention for compliant and non-compliant data. The administrator can save an archive on the local storage or network location by specifying the `-path` parameter and credentials.

Usage

The usage for the command util/archive is as follows:

```
/archive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP
address2]"] -path [location] -startdate [time string] enddate [time string] -
archiveusername [name] -archivepassword [password] -archiveCredentialsVaultAccount
[id | user name | description] -comment [text] -cloudaccountname [name] -
cloudcontainer [name] -recycleaction [type] -scheduletype [type] -dayofweek [name] -
dayofmonth [number] -time [time] -usecompatibleformat -scheduled -edit -id [id] -
initialpause -useglacierfordatafiles -legalhold -retentionmode ["governance" |
"compliance"] -retain [number of days] -vaultretain [number of days] -vaultlegalhold
-archiveretention [months]
```

Command Options

The following table describes the options available for the `archive` command:

Table 2: Archive command options

Option	Description
-core	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
-user	Optional. Login to the remote core host machine. If you specify a login you also have to provide a password. If none are provided then the logged-in user's credentials will be used.
-password	Optional. Password to the remote core host machine. If you specify just a login then you're prompted to enter a password. When none are provided then the logged in user's credentials will be used.
-all	Archive recovery points for all protected machines on the core.
-protectedserver	Protected Protected machine with recovery points to be archived. You can specify several machine names enclosed in double quotes and separated by space.
-path	Path where archived data will be placed. For instance, "d:\work\archive", network path "\\servername\sharename" or folder on the cloud "Some Folder Name".
-startdate	Is not supported for scheduled archive. Start date to select recovery points by creation date. Value must be enclosed in double quotes.
-enddate	Optional. Is not supported for scheduled archive. End date to select recovery points by creation date. Value must be enclosed in double quotes. By default, the current system time is used.
-archiveusername	Optional. Login to the remote machine. Required for network path only.
-archivepassword	Optional. Password to the remote machine. Required for network path only.
-archiveCredentialsVaultAccount	Optional. Id, user name or description of the account stored in the Credentials Vault which has credentials to the remote machine. Required for network path only.
-comment	Optional. Is not supported for scheduled archive. Comment text must be enclosed in double quotes. Example: -comment "some comment goes here ...".
-usecompatibleformat	Is not supported for scheduled archive. New format offers better performance however it is not compatible with older Cores. Use this flag to create archive with old compatible format.
-cloudaccountname	Optional. Name of the cloud account, where archive will be saved to.
-cloudcontainer	Optional. Name of the cloud container in the chosen cloud account, where archive will be saved to. "-cloudaccountname" parameter should be specified.
-recycleaction	Specifies one of the following recycle action types:

Option	Description
	• `donotreuse` - Is not supported for scheduled archive. Does not overwrite or clear any existing archived data from the location. If the location is not empty, the archive write fails. • `replacethiscore` - Overwrites any pre-existing archived data pertaining to this core but leaves the data for other cores intact. • `erasecompletely` - Clears all archived data from the directory before writing the new archive. • `incremental` - Lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.
`-scheduled`	Optional. Specify this option to configure a scheduled archive job.
`-edit`	Optional. Only for scheduled archives. Specify this option to edit existed configuration of scheduled archive.
`-id`	ID of the scheduled archive to edit.
`-scheduletype`	Type of schedule interval. Should be specified by one of the next four values: • `daily` - For daily automatically created archives. • `weekly` - For weekly automatically created archive. Need to specify "-dayofweek" parameter. • `monthly` - For monthly automatically created archive. Need to specify "-dayofmonth" parameter. If there are less days in month than specified, the archive will be ignored. • `lastdayofmonth` - For automatically created archive at every last day of month.
`-dayofweek`	Only for "weekly" option of "-scheduletype" parameter. Day of the week on which to automatically create the archive (for example, "Monday", "Friday" etc.).
`-dayofmonth`	Only for "month" option of "-scheduletype" parameter. Day of the month on which to automatically create the archive (number).
`-time`	The hour of the day you want to create an archive.
`-initialpause`	Optional. Specify if you want to configure initial pause archiving.
`-useglacierfordatafiles`	Optional. Only for cloud archiving to Amazon. Use Glacier for data files.
`-legalhold`	Optional. Supported only for Amazon S3! "Legal hold" object locking mode. Provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it. Legal holds are independent from retention periods.

Option	Description
-retentionmode	Optional. Supported only for Amazon S3! Retention period and retention mode are always configured in tandem, unlike legal holds, which are configured independently. S3 Object Lock provides two retention modes that apply different levels of protection to your archives: • governance mode - In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. • compliance mode - In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, you cannot change the retention mode, and you cannot shorten the retention period. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.
-retain	Optional. Supported only for Amazon S3! Specifies a fixed period of time during which an object remains locked. During this period, your object is WORM-protected and can't be overwritten or deleted.
-vaultlegalhold	Optional. Supported only for Amazon Glacier! "Legal hold" Vault locking mode. Provides the same protection as a retention period, but it has no expiration date.
-vaultretain	Optional. Supported only for Amazon Glacier! Specifies a fixed period of time during which an Vault remains locked. During this period, your vault is WORM-protected and can't be overwritten or deleted.
-archiveretention	Optional. Number of months to retain archived recovery points. Archived recovery points older than the specified number of months will be automatically removed.

Examples:

Archive all recovery points with creation dates starting from 04/30/2012 02:55:00 PM for all machines on the core:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
"d:\work\archive" -startdate "04/30/2012 02:55:00 PM" -all -recycleaction
replacethiscore
```

Archive all recovery points to Amazon S3 cloud storage with creation dates starting from 12/31/2023 12:00:00 PM for specified machine on the core, set object lock mode "Legal hold" and retention mode "Governance" with retain period of 5 days:

```
>cmdutil /archive -protectedserver localhost -cloudaccountname "storage account
name" -cloudcontainer "bucket-01" -path "Archive-0000001" -startdate "12/31/2023
12:00:00 PM" -recycleaction donotreuse -legalhold -retentionmode governance -
retain 5
```

Archive all recovery points to Amazon S3 cloud storage with creation dates starting from 12/31/2023 12:00:00 PM for specified machine on the core, set object lock mode "Legal hold" and retention mode "Governance" with retain period of 5 days. Setup Glacier with retention period of 10 days:

```
>cmdutil /archive -protectedserver localhost -cloudaccountname "storage account
name" -cloudcontainer "bucket-01" -path "Archive-0000001" -startdate "12/31/2023
12:00:00 PM" -recycleaction donotreuse -legalhold -retentionmode governance -retain
5 -useglacierfordatafiles -vaultretain 10
```

Archive recovery points that fall within a date range for 2 protected machines:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate
"04/30/2012 02:55:00 PM" -enddate "05/31/2012 11:00:00 AM" -recycleaction
erasecompletely
```

Archive all recovery points to the cloud storage:

Create incremental archive for all recovery points with creation dates starting from 04/30/2012 02:55:00 PM for all machines on the core on the cloud with account name "Amazon S3" and container named "Container":

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
"ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -
startdate "04/30/2012 02:55:00 PM" -all -recycleaction incremental
```

Create weekly initially paused scheduled archive for machine 10.20.30.40 with replacing pre-existing archived data pertaining to this core:

```
>cmdutil /archive -scheduled -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.20.30.40 -path "d:\work\archive" -recycleaction
replacethiscore -scheduletype weekly -dayofweek thursday -time "10:00 PM" -
initialpause
```

Create scheduled archive for last day of every month for machine 10.20.30.40 with replacing pre-existing archived data pertaining to this core:

```
>cmdutil /archive -scheduled -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.20.30.40 -path "d:\work\archive" -recycleaction
replacethiscore -scheduletype lastdayofmonth -time "10:00 PM"
```

Create scheduled archive with archive pruning period 10 months scheduled for last day of every month for machine 10.20.30.40 with recycle action incremental. Pruning is supported only by recycle action incremental:

```
>cmdutil /archive -scheduled -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.20.30.40 -path "d:\work\archive" -recycleaction
incremental -scheduletype lastdayofmonth -time "10:00 PM" -archiveretention "10"
```

Edit the path of existed scheduled archive configuration:

```
>cmdutil /archive -scheduled -edit -id F595F697-2126-4F77-AE93-27AE2A022AF1 -
protectedserver 10.20.30.40 -path "d:\work\Newarchive"
```

Edit the path and scheduletype of existed scheduled archive configuration:

```
>cmdutil /archive -scheduled -edit -id F595F697-2126-4F77-AE93-27AE2A022AF1 -
protectedserver 10.20.30.40 -path "d:\work\Newarchive" -scheduletype daily -time
"10:00 PM"
```

Edit scheduled archive configuration to enable archive pruning for period of 5 months:

```
>cmdutil /archive -scheduled -edit -id F595F697-2126-4F77-AE93-27AE2A022AF1 -
protectedserver 10.20.30.40 -path "d:\work\Newarchive" -archiveretention "5"
```

CancelActiveJobs

Use the `cancelactivejobs` command to cancel the execution of all in-progress jobs of a specific type, such as transfer or replication.

Usage

The usage for the command is as follows:

```
/cancelactivejobs [-protectedserver [name : IP address] : -a[ll]] -core [host name]
-user [user name] -password [password] -jobtype [job type filter]
```

Command Options

The following table describes the options available for the `cancelactivejobs` command:

Table 3: CancelActiveJobs command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote core host machine. If you specify a password, you must also provide a user name. If none is provided, the logged-in user's credentials are used.
`-protectedserver`	Determines the protected machine on which the jobs should be canceled.
`-all`	Select and cancel events of specified type for all protected servers.
`-jobtype`	Optional. Specifies job type filter. Available values are: • 'transfer' (data transfer) • 'repository' (repository maintenance) • 'replication' (local and remote replications) • 'backup' (backup and restore)

Option	Description
	• 'bootcdbuilder' (create boot CDs) • 'diagnostics' (upload logs) • 'exchange' (Exchange Server files check) • 'export' (recovery point export) • 'pushinstall' (deploy agents) • 'restore' (recovery point restore) • 'rollup' (recovery point rollups) • 'sqlattach' (agent attachability checks) • 'mount' (mount repository) By default, all jobs of the specified type are canceled.

Example:

Cancel all transfer jobs on Core 10.10.10.10:

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd -jobtype transfer
```

CheckRepository

You can use the CheckRepository command to verify the integrity of an existing DVM repository created in AppAssure Core or Rapid Recovery Core.

Usage

The usage for the command is as follows:

```
/checkrepository -repository [repository name] | -all [check all repositories] -core
[host name] -user [user name] -password [password] name] -force
```

Command Options

The following table describes the options available for the `CheckRepository` command:

Table 4: CheckRepository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine

Option	Description
	IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Optional. This option checks all DVM repositories associated with the Core.

Option	Description
`-repository`	The name of the DVM repository. Optional.
`-force`	This option performs the check without your confirmation.

Example:

Start checking the DVM repository:

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user
administrator -password 23WE@#$sdd
```

ConfigureAgentMigration

This command lets you move the recovery points of a protected machine from an AppAssure repository to a Rapid Recovery repository. This command also reassigns the protected machine to the new repository.

Usage

The usage for the command is as follows:

```
/configureagentmigration -core [host name] -user [user name] -password [password]
name] -agentname [name of the protected machine] -targetrepository [repository name]
-lastrecoverypointdate [MM/dd/yyyy HH:mm:ss tt] -asnightlyjob
```

Command Options

The following table describes the options available for the `ConfigureAgentMigration` command:

Table 5: ConfigureAgentMigration command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.

Option	Description
-agentname	The name of the protect machine you want to migrate.
-targetrepositoryname	The name of the repository to which you want to migrate the protected machine.
-lastrecoverypointdate	Optional. The date and time of the last recovery point you want to migrate. Migration will not occur for recovery points older than the specified date and time. If you do not specify a date and time, then all recovery points for the protected machine will migrate.
-asnightlyjob	Optional. Use this option if you want the command to occur as a nightly job rather than during peak business hours.

Example:

Migrate the protected machine from an AppAssure repository to a Rapid Recovery repository:

```
>cmdutil /configureagentmigration -agentname localhost -targetrepositoryname
repository1 -lastRecoveryPointDate "10/15/2014 3:19:10 PM" -asNightlyJob
```

CreateArchiveRepository

When you create an archive repository, you create a destination for the contents of a scheduled archive. This feature lets you mount an archived recovery point and restore a machine without importing the archive.

Usage

The usage for the command is as follows:

```
/createarchiverepository -core [host name] -user [user name] -password [password]
name] -name [archive repository name] -path [path to the archive] -archiveusernamme
[network user name] -archivepassword [network password] -cloudaccountname [name of
the cloud account] -cloudcontainer [name of the cloud container]
```

Command Options

The following table describes the options available for the `CreateArchiveRepository` command:

Table 6: CreateArchiveRepository command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.

Option	Description
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-name	Required. The name of the archive repository.
-path	The path to the existing archive. It can be a local, network, or cloud location. For example: d:\work\archive or \\servername\sharename.
-archiveusername	Optional. This option is the login to the remote machine. It is required for a network path only.
-archivepassword	Optional. This option is the password for the remote machine. It is only required for a network path only.
-cloudaccountname	Optional. This option is the display name for an existing cloud account. It is required for a cloud path only.
-cloudcontainer	Optional. The cloud container is where the archive is located. It is required for a cloud path only.

Examples:

Create an archive repository with the name "NewArchive:"

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user
administrator -password 23WE@#$sdd -path d:\work\archive
```

Additionally, if an archive contains more than one location, then the command should include paths for all of the segments ordered from 1 to N, where N equals the number of segments.

Create an archive repository with the name "NewSegmentArchive:"

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1
\\RemmoteServer1\Share\Archive\Segment1 - archiveusername1 Administrator -
archivepassword1 23WE@#$sdd -path2 Archives\NewSegment -cloudcontainer2
ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work\archive\Third
```

CreateBootCD

This command lets you create a bare metal restore (BMR) boot CD without using the Rapid Recovery Core Console.

Usage

The usage for the command is as follows:

```
/createbootcd -ip [IP address] -mask [mask] -defaultgateway [defaultgateway] -
dnsserver [dnsserver] -vncpassword [vncpassword] -vncport [vncport] -isofilepath
[destination for the boot image]
```

Command Options

The following table describes the options available for the `CreateBootCD` command:

Table 7: CreateBootCD command options

Option	Description
`-?`	Display this help message.
`-ip`	Optional. This option specifies the IP address of the target BMR machine. By default, it generates automatically.
`-mask`	Optional. This option specifies the subnet mask of the target BMR machine. By default, it generates automatically.
`-defaultgateway`	Optional. This option specifies the default gateway of the target BMR machine. By default, it generates automatically.
`-dnsserver`	Optional. This option specifies the DNS server for the target BMR machine. By default, it generates automatically.
`-vncpassword`	Optional. This option specifies the user password for an existing UltraVNC account. By default, this option is empty.
`-vncport`	Optional. This option specifies the port to use for UltraVNC. You can change it only if you used the `-vncpassword` option. By default, the port is 5900.
`-isofilepath`	Optional. This option specifies the patch to the boot CD file. The default path is C:\ProgramData\AppRecovery\Boot CDs.

Example:

Create a boot CD:

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway
192.168.20.2 -dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateEncryptionKey

The `createencryptionkey` command lets you create a phrase to use for securing the data associated with a specified Core.

Usage

The usage for the command is as follows:

```
/createencryptionkey -core [host name] -user [user name] -password [password name] -
name [encryption key name] -comment [comment or description of key]
```

Command Options

The following table describes the options available for the `CreateEncryptionKey` command:

Table 8: CreateEncryptionKey command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Required. The name of the repository.
`-passphrase`	The passphrase of the encryption key that you want to create.
`-comment`	Optional. A comment on or a description of the encryption key that you want to create.

Example:

Create an encryption key without a comment:

```
>cmdutil /createencryptionkey -name EKname -passphrase password
```

Create an encryption key with a comment:

```
>cmdutil /createencryptionkey -name EKname -passphrase password -comment "This is a comment."
```

CreateNASRepository

Use the `createnasrepository` command to create a new NAS repository in Azure.

Usage

The usage for the command when creating a NAS repository is as follows:

```
/createnasrepository -name [repository name] -storageaccountid [storageaccountid] -datadirectory [datadirectory] -maxsize [maxsize] -dedupecachesize [dedupecachesize] -concurrentOperations [concurrentOperations] -comment [comment] -core [host name] -user [login] -password [password]
```

Command Options

The following table describes the options available for the `createnasrepository` command:

Table 9: CreateNASRepository command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Repository name.
`-storageccountid`	ID of the Azure storage account that will serve as the container for repository data.
`-datadirectory`	Path to a directory on the local file system for storing deduplication and metadata caches, index files, logs, and other information.
`-maxsize`	Maximum size of repository. Available units are GB and TB.
`-dedupecachesize`	Optional. Amount of memory to be allocated for deduplication cache. Available units are B, KB, MB, and GB. The default value is 1.5 GB.
`-comment`	Optional. Description of repository.
`-concurrentoperations`	Optional. Maximum number of operations that can be pending at one time. Value by default: 64.

Examples:

Create a NAS repository:

```
>cmdutil /createnasrepository -name "Repository 1" -storageaccountid AzureStorageID
-maxsize 200 Gb -datadirectory d:\repository\data -core 10.10.10.10:8006 -user
administrator -password 23WE@#$sdd
```

CreateRepository

Use the `createrepository` command to create a new DVM repository on a local machine or on a shared location.

Note: This command is deprecated.

Usage

The usage for the command when creating a DVM repository is as follows:

```
/createrepository -name [repository name] -size [size allocated for repository] [[-
datapath [datapath] -metadatapath [metdatapath] -uncpath [path for data and
metadata] -shareusername [user name for share location] -sharepassword [password for
```

```
share user name] -concurrentoperations [number of operations to occur at one time] -
core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `createrepository` command:

Table 10: CreateRepository command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Repository name.
`-size`	Size of repository storage location. Available units are b, Kb, Mb, Gb, Tb, and Pb.
`-datapath`	For local location only. Determines data path of repository storage location.
`-metadatapath`	For local location only. Determines metadata path of repository storage location.
`-uncpath`	For share location only. Determines data and metadata paths of repository storage location.
`-shareusername`	For share location only. Determines the user name to the share location.
`-sharepassword`	For share location only. Determines password to share location.
`-comment`	Optional. Description of repository.
`-concurrentoperations`	Optional. Maximum number of operations that can be pending at one time. Value by default: 64.

Examples:

Create a DVM repository at a local location:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath
d:\repository -metadatapath d:\repository -core 10.10.10.10:8006 -user
administrator -password 23WE@#$sdd
```

Create a DVM repository at a share location:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath
\\share\repository -shareusername login -sharepassword pass123 -comment "First
repository." -concurrentoperations 8 -core 10.10.10.10:8006 -user administrator -
password 23WE@#$sdd
```

DedupCacheConfig

This command lets you used the Command Line Utility to set the location, size, and metadata location for the primary and secondary cache of a DVM repository.

Usage

The usage for the command when creating a DVM repository is as follows:

```
/dedupcacheconfig -core [host name] -user [user name] -password [password] -primary [cache location] -secondary [cache location] -metadata [metadata location] -size [cache size] -restoredefault
```

Command Options

The following table describes the options available for the `dedupcacheconfig` command:

Table 11: DedupCacheConfig command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-primary`	Optional. Primary cache location.
`-secondary`	Optional. Secondary cache location.
`-metadata`	Optional. Metadata cache location.
`-size`	Optional. Deduplication cache size in GB.
`-restoredefault`	Optional. Restore to default deduplication cache configuration. If this parameter is specified, all other parameters are ignored.

Examples:

Set primary deduplication cache location and deduplication cache size:

```
>cmdutil /dedupcacheconfig -primary D:\primary -size 6
```

Set secondary and metadata deduplication location:

```
>cmdutil /dedupcacheconfig -secondary D:\secondary -metadata D:\metadata
```

Restore default deduplication configuration:

```
>cmdutil /dedupcacheconfig -restoredefault
```

DeleteReplication

This command lets you remove a replication configuration from a source Core or target Core, as well as remove replicated recovery points.

Usage

The usage for the command is as follows:

```
/deletereplication -incoming [replication IDs] -outgoing [replication IDs] -deleterecoverypoints
```

Command Options

The following table describes the options available for the `DeleteReplication` command:

Table 12: DeleteReplication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-incoming`	The identifier (ID) of the incoming replication that should be deleted. It could be a remote Core ID or a host name. Use the word "all" to delete all replications. **Note:** You can specify different protected machines for different replications by using the following pattern: `Replication1:Agent1,Agent2;Replication2:Agent2,Agent3`. If you do not specify a machine after the colon (:), the replication is deleted for all replicated machines.
`-outgoing`	The identifier (ID) of the outgoing replication that should be deleted. It could be a remote Core ID or a host name. Use the word "all" to delete all replications. **Note:** You can specify different protected machines for different replications by using the following pattern: `Replication1:Agent1,Agent2;Replication2:Agent2,Agent3`. If you do not specify a machine after the colon (:), the replication is deleted for all replicated machines.
`-deletepoints`	Specify which recovery points, if any, of the replicated machine that you want to remove.

Example:

Delete all incoming and all outgoing replications:

```
>cmdutil /deletereplication -incoming all -outgoing all
```

Delete two outgoing replications with all machines:

```
>cmdutil /deletereplication -outgoing TargetCore1;TargetCore2
```

Delete one protected machine from incoming replication and delete recovery points:

```
>cmdutil /deletereplication -incoming TargetCore1:10.10.10.10 -deletepoints
```

DeleteRepository

You can use the DeleteRepository command to remove an entire DVM repository created in AppAssure Core or Rapid Recovery Core.

NOTE: This command is deprecated.

Usage

The usage for the command is as follows:

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name [repository name] | -a [all repositories]
```

Command Options

The following table describes the options available for the `DeleteRepository` command:

Table 13: DeleteRepository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-a`	Optional. This option deletes all DVM repositories associated with the Core.
`-name`	The name of the DVM repository you want to delete.

Example:

Delete all DVM repositories:

```
>cmdutil /deleterepository -a
```

Delete the repository with the name "RepositoryName:"

```
>cmdutil /deleterepository -name RepositoryName
```

DeleteTieredRepository

You can use the `DeleteTieredRepository` command to remove a tiering repository created from a Rapid Recovery Core.

NOTE: This command is deprecated.

Usage

The usage for the command is as follows:

```
/deletetieredrepository -name [repository name] -deletecontent [delete all repository content] -rdshost [tiered repository host name]
```

Command Options

The following table describes the options available for the `DeleteTieredRepository` command:

Table 14: DeleteTieredRepository command options

Option	Description
`-?`	Display this help message.
`-name`	Required. The name of the tiered repository.
`-deletecontent`	Required. Specifies whether all repository content should be deleted. If you want to delete all, use `true`; if you do not want to delete all content, use `false`.
`-rdshost`	Optional. The name of the tiered repository host, such as the DR server. Use this option when the repository does not exist on the current Core.

Example:

Delete tiering repository:

```
>cmdutil /deletetieredrepository -name NewTieredRepo -deletecontent true -rdshost localhost
```

DeployToAzure

You can use the `deploytoazure` command to export a virtual machine (VM) to a Microsoft Azure cloud account.

Usage

The usage for the command is as follows:

```
/deploytoazure -core [host name] -user [user name for Core]
               -password [password for Core] -protectedserver [name | IP
address] -volumes
               [volume names | all] -destinationcontainer [Azure destination
container]
               -deploymentname [name of deployment] -subscriptionid [Azure
subscription ID]
               -cloudservicename [cloud service name] -vmname [virtual machine
name] -vmsize
               [virtual machine size] -endpointname [rdp | ssh] -protocol [tcp
| udp]
               -publicremoteaccessport [public port number] -
privateremoteaccessport [private
               port number]
```

Command Options

The following table describes the options available for the `DeployToAzure` command:

Table 15: DeployToAzure command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points that you want to export.
`-volumes`	Optional. List of additional volume names for the deploy. If you use the value `all` or use no value, then all volumes deploy.
`-destinationcontainer`	The name of the Azure destination container you want to use for the deploy.
`-deploymentname`	The name of the deployment.

Option	Description
-subscriptionid	The Azure subscription ID.
-cloudservicename	The name of the Azure cloud service.
-vmname	The name of the virtual machine.
-vmsize	The size of the virtual machine; for example, A0, Basic_A4, or Standard_G1.
-endpointname	The Azure endpoint protocol used only for remote access rdp or ssh. The default value is rdp.
-protocol	The protocol used only for remote access tcp or udp. The default value is tcp.
-publicremoteaccessport	The public port for using remote access. The default value is 3389.
-privateremoteaccessport	The private port for using remote access. The default value is 3389.
-privateagentport	Optional. The Agent port. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-publicagentport	Optional. The external Agent port. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-privatetransferport	Optional. The TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.
-publictransferport	Optional. The external TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.

Example:

Deploy data to Azure:

```
>cmdutil /deploytoazure -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1 -subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname VirtualMachine -vmsize A0
```

Deploy data to Azure using a specified endpoint:

```
>cmdutil /deploytoazure -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -endpointname ssh -protocol udp -publicremoteaccessport
1555 -privateremoteaccessport 22
```

Deploy data to Azure with specified Agent and transfer endpoint when the `-privateagentport` option has a user-defined value of `8006`. The parameter for `-publicagentport` uses the special value `0`, which is copied from `-privateagentport`. The parameter for `-privatetransferport` uses the special value `0`, which is taken from the Agent configuration. The parameter for `-publictransferport` uses the special value `0`, which is copied from `-privatetransferport`:

```
>cmdutil /deploytoazure -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 8006 -publicagentport 0 -
privatetransferport 0 -publictransferport 0
```

Deploy data to Azure using all available disks:

```
>cmdutil /deploytoazure -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 8006 -publicagentport 0 -
privatetransferport 0 -publictransferport 0 -Volumes all
```

Dismount

Use the `dismount` command to dismount a mounted recovery point specified by the `-path` option, dismount points for the selected agent by the `-protectedserver` parameter, or dismount all mounted recovery points—`-all`.

Usage

The usage for the command is as follows:

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -
protectedserver [name | IP address] | -path [location]
```

Command Options

The following table describes the options available for the `dismount` command:

Table 16: Dismount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name,

Option	Description
	you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-all	Dismount all mounted recovery points.
-protectedserver	Dismount all mounted recovery points for current agent.
-path	Dismount selected mount point.

Example:

Dismount a recovery point that was mounted to folder c:\mountedrecoverypoint:

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
c:\mountedRecoveryPoint
```

Dismount-Repository

Use this command to dismount a selected mounted repository.

Usage

The usage for the command is as follows:

```
Dismount-Repository -core [host name] -user [login] -password [password] -name
[repository name]
```

Command Options

The following table describes the options available for this command:

Table 17: Dismount command options

Option	Description
-?	Display this help message.
-core	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-name	Name of a repository you want to dismount.

Example:

Dismount repository "Repository 2":

```
>Dismount-Repository -name "Repository 2"
```

DismountArchiveRepository

After retrieving the information you want from a mounted archive, you should dismount the archive to avoid potential issues.

Usage

The usage for the command is as follows:

```
/dismountarchiverepository -core [host name] -user [user name] -password [password]
name] -name [archive repository name]
```

Command Options

The following table describes the options available for the `DismountArchiveRepository` command:

Table 18: DismountArchiveRepository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Required. The name of the archive repository.

Examples:

Dismount the repository named "NewArchive:"

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user
administrator -password 23WE@#$sdd -path d:\work\archive
```

DismountRemote

Use the `dismountremote` command to dismount a mounted recovery point mounted from a remote location.

Usage

The usage for the command is as follows:

```
/dismountremote -core [host name] -user [user name] -password [password] [-all | -protectedserver [name | IP address] | -protectedserver [name | IP address] -path [location]
```

Command Options

The following table describes the options available for the `dismountremote` command:

Table 19: DismountRemote command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Dismount all mounted recovery points.
`-protectedserver`	Dismount all mounted recovery points for current agent.
`-path`	Dismount selected mount point.

Example:

Dismount a remotely mounted recovery point by a specific path:

```
>cmdutil /dismountremote -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver "11.11.11.11" -path "C:\ProgramData\AppRecovery\MountPoints\LMU_DESKTOP-IA8FI3J-2022-03-21T142354\F__\"
```

Dismount all remotely mounted recovery points for specified protected server:

```
>cmdutil /dismountremote -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver "11.11.11.11"
```

Dismount all remotely mounted recovery points for all protected servers:

```
>cmdutil /dismountremote -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

EditEsxServer

You can use the `editesxserver` command whenever you want to make changes to the number of VMware ESX (i) virtual machines that you want to protect agentlessly.

Usage

The usage for the command is as follows:

```
/editEsxServer -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -add | -remove -virtualMachines [virtual
machines collection | all] -autoprotect [object ID or name collection]
```

Command Options

The following table describes the options available for the `editesxserver` command:

Table 20: EditEsxServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to edit vCenter and ESX(i) objects for a specific protected machine.
`-add`	Use this option to add a specified vCenter or ESXi object.
`-remove`	Use this option to remove a specified vCenter or ESXi object.
`-virtualmachines`	Optional. This option lets you list the virtual machines that you want to protect.
`-autoprotect`	Optional. This option lets you list the new virtual machines that you want to automatically protect.

Examples:

Automatically protect specific vCenter or ESXi objects of a vCenter or ESXi server with the Core:

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1"
"Folder2"
```

EditHyperVCluster

You can use the `edithypervcluster` command whenever you want to add or remove a Hyper-V cluster or virtual machine using agentless protection.

Usage

The usage for the command is as follows:

```
/edithypervcluster -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -add | -remove -virtualMachines [virtual machines collection | all] -shareddisks [name/path collection | all]
```

Command Options

The following table describes the options available for the `edithypervcluster` command:

Table 21: EditHyperVCluster command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **NOTE:** You must enclose the name in double quotes.
`-protectedserver`	The name of the protected cluster from which you want to add or remove virtual machines or shared virtual disks.
`-add`	Use this option to add virtual machines or shared virtual disks under protection.
`-remove`	Use this option to remove a virtual machine or shared virtual disks from protection.
`-virtualmachines`	Optional. This option lets you list the clusters or virtual machines that you want to protect. Separate the names by spaces and enclose the names of virtual machines in double quotes.
`-deleterecoverypoints`	Optional. This option can only be used with the "-remove" parameter. Use it to delete all recovery points for specified virtual machines.
`-shareddisks`	Optional. List the shared virtual disks that you want to protect or remove, separated by spaces. The name of the shared virtual disk must be enclosed double quotes.

Example:

Protect a specific Hyper-V cluster with the Core:

```
>cmdutil /edithypervcluster -protectedserver 10.10.8.150 -add -shareddisks
C:\SharedDisks\Folder1
```

EditHyperVServer

You can use the `edithypervserver` command whenever you want to add or remove a Hyper-V server using agentless protection.

Usage

The usage for the command is as follows:

```
/edithypervserver -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -add | -remove -virtualmachines [virtual
machines collection | all]
```

Command Options

The following table describes the options available for the `edithypervserver` command:

Table 22: EditHyperVServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to specify Hyper-V objects for a specific protected machine.
`-add`	Use this option to add specific Hyper-V objects under protection.
`-remove`	Use this option to remove specific Hyper-V objects from protection.
`-virtualmachines`	Optional. This option lets you list the virtual machines that you want to protect. Separate the names by spaces and enclose the names of virtual machines in double quotes.

Example:

Protect all of the virtual machines for a specific Hyper-V server:

```
>cmdutil /edithypervserver -protectedserver 10.10.8.150 -add -virtualmachines all
```

EditOracleDBVerifyNightlyJob

Use the command `editoracledbverifynightlyjob` to enable or disable this nightly job for specific Oracle machines that are under protection.

Usage

The usage for the command is as follows:

```
/editoracledbverifynightlyjob -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] [-enable | -disable] [-global]
```

Command Options

The following table describes the options available for the `editoracledbverifynightlyjob` command:

Table 23: EditOracleDBVerifyNightlyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle DBVerify nightly job.
`-enable`	Use this option to enable the DBVerify nightly job for the specified protected machine.
`-disable`	Use this option to disable the DBVerify nightly job for the specified protected machine.
`-global`	Use this option to apply the specified setting as the default for this Core.
`-all`	This option applies the specified changes for every protected machine that has at least one Oracle instance installed.

Example:

Enable the Oracle DBVerify nightly job for a protected server:

```
>cmdutil /editoracledbverifynightlyjob -core 10.10.127.42 -user admin -password
676df#df -protectedserver 10.10.34.88 -enable
```

EditOracleLogTruncationNightlyJob

Use the command `editoraclelogtruncationnightlyjob` to enable or disable this nightly job for specific Oracle machines that are under protection and to set the deletion policy and retention duration for the logs.

Usage

The usage for the command is as follows:

```
/editoraclelogtruncationnightlyjob -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] [-enable | -disable] [-global] [-
usedefault] -deletionpolicy [automatic | keepnewest | keepspecificnumber] -
retentionduration [duration value] -retentionunit [day | week | month | year] -
numberoffiles [number of archive files to create]
```

Command Options

The following table describes the options available for the `editoraclelogtruncationnightlyjob` command:

Table 24: EditOracleLogTruncationNightlyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable Oracle log truncation as a nightly job.
`-enable`	Use this option to enable log truncation for the specified protected machine. This is the default option and can be omitted.
`-disable`	Use this option to disable log truncation for the specified protected machine.
`-global`	Use this option to apply the specified setting as the default for this Core.
`-all`	This option applies the specified changes for every protected machine that has at least one Oracle instance installed.

Option	Description
-usedefault	Optional. Use this option to apply the default Core settings to the specified machine, which may also be set by using the -global option.
-deletionpolicy	Optional. This option must be represented by one of the following values: • "automatic" • "keepnewest" • "keepspecificnumber"
-retentionduration	Optional. This value determines the length of time to keep a log before truncating and is constrained to positive integer values. If using the "keepnewest" value of the -deletionpolicy option, a retention duration value is required.
-retentionunit	Optional. This option identifies the time unit for the -retentionduration option. It must be represented by one of the following values: • "day" • "week" • "month" • "year"
-numberoffiles	Optional. This option sets the number of recent archive log files to keep. If using the "keepspecificnumber" value of the -deletionpolicy option, a number of files value is required.

Examples:

Enable the Oracle log truncation nightly job for a protected server:

```
>cmdutil /editoraclelogtruncationnightlyjob -core 10.10.127.42 -user admin -password
676df#df -protectedserver 10.10.34.88 -enable
```

Enable the Oracle log truncation nightly job (when -enable is the default option) for a protected server and configure the deletion policy as "keepnewest" with the logs kept for 10 days:

```
>cmdutil /editoraclelogtruncationnightlyjob -core 10.10.127.42 -user admin -password
676df#df -protectedserver 10.10.34.88 -deletionpolicy keepnewest -retentionduration
10 -retentionunit day
```

EnableOracleArchiveLogMode

Use the command enableoraclearchivelogmode to enable or disable this mode for specific Oracle machines that are under protection.

Usage

The usage for the command is as follows:

```
/enableoraclearchivelogmode -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `enableoraclearchivelogmode` command:

Table 25: EnableOracleArchiveLogMode command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle archive log mode.

Example:

Enable the Oracle archive log mode for a protected server:

```
>cmdutil /enableoraclearchivelogmode -core 10.10.127.42 -user admin -password
676df#df -protectedserver 10.10.34.88
```

FileSearch

The `filesearch` command lets you search for a specific file among the recovery points in a repository, which helps you determine which recovery point you need to mount for a restore.

Usage

The usage for the command is as follows:

```
/filesearch -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -startdate [start date] -enddate [end date]
-filemasks [file masks] -paths [paths] -subdiroff -ntfsfastoff -limitsearch
[limit search]
```

Command Options

The following table describes the options available for the `filesearch` command:

Table 26: FileSearch command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle archive log mode.
`-startdate`	The earliest date of a period within you want to conduct your search. Use the date pattern "MM/DD/YYYY HH:mm:ss AM."
`-enddate`	The latest date of a period within you want to conduct your search. Use the date pattern "MM/DD/YYYY HH:mm:ss AM."
`-filemasks`	A combination of fixed and wildcard characters to search for the file. It can be one string or an array of strings. All masks should be separated by a space; for example: `-filemasks "first" "second."`
`-paths`	Optional. If there are specific directories in which you want to search, use this option to list the paths. It can be one string or an array of strings. All directories should be separated by a space; for example: `-paths "E:\" "C:\Program Files."`
`-subdiroff`	Optional. By default, the file search is performed in subdirectories. Use this option if you want to turn this feature off and not search in subdirectories.
`-ntfsfastoff`	Optional. By default, the file search is performed using the NTFS fast algorithm. If you want to perform the search without this feature, specify this option.
`-limitsearch`	Optional. Use this option to limit the number of search results. The default value is 1000.

Examples:

Perform a file search with one file mask:

```
>cmdutil /filesearch -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.10 -filemasks "sample"
```

Perform a file search with multiple file masks in specified directories and without the NTFS fast algorithm:

```
>cmdutil /filesearch -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.10 -filemasks "sample" "second" -paths "C:\dir" -
ntfsfastoff
```

Force

The `force` command forces a snapshot of a specified protected server. Forcing a snapshot lets you force a data transfer for the current protected machine. When you force a snapshot, the transfer will start immediately or will be added to the queue. Only the data that has changed from a previous recovery point will be transferred. If there is no previous recovery point, all data on the protected volumes will be transferred.

Usage

The usage for the command is as follows:

```
/force [snapshot | base] -core [host name] -user [login] -password [password] -all |
-protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `force` command:

Table 27: Force command options

Option	Description
`-?`	Display this help message.
`-force`	Optional. Type of snapshot to create. Available values: 'snapshot' (incremental snapshot) and 'base' (base image snapshot). By default, an incremental snapshot is performed.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Force snapshots for all machines on the core.
`-protectedserver`	Force a snapshot for a specific protected machine.
`-synthetic`	Force a synthetic snapshot.

Example:

Force a snapshot for all machines on the Core:

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password
23WE@#$sdd -all
```

ForceAttach

The `forceattach` command lets you force a SQL database files attachability check. When you force an attachability check, the check begins immediately.

Usage

The usage for the command is as follows:

```
/forceattach -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Command Options

The following table describes the options available for the `forceattach` command:

Table 28: ForceAttach command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine against which to perform the attachability check.
`-rpn`	The sequential number of a recovery point against which to perform checks (run command /list rps to obtain the numbers). To perform checks against multiple recovery points with a single command, you can specify several numbers separated by spaces.
`-time`	Select a recovery point by its creation time. You must specify the exact time in the format “mm/dd/yyyy hh:mm tt” (for example, “2/24/2012 09:00 AM”). Keep in mind to specify the date and time values of the time zone set on your PC.

Example:

Perform attachability checks for recovery points with numbers 5 and 7:

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

The `forcechecksum` command lets you force an integrity check of any Exchange Message Databases (MDBs) present on the specified recovery point or points. When you force a checksum check, the command begins immediately.

Usage

The usage for the command is as follows:

```
/forcechecksum -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] -time [time string]
```

Command Options

The following table describes the options available for the `forcechecksum` command:

Table 29: ForceChecksum command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine against which to perform the checksum check.
`-rpn`	The sequential number of a recovery point against which to perform checks (run command /list rps to obtain the numbers). To perform checks against multiple recovery points with a single command, you can specify several numbers separated by spaces.
`-time`	Select a recovery point by its creation time. You must specify the exact time in the format “mm/dd/yyyy hh:mm tt” (for example, “2/24/2012 09:00 AM”). Keep in mind to specify the date and time values of the time zone set on your PC.

Example:

Perform a checksum check for recovery points with numbers 5 and 7:

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

Forcing log truncation lets you perform this job one time, on-demand. It immediately truncates the logs for the specified SQL Server agent machine.

Usage

The usage for the command is as follows:

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `forcelogtruncation` command:

Table 30: ForceLogTruncation command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine against which to perform log file truncation.

Example:

Force log truncation for a protected server:

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.20.20
```

ForceMount

Use the `forcemount` command to conduct an one-time recovery point mountability check. This determines whether or not the specified recovery point or recovery points can be mounted and used to restore backed up data. You must list either one or more specific recovery points on which to conduct the check, or a time range during which the recovery points were created.

Usage

The usage for the command is as follows:

```
/forcemount -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Command Options

The following table describes the options available for the `forcemount` command:

Table 31: ForceMount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine against which to perform a mountability check.
`-rpn`	The sequential number of a recovery point against which to perform checks (run command /list rps to obtain the numbers). To perform checks against multiple recovery points with a single command, you can specify several numbers separated by spaces.
`-time`	Select a recovery point by its creation time. You must specify the exact time in the format “mm/dd/yyyy hh:mm tt” (for example, “2/24/2012 09:00 AM”). Keep in mind to specify the date and time values of the time zone set on your PC.

Example:

Perform mountability checks for recovery points with numbers 5 and 7:

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.20.20 -rpn 5 7
```

ForceOptimizationJob

The `forceoptimizationjob` command lets you perform optimize a repository on demand.

Usage

The usage for the command is as follows:

```
/forceoptimizationjob -repository [repository name] | -all -core [host name] -user
[user name] -password [password]
```

Command Options

The following table describes the options available for the `forceoptimizationjob` command:

Table 32: ForceOptimizationJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	The name of the repository that you want to optimize.
`-all`	Use this option to perform the optimization job on all repositories for this Core.

Example:

Force a repository optimization job:

```
>cmdutil /forceoptimizationjob -repository "Repository 1" -core 10.10.10.10 -user
administrator -password 23WE@#$sdd
```

ForceReplication

Use the `forcereplication` command to force a one-time transfer of replicated data from the source core to the target core. You can replicate one specific protected server or replicate all protected servers. The protected servers must be already configured for replication.

Usage

The usage for the command is as follows:

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -
targetcore [host name] -all | -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `forcereplication` command:

Table 33: ForceReplication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
`-targetcore`	Host name of the target core against which replication should be forced.
`-protectedserver`	The protected machine you want to replicate.
`-all`	Force replication for all machines being replicated to the target core.

Example:

Force replication for a protected server on a specific target core:

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

Use the `forcerollup` command to force the rollup of recovery points on a protected machine.

Usage

The usage for the command is as follows:

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `forcerollup` command:

Table 34: ForceRollup command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name,

Option	Description
	you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
-protectedserver	Optional. Protected machine against which to perform rollup.

Example:

Force rollup for agent 10.10.10.1 on the Core:

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#$sdd -protectedserver 10.10.10.1
```

ForceScheduledArchive

The `forcescheduledarchive` command lets you force an archive to occur outside of its regularly scheduled time.

Usage

The usage for the command is as follows:

```
/forcescheduledarchive -core [host name] -user [user name] -password [password] -all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `forcescheduledarchive` command:

Table 35: ForceScheduledArchive command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-all	Use this option to force all scheduled archives.
-ids	The identifier (ID) or IDs separated by spaces of the scheduled archives that you want to force.

Examples:

Force all scheduled archives:

```
>cmdutil /forcescheduledarchive -all
```

Force one scheduled archive:

```
>cmdutil /forcescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

ForceVirtualStandby

Exporting data from a protected machine to a virtual machine creates a virtual standby machine. If you have continuous virtual export set up, you can use this command to force Rapid Recovery to export data on demand, regardless of the predetermined schedule.

Usage

The usage for the command is as follows:

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login]
-protectedserver [name] | -all
```

Command Options

The following table describes the options available for the `ForceVirtualStandby` command:

Table 36: ForceVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or space-separated names of virtualized machines.
`-all`	This command specifies whether to force all scheduled virtual exports.

Examples:

Force all virtual standby exports:

```
>cmdutil /forcevirtualstandby -all
```

Force virtual standby for two machines:

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

GetOracleInstanceMetadata

The `getoracleinstancemetadata` command lets you retrieve the detailed metadata for a specified Oracle instance.

Usage

The usage for the command is as follows:

```
/getoracleinstancemetadata -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address] -instancename [Oracle instance SID]
```

Command Options

The following table describes the options available for the `getoracleinstancemetadata` command:

Table 37: GetOracleInstanceMetadata command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.
`-instancename`	The Oracle SID from which you want to fetch metadata.

Example:

Get detailed metadata for the named Oracle instance. If no metadata credentials are set, then only summary metadata displays:

```
>cmdutil /getoracleinstancemetadata -core 10.10.127.42 -user admin -password -
676df#df -protectedserver 10.10.34.88 -instancename ORCL
```

Help

The `help` command displays a list of the available commands and their definitions. It also provides copyright and version details.

Usage

The usage for the command is as follows:

```
/help
```

Example:

Request Command Line help:

```
>cmdutil /help
```

List

The `list` command returns information about all recovery points, active jobs, completed jobs, failed jobs, invalid (failed) recovery points, valid (passed) recovery points, mounts, protected servers, volumes, virtualized servers, unprotected volumes, clusters, protection groups, SQL databases, Exchange databases, replicated servers, and repositories for the specified agent or list of servers currently protected by the Core. The most recent records return by default. You can list all records or specify how many records display by using a number parameter. This parameter should contain the letter "l" for the latest recovery points and "f" for the first recovery point. Each recovery point has its own number, which the administrator can use for mounting.

Usage

The usage for the command is as follows:

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs |
completed jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters |
protectiongroups | sqldatabases | exchangemailstores | replicatedservers |
repositories] -protectedserver [name | IP address] -core [host name] -user [user
name] -password [password] –number [all | l<number> | f<number> | <number>] -jobtype
```

Command Options

The following table describes the options available for the `list` command:

Table 38: List command options

Option	Description
`-?`	Display this help message.
`-list`	Select one of the following options:

Option	Description
	• all recovery points ('rps') • valid recovery points ('passed') • invalid recovery points ('failed') • mounts ('mounts') • protected volumes ('volumes') • unprotected volumes ('unprotectedvolumes') • protected machines ('protectedservers') • active jobs ('activejobs') • failed jobs ('failedjobs') • completed jobs ('completedjobs') • virtualized servers ('virtualizedservers') • clusters ('clusters') • protection groups ('protectiongroups') • SQL Server databases ('sqldatabases') • MS Exchange databases ('exchangemailstores') • replicated servers ('replicatedservers') • repositories ('repositories')
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	For show jobs only. Display al events of a specific type (active/failed/completed) on the core server.
`-protectedserver`	Protected machine with recovery points to display.
`-number`	Optional. Number of data items to display. Use only with the following specifiers: 'rps', 'activejobs', 'completedjobs', 'failedjobs'. Available values are: • all (fetch all data items) • l[number] or [number] (fetches top ## data items) • f[number] (fetches first ## data items) Only takes effect when displaying recovery points and jobs.
`-jobtype`	Optional. Filter output by job type. Available values include: • 'transfer' (data transfer)

Option	Description
	• 'repository' (repository maintenance) • 'replication' (local and remote replications) • 'backup' (backup and restore) • 'bootcdbuilder' (create boot CDs) • 'diagnostics' (upload logs) • 'exchange' (Exchange Server files check) • 'export' (recovery point export) • 'pushinstall' (deploy agents) • 'restore' (recovery point restores) • 'rollup' (protected machine rollups) • 'sqlattach' (agent attachability checks) • 'mount' (mount repository)

Examples:

List the 30 most recent recovery points:

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -number 130
```

View all failed data transfer jobs performed by a protected machine:

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -number all -jobtype transfer
```

ListAzureVMSizes

Use the `listazurevmsizes` command to determine the size of a virtual machine (VM) that has been deployed to a Microsoft Azure cloud account.

Usage

The usage for the command is as follows:

```
/listazurevmsizes -storageaccountname [Azure storage account name] -core [host
name] -user [user name] -password [password] -protectedserver [name | IP
address] or [IP]
```

Command Options

The following table describes the options available for the `listazurevmsizes` command:

Table 39: ListAzureVMSizes command options

Option	Description
`-?`	Display this help message.
`-cloudaccountname`	Optional when specifying `-storageaccountname`. Specify the name of the Azure cloud account.
`-storageaccountname`	Optional when specifying `-cloudaccountname`. Specify the name of the Azure storage account.
`-subscriptionid`	The Azure subscription ID.
`-cloudservicename`	The name of the Azure cloud service.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.

Examples:

View a list of the available virtual machine sizes for the cloud account Account1:

```
>cmdutil /listazurevmsizes -cloudaccountname Account1 -cloudservicename Service
```

View a list of the available virtual machine sizes for the storage account named "teststorage:"

```
>cmdutil /listazurevmsizes -storageaccountname teststorage -cloudservicename Service
```

ListOracleInstances

The `listoracleinstances` command lets you retrieve a list of all Oracle instances running on a specified protected machine.

Usage

The usage for the command is as follows:

```
/listoracleinstances -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `listoraclesinstances` command:

Table 40: ListOracleInstances command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.

Example:

List the Oracle instances running on the specified protected server:

```
>cmdutil /listoracleinstances -core 10.10.127.42 -user admin -password -676df#df -
protectedserver 10.10.34.88
```

ManagementCertificates

Use the `managementcertificates` command to view a list of the Microsoft Azure management certificates.

Usage

The usage for the command is as follows:

```
/managementcertificates -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -list [list certificates] -
upload [publish setting file path] -delete [subscription IID]
```

Command Options

The following table describes the options available for the `managementcertificates` command:

Table 41: ManagementCertificates command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name,

Option	Description
	you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of a protected machine.
`-list`	Optional. List of Azure management certificates.
`-upload`	Optional. The location of the publish settings file from which you want to upload Azure management certificates.
`-delete`	Use this option to delete an Azure management certificate by using the subscription ID.

Examples:

View a list of the Azure management certificates previously added on the Core:

```
>cmdutil /managementcertificates
>cmdutil /managementcertificates -list
```

Upload Azure management certificates from a publish settings file:

```
>cmdutil /managementcertificates -upload "c:\file.publishsettings"
```

Delete an Azure management certificate using the subscription ID:

```
>cmdutil /managementcertificates -delete "111111-22222-33333-4444-555555"
```

MigrateAgent

Use the `migrateagent` command to migrate an agent from one repository to another.

Usage

The usage for the command is as follows:

```
/migrateagent -protectedserver [name | IP address] -targetrepository [repository name] -core [host name] -user [login] -password [password]
```

Command Options

The following table describes the options available for the `migrateagent` command:

Table 42: ManagementCertificates command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of a protected machine to migrate to specified DVM repository.
`-targetrepository`	Optional. List of Azure management certificates.

Examples:

Migrate protected machine to DVM repository "Repository 2":

```
>cmdutil /migrateagent -protectedserver 192.254.156.248 - targetrepository
"Repository 2" -core 10.10.10.10 -user administrator -password 23WE@#$sdd
```

Mount

The `mount` command mounts a snapshot of one or more drives. You can specify whether the mount should be read, write, or read-only with previous writes. The default selection is read-only.

Usage

The usage for the command is as follows:

```
/mount -core [host name] -user [user name] -password [password] -protectedserver
[name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives
[drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -
time [time string]
```

Command Options

The following table describes the options available for the `mount` command:

Table 43: Mount command options

Option	Description
`-?`	Display this help message.

Option	Description
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-protectedserver	Protected machine with a recovery point or points to be mounted.
-mounttype	Optional. Specifies a mount mode. Available values are 'read' (read-only), 'readOnlyWithPreviousWrites' (read-only with previous writes), 'write' (writable). The default mode is read-only.
-volumes	Optional. List of volume names to mount. If not specified, all volumes are mounted. Values must be enclosed in double quotes and separated by spaces; for example: "c:" "d:". Do not use trailing slashes in volume names.
-path	Path to a folder on the core server to which the recovery point should be mounted. If one does not exist, a folder is automatically created.
-rpn	Optional. The sequential number of a recovery point to mount (use /list rps command to get the numbers). Specify several space-separated numbers to mount multiple recovery points with a single command. In this case data from each recovery point will be stored in a separate child folder. Note: if neither option -time nor -rpn is specified then the most recent recovery point that successfully passed integrity check will be mounted.
-time	Optional. Determines recovery point or points to be selected for mount. Available values include: 'latest', 'passed', exact time in the format "mm/dd/yyyy hh:mm tt" (for instance, "2/24/2012 09:00 AM"). Keep in mind to specify date time values of the time zone set on your PC. If neither the -time option nor the -rpn option is specified, then the most recent recovery point that successfully passed an integrity check is mounted.
-localdrive	Optional. Perform mount to user disk on local PC.

Examples:

Mount the most recent recovery points containing volumes “c:\” and “d:\” in the read-only mode:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

Mount recovery points with numbers 2 and 7:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

Mount-Repository

The command mounts a selected repository.

Usage

The usage for the command is as follows:

```
Mount-Repository -core [host name] -user [login] -password [password] -name
[repository name]
```

Command Options

The following table describes the options available for the `mount-repository` command:

Table 44: Mount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Name of a repository you want to mount.

Examples:

Mount repository "Repository 2":

```
> Mount-Repository -name "Repository 2"
```

MountArchiveRepository

To restore data from an archive in Rapid Recovery, you must first mount it.

Usage

The usage for the command is as follows:

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -
name [archive repository name]
```

Command Options

The following table describes the options available for the `mountarchiverepository` command:

Table 45: MountArchiveRepository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Required. The name of the archive repository.

Examples:

Mount the repository named "NewArchive:"

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

Use the NewCloudAccount command to add an account for a cloud provider to the Rapid Recovery Core. You can then use the account to store archives for retention or replication.

Usage

The usage for the command is as follows:

```
/newcloudaccount -core [host name] -user [user name] -password [password] -
displayname [name for the account] -type [cloud account provider] -useername [user
name for the account] -key [secret key] -region [region for account] tenanatid
[tenant ID] -authurl [authorization URL]
```

Command Options

The following table describes the options available for the `NewCloudAccount` command:

Table 46: NewCloudAccount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you

Option	Description
	must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-displayname	The name you want to use for the cloud account.
-type	The type of cloud account. Supported values include: • amazon • openstack • rackspace • windowsazure • "windows azure" • azure
-username	The user name for the cloud account you want to add. This is the credential you use in the authentication process. The property has the following variations based on the cloud type: • Amazon - Access Key • OpenStack - User Name • Rackspace - User Name • Windows Azure - Storage Account Name
-key	The authentication key for the cloud account you want to add. This is the credential you use in the authentication process. The property has the following variations based on the cloud type: • Amazon - Secret Key • OpenStack - API Key • Rackspace - API Key • Windows Azure - Access Key
-region	The region of the cloud account you want to add. This option is required only for OpenStack and Rackspace acocunts.
-tenantid	The ID you use to authenticate an OpenStack cloud account. This option is required only for OpenStack accounts.
-authurl	The URL you use to authenticate an OpenStack cloud account. This option is required only for OpenStack accounts.

Examples:

Add a new cloud account with the name "Amazon S3 Account" with the access key "akey" and the secret key "skey:"

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -useername
akey -key skey
```

OpenDvmRepository

Use this command to open an existing DVM repository created in AppAssure Core or Rapid Recovery Core.

Usage

The usage for the command is as follows:

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -
shareusername [user name for network share] -sharepassword [network share password]
```

Command Options

The following table describes the options available for the `OpenDvmRepository` command:

Table 47: OpenDvmRepository command options

Option	Description
`-?`	Display this help message.
`-localpath`	The path to the folder with a DVM repository on the local Core.
`-sharepath`	The path to the folder with the DVM repository on a CIFS share.
`-shareusername`	The user name you use to log in to the shared folder.
`-sharepassword`	The password you use to log in to the shared folder.

Example:

Open an existing DVM repository on the local machine:

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pause

An administrator can pause snapshots, export to virtual machines, or replicate a Core. The `pause` command accepts three parameters: `snapshot`, `vmexport`, and `replication`. Only one parameter can be specified. A snapshot can be paused until a certain time, if a time parameter is specified.

A user can pause replication in three ways:

- On a source Core for all protected machines.(`-[outgoing]`).
  The administrator must specify the remote machine name with the outgoing replication pairing to pause outgoing replication on the source Core:

  ```
  >cmdutil /pause replication /o 10.10.12.10
  ```

- On the source Core for a single protected machine.(`-protectedserver`):

  ```
  >cmdutil /pause replication /protectedserver 10.10.12.97
  ```

- On target Core (`-incoming`).
  If the local Core is a target Core, the administrator can pause replication by specifying the source Core using the incoming parameter:

  ```
  >cmdutil /pause replication /i 10.10.12.25
  ```

Usage

The usage for the command is as follows:

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

Command Options

The following table describes the options available for the `pause` command:

Table 48: Pause command options

Option	Description
`-?`	Display this help message.
`-pause`	[`snapshots`], [`replication`] or [`vmexport`]. Optional.
`-core`	Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.

Option	Description
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-all	Optional. Pause all agents on the selected Core.
-protectedserver	Optional. Pause current protected server.
-incoming	Optional. Host name of the remote core that replicates to the core machine.
-outgoing	Optional. Host name of the remote target core to which data is replicated.
-time	Optional. The time in the format 'Day-Hours-Minutes' when the snapshots will be resumed (only for snapshots pause).

Examples:

Pause creating snapshots for a specific protected server:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.10.4
```

Pause creating snapshots for a protected machine and resume it after three days, 20 hours, and 50 minutes:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd
-protectedserver 10.10.10.4 -time 3-20-50
```

Pause export to virtual machine for all protected machines on the core:

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password
23WE@#$sdd -all
```

Pause outgoing replication on the core for a specific protected machine:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.1.76
```

Pause outgoing replication for all protected machines on the target core:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password -
23WE@#$sdd -outgoing 10.10.1.63
```

Pause incoming replication for all machines on the target core:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -incoming 10.10.1.82
```

Protect

The `protect` command adds a server under protection by a core.

Usage

The usage for the command is as follows:

```
/protect -core [host name] -user [user name] -password [password] -repository [name]
-agentname [name | IP address] -agentusername [user name] -agentpassword [password]
-agentport [port] -volumes [volume names]
```

Command Options

The following table describes the options available for the `protect` command:

Table 49: Protect command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on

Option	Description
	user are used.
-repository	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
-agentname	Name or IP address of the server you want to protect.
-agentusername	User name for the server to be protected.
-agentpassword	Password for the server to be protected.
-agentport	Protected server port number.
-volumes	List of volumes to protect. Values must be enclosed in double quotes and separated by a space. Do not use trailing slashes in volume names; for example: “c:” “d:”.

Example:

Protect specific volumes of a server with the Core:

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#$sdd -repository “Repository 1” -agentname 10.10.9.120 -agentport 5002 -agentusername administrator agentpassword 12345 -volumes “c:” “d:”
```

ProtectCluster

The `protectcluster` command adds a cluster under protection by a core.

Usage

The usage for the command is as follows:

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

Command Options

The following table describes the options available for the `protectcluster` command:

Table 50: ProtectCluster command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name,

Option	Description
	you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-repository	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
-clustername	Name or IP address of the cluster you want to protect.
-clusterusername	User name for the cluster to be protected.
-clusterpassword	Password for the cluster to be protected.
-clusterport	Protected cluster server port number.
-clustervolumes	List of volumes to protect. Values must be enclosed in double quotes and separated by a space. Do not use trailing slashes in volume names; for example: “c:” “d:”.
-clusternodes	List of the cluster nodes and the volumes you want to protect on each node.

Example:

Protect specific volumes of a cluster server with the Core:

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password
23WE@#$sdd -repository “Repository 1” -clustername 10.10.8.150 -clusterport 8006 -
clusterusername clusterAdmin clusterpassword password -volumes
“C:\ClusterStorage\Volume1” -clusternodes nodeName 10.10.8.150 volumes “c:” nodeName
10.10.8.151 volumes “c:”
```

ProtectEsxServer

You can use the `protectesxserver` command whenever you want to add a VMware ESX(i) virtual machine to protection.

Usage

The usage for the command is as follows:

```
/protectesxserver -core [host name] -user [user name] -password [password] -
repository [repository name] -server [name | IP address] -serverusername [user name]
-serverpassword [password for server login] -serverport [port] -virtualMachines
[virtual machines collection | all] -autoProtect [object ID or name collection]
```

Command Options

The following table describes the options available for the `protectesxserver` command:

Table 51: ProtectEsxServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
`-server`	The name or IP address for the vCenter or ESXi server you want to protect.
`-serverusername`	The user name for logging in to the vCenter or ESXi server that you want to protect.
`-serverpassword`	The password for logging in to the vCenter or ESXi server that you want to protect.
`-serverport`	Optional. The port number for the vCenter or ESXi server that you want to protect.
`-virtualmachines`	Optional. This option lets you list the virtual machines that you want to protect.
`-autoprotect`	Optional. This option lets you list new virtual machines that you want to automatically protect.

Example:

Protect specific virtual machines from a vCenter or ESXi server with the Core:

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -
repository "Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -
serverpassword password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

ProtectHyperVCluster

The `protecthypervcluster` command adds a Hyper-V cluster under protection by a Core using agentless protection.

Usage

The usage for the command is as follows:

```
/protecthypervcluster -core [host name] -user [user name] -password [password] -
repository [name] -server [name | IP address] -serverusername [user name] -
serverpassword [password] -serverport [port] -virtualmachines [virtual machines
collection | all] -isagentprotection
```

Command Options

The following table describes the options available for the `protecthypervcluster` command:

Table 52: ProtectHyperVCluster command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
`-server`	Name or IP address of the Hyper-V server that you want to protect.
`-serverusername`	User name for the Hyper-V server to be protected.
`-serverpassword`	Password for the Hyper-V server to be protected.
`-serverport`	Optional. Protected Hyper-V server port number.
`-virtualmachines`	Optional. List of virtual machines to protect. Values must be enclosed in double quotes and separated by a space. If you exclude this parameter, only the Hyper-V cluster container is protected.
`-isagentprotection`	Optional. Use this option to protect a cluster with an Agent in each guest virtual machine, which is false by default.
`-autoprotect`	Optional. This option enables the autoprotect feature for the Hyper-V server. It is not compatible with the `-isagentprotection` option.

Example:

Protect specific virtual machines of a Hyper-V cluster:

```
>cmdutil /protecthypervcluster -core 10.10.10.10 -username admin -password password
-repository “Repository 1” -server 10.10.8.150 -serverport 443 -serverusername root
clusterpassword password -virtualmachines “VM1” "VM2" -autoprotect
```

ProtectHyperVServer

The `protecthypervserver` command adds a Hyper-V server under protection by a Core using agentless protection.

Usage

The usage for the command is as follows:

```
/protecthypervserver -core [host name] -user [user name] -password [password] -
repository [name] -server [name | IP address] -serverusername [user name] -
serverpassword [password] -serverport [port] -virtualmachines [virtual machines
collection | all] -isagentprotection
```

Command Options

The following table describes the options available for the `protecthypervserver` command:

Table 53: ProtectHyperVServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
`-server`	Name or IP address of the Hyper-V server that you want to protect.
`-serverusername`	User name for the Hyper-V server to be protected.
`-serverpassword`	Password for the Hyper-V server to be protected.
`-serverport`	Optional. Protected Hyper-V server port number.
`-virtualmachines`	Optional. List of virtual machines to protect. Values must be enclosed in double quotes and separated by a space. If you exclude this parameter, only the Hyper-V cluster container is protected.

Example:

Protect specific virtual machines of a Hyper-V server:

```
>cmdutil /protecthypervserver -core 10.10.10.10 -username admin -password password -
repository “Repository 1” -server 10.10.8.150 -serverport 443 -serverusername root
clusterpassword password -virtualmachines “VM1” "VM2"
```

RemoveAgent

The `RemoveAgent` command lets you remove a protected machine from the protection of a Core and optionally delete the recovery points of the removed machine. If you do not delete the recovery points, Rapid Recovery retains and labels them as a recovery points only machine.

Usage

The usage for the command is as follows:

```
/removeagent -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -deleterecoverypoints
```

Command Options

The following table describes the options available for the `RemoveAgent` command:

Table 54: RemoveAgent command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the server you want to remove from protection.
`-deleterecoverypoints`	Optional. Deletes all recovery points for the machine you want to remove.

Example:

Remove a machine from protection and delete the associated recovery points:

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

You can use the `removearchiverepository` command to delete a repository from the Rapid Recovery Core.

Usage

The usage for the command is as follows:

```
/removearchiverepository -core [host name] -user [user name] -password [password]
name] -name [archive repository name]
```

Command Options

The following table describes the options available for the `removearchiverepository` command:

Table 55: RemoveArchiveRepository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-name`	Required. The name of the archive repository.

Examples:

Remove the repository named "NewArchive" from the local Core:

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints

The `removepoints` command lets you delete specific recovery points of a protected machine.

Usage

The usage for the command is as follows:

```
/removepoints -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Command Options

The following table describes the options available for the `removepoints` command:

Table 56: RemovePoints command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the server for which you want to delete recovery points
`-rpn`	Optional. The sequential number of a recovery point to be deleted (use `/list rps` command to get the numbers). Specify several space-separated numbers to delete multiple recovery points with a single command.
`-time`	Optional. Determines which recovery point or points to delete by creation time. Specify the exact time in the format "mm/dd/yyyy hh:mm tt" (for example, "2/24/2012 09:00 AM"). Keep in mind to specify the date time values of the time zone set on your PC.

Example:

Delete the recovery points with number 5 and 7:

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

Use this command to discontinue an existing Rapid Recoveryscheduled continuous archive.

Usage

The usage for the command is as follows:

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `removescheduledarchive` command:

Table 57: RemoveScheduledArchive command options

Option	Description
`-?`	Display this help message.

Option	Description
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-all	This option specifies whether to remove all scheduled archives associated with this Core.
-ids	Use this option to list the ID or IDs for each scheduled archive you want to remove. Separate multiples IDs with spaces.

Examples:

Remove all scheduled archives:

```
>cmdutil /removescheduledarchive -all
```

Remove one scheduled archive:

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

Use this command to discontinue the continuous export of data to a virtual machine in the Rapid Recovery command utility.

Usage

The usage for the command is as follows:

```
/removevirtualstandby -core [host name] -user [user name] -password [password login]
-protectedserver [name] | -all
```

Command Options

The following table describes the options available for the `removevirtualstandby` command:

Table 58: RemoveVirtualStandby command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.

Option	Description
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or space-separated names of virtualized machines.
`-all`	This command specifies whether to remove all scheduled virtual exports.

Examples:

Remove all virtual standby exports:

```
>cmdutil /removevirtualstandby -all
```

Remove virtual standby export for two machines:

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Replicate

Use the `Replicate` command to set up replication between two Rapid Recovery Cores.

Usage

The usage for the command is as follows:

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port | hostname user name password | hostname port user name password] -replicationname [name] -seeddrive [localpath | network path username password] [comment] -protectedserver [name | name repository]
```

Command Options

The following table describes the options available for the `Replicate` command:

Table 59: Replicate command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.

Option	Description
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
`-request`	Optional. Specify this option if you want to use a subscription to a third-party provider of off-site backup and disaster recovery services.
`-targetserver`	The name of the server where you want to establish replication. It includes the following parameters: • port • user name • password The port parameter is optional, with a default of 8006. If you used the `request` option, you should also use the user name and password for the target server.
`-replicationname`	Optional. Use the name of the replication job if you do not use the `request` option.
`-seeddrive`	Optional. Use this option to specify a seed drive for the initial data transfer. The comment parameter is optional.
`-protectedserver`	The list of protected machines you want to replicate. If you use the `request` option, list only the names or IP addresses of protected machines. Otherwise, list both protected machines and the corresponding remote repository name.

Example:

Replicate two protected machines to the remote Core using a seed drive from a network share:

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname
ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -
protectedserver 10.10.1.1 Repository1 10.10.1.2 Repository2
```

Replication

Use the `replication` command to control existing replication between two Rapid Recovery Cores and manage pending replication requests.

NOTE: This command succeeds the `Replicate` command, which establishes the connection—called pairing—between the Cores and uses a seed drive for the initial data transfer. For more information about this command, see Replicate.

Usage

The usage for the command is as follows:

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -
delete | -edit] -id [replication ID] -protectedserver [name | name repository] -
responsecomment [comment] -deleterecoverypoints -scheduletype [type] -dailystarttime
[time] -dailyendtime [time] -weekdaystarttime [time] -weekdayendtime [time] -
weekendstarttime [time] -weekendendtime [time]
```

Command Options

The following table describes the options available for the `replication` command:

Table 60: Replication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
`-list`	The list of incoming or outgoing replication jobs or pending replication requests.
`-accept`	Accepts the replication request.
`-deny`	Denies the replication request.
`-ignore`	Ignores the replication request.
`-delete`	Use this option to delete an existing replication job or a machine from the replication job. Specify only the `-id` parameter to delete an entire replication relationship, or specify both the `-id` and `-protectedserver` parameters to delete only specific machines from replication.
`-edit`	Edits the schedule of existing replication jobs.
`-id`	The identifier for the replication job or pending replication request. It can be a remote Core ID, host name, customer ID, email address, or pending replication request ID.
`-protectedserver`	When responding to a replication request, use this option to apply your response to list of protected servers with a repository name or ID. Use the parameter "all" to apply response to all requested machines.
`-responsecomment`	The comment you provide with the response to a pending replication request.
`-deleterecoverypoints`	Use this option if specific recovery points from a deleted replicated machine should also be removed.
`-scheduletype`	If you use the `-edit` option, this option specifies the type of replication schedule. Include one of the following four values: • atalltimes - Automatically replicate at any time. • daily - Replicate daily. Specify the `-dailystarttime` and `-dailyendtime` parameters. • custom - When using daily replication, use this value to schedule replication on weekdays or weekends. Specify the `-weekdaystarttime`, `-weekdayendtime`, `-weekendstarttime`, and `-weekendendtime` parameters.
`-dailystarttime`	Use only for the daily value of the `-scheduletype` option. It is used to

Option	Description
	establish a window of time for when replication should occur. Use this option to specify the earliest time of day when you want replication to start. Confirm with Dev.
-dailyendtime	Use only for the daily value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of day when you want replication to start. Confirm with Dev.
-weekdaystarttime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the earliest time of a weekday when you want replication to start. Confirm with Dev.
-weekdayendtime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of a weekday when you want replication to start. Confirm with Dev.
-weekendstarttime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the earliest time of the weekend when you want replication to start. Confirm with Dev.
-weekendendtime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of the weekend when you want replication to start. Confirm with Dev.

Examples:

List all incoming replication:

```
>cmdutil /replication -list incoming
```

Accept pending replication requests for two protected machines:

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1
Repository1 10.10.1.2 Repository2 -responsecomment A response comment
```

Deny a pending replication request:

```
>cmdutil /replication -deny -id customer@email.address
```

Delete existing replication with replicated recovery points:

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

Remove two machines from existing replication:

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -
protectedserver 10.10.1.1 10.10.1.2
```

Edit schedule of replication with specified weekday and weekend times:

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -
weekdaystarttime "9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -
weekendendtime "6:00 PM"
```

ResizeDedupeCache

Use the `resizededupecache` command to change the size of the deduplication cache location for the Azure repository.

Usage

The usage for the command when resizing the deduplication cache location for an Azure repository is as follows:

```
/resizededupecache -core [host name] -user [login] -password [password] -repository
[repository id] -dedupecachesize [cache size]
```

Command Options

The following table describes the options available for the `resizededupecache` command:

Table 61: ResizeDedupeCache command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	ID of the Azure repository.
`-dedupecachesize`	Optional. Amount of memory to be allocated for deduplication cache. Available units are B, KB, MB, and GB. The default value is 1.5 GB.

Examples:

Resize the deduplication cache for an Azure repository:

```
>cmdutil /resizededupecache -repository AzureStorageID -dedupecachesize 200 Gb -core
10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

RestartCoreService

If the Core service on the Core machine is stopped, use the `restartcoreservice` command to start it again.

Usage

The usage for the command is as follows:

```
/restartcoreservice -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false] -wait [time in seconds]
```

Command Options

The following table describes the options available for the `restartcoreservice` command:

Table 62: RestartCoreService command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."
`-wait`	Optional. This option indicates that the command should wait until the Core service is fully restarted for the specified period of time in seconds before canceling active jobs.

Example:

Restart the Core service:

```
>cmdutil /restartcoreservice -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true -wait 600
```

RestoreAgent

The `restoreagent` command lets you restore a protected machine or volume from a specific Rapid Recovery recovery point.

Usage

The usage for the command is as follows:

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -
volumes [IDs | names | all] -targetmachine [name] -targetvolume [volume name] -
forcedismount -autorestart
```

Command Options

The following table describes the options available for the `restoreagent` command:

Table 63: RestoreAgent command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the server you want to restore.
`-rpn`	The identification number of the recovery point you want to use to restore the machine. To find the correct number, use the command `/list rps`.
`-volumes`	The IDs or names of the volumes you want to restore. To restore all protected volumes, use `-volumes all`.
`-targetmacchine`	The name of the machine to which you want to restore the protected machine.
`-targetvolume`	The name or ID of the volume to which you want to restore the machine.
`-forcedismount`	Optional. Use this option to force the dismount of the database on demand.
`-autorestart`	Optional. Use this command if restarting an Exchange Server machine is necessary.

Example:

Restore a machine to a protected machine with the IP address 192.168.20.130, including the force database dismount option:

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:"
"C:" -targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive

This command restores an archive from a local archive or share and places the restored data in a specified repository.

Usage

The usage for the command is as follows:

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address] -repository [name] -archiveusername [name] -
archivepassword [password] -path [location]
```

Command Options

The following table describes the options available for the `restorearchive` command:

Table 64: RestoreArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Restore data for all protected machines from the archive files.
`-protectedserver`	Protected machine with recovery points to restore. You can specify several machine names enclosed in double quotes and separated by spaces.
`-repository`	Name of a repository on the Core to which the restored recovery points should be placed. The name must be enclosed in double quotes.
`-archiveusername`	Optional. User name for the remote machine. Required for network path only.
`-archivepassword`	Optional. Password to the remote machine. Required for network path only.
`-path`	Location of the archived data to be restored; for example: d:\work\archive or network path \\servename\sharename.

Examples:

Restore archived data for all protected servers:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password
23WE@#$sdd -all -repository repository1 -path d:\work\archive
```

Restore archived data for specific protected servers:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password
23WE@#$sdd -protectedserver “10.10.20.30” “20.10.10.5” -repository repository1 -path
d:\work\archive
```

RestoreUrc

The `restoreurc` command lets you restore a protected machine or volume from a specific Rapid Recovery recovery point to a bare-metal machine using the Universal Recovery Console (URC).

Usage

The usage for the command is as follows:

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk number | all]
```

Command Options

The following table describes the options available for the `restoreurc` command:

Table 65: RestoreUrc command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the server you want to which you want to restore the URC.
`-rpn`	The identification number of the recovery point you want to use to restore the machine. To find the correct number, use the command `/list rps`.
`-volumes`	The IDs or names of the volumes you want to restore. To restore all protected volumes, use `-volumes all`.
`-targetmacchine`	The name of the machine to which you want to restore the protected machine.
`-urcpassword`	The authentication key from the URC.
`-targetdisk`	The numbers of the disks on which you want to restore the machine. To select all disks from the machine using the URC, use `-targetdisk all`.

Example:

Restore a machine to disks 0 and 1 of the machine using the URC, when the IP address for the URC machine is 192.168.20.175:

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine 192.168.20.175 -urcpassword ******** -targetdisk 0 1
```

Resume

The administrator can use this command to resume snapshots, export to a virtual machine, and replicate. You must specify your need to resume by a parameter. The following parameters are valid: `snapshot`, `vmexport`, and

`replication`. See Pause for more details.

Usage

The usage for the command is as follows:

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host name] -time [time string]
```

Command Options

The following table describes the options available for the `resume` command:

Table 66: Resume command options

Option	Description
`-?`	Display this help message.
`-restore`	[`snapshots`], [`replication`] or [`vmexport`].
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Resume all agents on the selected Core.
`-protectedserver`	Resume current protected server.
`-incoming`	Host name of the remote core that replicates to the core machine.
`-outgoing`	Host name of the remote target core to which data is replicated.

Examples:

Resume snapshots for specific protected server:

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.10.4
```

Resume export to a virtual machine for all protected machines on the core:

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

Resume outgoing replication on the core for a specific protected machine:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.1.76
```

Resume outgoing replication for all protected machines on the target core:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -outgoing 10.10.1.63
```

Resume incoming replication for all machines on the target core:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password
23WE@#$sdd -incoming 10.10.1.82
```

ResumeScheduler

This command lets you resume the task scheduler it has been paused.

Usage

The usage for the command is as follows:

```
/resumescheduler -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `resumescheduler` command:

Table 67: ResumeScheduler command options

Option	Description
`-?`	Display this help message.
`-restore`	[`snapshots`], [`replication`] or [`vmexport`].
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.

Example:

Resume snapshots for specific protected server:

```
>cmdutil /resumescheduler -core 10.10.127.42 -user admin -password 676df#df
```

SeedDrive

You can use a seed drive for the initial data transfer when you establish Rapid Recovery replication.

Usage

The usage for the command is as follows:

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore [name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

Command Options

The following table describes the options available for the `seeddrive` command:

Table 68: SeedDrive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-list`	The list of outstanding seed drives with extended information.
`-startcopy`	Start copying data to the seed drive.
`-startconsume`	Start consuming the seed drive.
`-abandon`	Abandon the outstanding seed drive request.
`-path`	The local or network path of the seed drive.
`-seeddriveusername`	Optional. The user name for the network location of the seed drive.
`-seeddrivepassword`	Optional. The password for the network location of the seed drive.
`-targetcore`	Optional. Use only with the `-copy` option. It is the name or IP address of the remote Core. All protected machines replicating to this Core receive seed drive recovery points.
`-remotecore`	Use only with the `-consume` option. It is the name of the remote Core from which the seed drive recovery points are created or consumed.
`-protectedserver`	The name or IP address of the protected machine you are using to create or consume the seed drive of recovery points. For example: -protectedserver "10.10.60.48" "10.10.12.101."

Option	Description
`-all`	This option specifies whether to consume or copy all of the available protected machines.
`-usecompatibleformat`	The new archiving format offers improved performance, however it is not compatible with older Cores. Use this option when working with a legacy AppAssure Core. Confirm with dev.

Examples:

List outstanding seed drives:

```
>cmdutil /seeddrive -list
```

Copy two protected machines to the seed drive on the network share:

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path
\\10.10.1.1\Share\Seed\ -seeddriveusername Administrator -seeddrivepassword 12345 -
usecompatibleformat
```

Starting consuming the seed drive:

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername
Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

Abandon an outstanding seed drive request:

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

SetAgentMetadataCredentials

The `setagentmetadatacredentials` command sets the metadata credentials for a specified protected machine.

Usage

The usage for the command is as follows:

```
/setagentmetadatacredentials -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -target [default | SQL | Exchange] -
metadatausername [user name] -metadatapassword [password] -sqlinstancename [SQL
instance name] -usewindowsauthentication
```

Command Options

The following table describes the options available for the `setagentmetadatacredentials` command:

Table 69: SetAgentMetadataCredentials command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.
`-target`	Optional. The type of metadata, such as SQL, Exchange, or default.
`-metadatausername`	Optional. The metadata-related login.
`-metadatapassword`	Optional. The metadata-related password.
`-sqlinstancename`	Optional. The specific SQL instance name. Use this option in conjunction with the `-target` "sql."
`-usewindowsauthentication`	Optional. Use this option if your SQL credentials are also used for Windows authentication.

Example:

Set credentials for Exchange metadata:

```
>cmdutil /setagentmetadatacredentials -core 10.10.10.10 -user administrator -
password -23WE@#$sdd -protectedserver 10.10.20.20 -target exchange -metadatausername
administrator -metadatapassword 123#
```

SetOracleMetadataCredentials

The `setoraclemetadatacredentials` command lets you set the metadata credentials for a specified Oracle instance.

Usage

The usage for the command is as follows:

```
/setoraclemetadatacredentials -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -instancename [Oracle instance
SID] -connectiontype [-basic | TNS] -hostname [host name | IP address] -port
[port number] [-usesid] -instanceservicename [service name] -tnsnetworkalias [TNS
alias] [-usewindowsauthentication] -oracleusername [user name] -oraclepassword
[password] [-edit]
```

Command Options

The following table describes the options available for the `setoraclemetadatacredentials` command:

Table 70: SetOracleMetadataCredentials command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.
`-instancename`	The Oracle SID from which you want to fetch metadata.
`-connectiontype`	Use this option to identify the connection type. It must be represented by either `basic` or `TNS`.
`-hostname`	Optional. The name of the Oracle host. Use it for the `basic` connection type.
`-port`	Optional. A port number. Use it for the `basic` connection type.
`-usesid`	Optional. This option uses the `-instancename` to identify the Oracle instance. Use it for the `basic` connection type.
`-instanceservicename`	Optional. The Oracle instance service name. Use it when the `-usesid` is not specified and for the `basic` connection type.
`-tnsnetworkalias`	Optional. Use this option to identify the TNS network alias when using the `TNS` connection type.
`-usewindowsauthentication`	Optional. This option lets you authenticate with your Windows credentials.
`-oracleusername`	Optional. The user name for the Oracle instance.
`-oraclepassword`	Optional. The password for the Oracle instance.
`-edit`	Optional. This option lets you omit any number of options.

Examples:

Set the metadata credentials for the ORCL instance on a protected server using the `basic` connection type:

```
>cmdutil /setoraclemetadatacredentials -core 10.10.127.42 -user admin -password
-676df#df -protectedserver 10.10.34.88 -instancename ORCL -connectiontype basic
-hostname localhost -port 1521 -usesid -oracleusername User-ORA -oraclepassword
676df#df
```

Set the metadata credentials for the ORCL instance on a protected server using the `TNS` connection type and Windows authentication:

```
>cmdutil /setoraclemetadatacredentials -core 10.10.127.42 -user admin -password -
676df#df -protectedserver 10.10.34.88 -instancename ORCL -connectiontype TNS -
tnsnetworkalias ORCL_ALIAS -usewindowsauthentication
```

StartExport

The `startexport` command forces a one-time export of data from a protected machine to a virtual server. You can export to an ESXi, VMware Workstation, Hyper-V, or VirtualBox virtual machine. If exporting to ESXi, you must specify thick or thin disk provisioning.

Usage

The usage for the command is as follows:

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user
name] -password [password] -protectedserver [name | IP address] -volumes [volume
names] -rpn [recovery point number | numbers] | -time [time string] -vmname [virtual
machine name] -hostname [virtual host name] -hostport [virtual hostport number] -
hostusername [virtual host user name] -hostpassword [virtual host password] [-ram
[total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping
[automatic | manual | withvm] -targetpath [location] -pathusername [user name] -
pathpassword [password] [-uselocalmachine]
```

Command Options

The following table describes the options available for the `startexport` command:

Table 71: StartExport command options

Option	Description
`-?`	Display this help message.
`-exporttype`	Perform export of data from protected server to an ESXi server ('esxi'), VMware Workstation server ('vm'), Hyper-V server ('hyperv'), or VirtualBox server ('vb').
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points to be exported.
`-volumes`	Optional. List of volume names to be exported. If not specified, all volumes will be

Option	Description
	exported. Values must be enclosed in double quotes and separated with spaces; for example: “c:” “d:”. Do not use trailing slashes in volume names.
`-rpn`	Optional. The sequential number of a recovery point to be exported (use Get-RecoveryPoints command to get the numbers). If neither the ‘time’ nor the ‘rpn’ option is specified, then the most recent recovery point is exported.
`-time`	Optional. Determines the recovery point or points to be selected for export. You need to specify the exact time in the format "mm/dd/yyyy hh:mm tt" (for example, "2/24/2012 09:00 AM"). Be sure to specify the date time values of the time zone set on your PC. Note: if neither the 'time' nor the 'rpn' option is specified, then the most recent recovery point is exported.
`-vmname`	The Windows name of the virtual machine.
`-hostname`	For ESXi and Hyper-V virtual exports only. The virtual server host name.
`-linuxhostname`	For VirtualBox exports only. The virtual server host name.
`-hostport`	For ESXi and Hyper-V virtual exports only. The virtual server port number.
`-hostusername`	For ESXi and Hyper-V virtual exports only. The user name for the virtual server host.
`-hostpassword`	For ESXi and Hyper-V virtual exports only. The password for the virtual server host.
`-ram`	Use this option to allocate a specific amount of RAM on the virtual server.
`-usesourceram`	Optional. Use this option to allocate the same amount of RAM on the virtual server that the source machine contains.
`-diskprovisioning`	Use this option for ESXi exports only. Optional. The amount of disk space that you want to allocate on the virtual machine. Use one of the two following specifications: • Thick - This specification makes the virtual disk as large as the original drive on the protected machine. • Thin - This specification allocates the amount of actual disk space occupied on the original drive with a few additional megabytes. The default specification is "thin."
`-diskmapping`	Use this option for ESXi exports only. Optional. This option determines how to map the disks from the protected machine to the virtual machine. Use one of the following values: • auto - This value automatically maps the disks. • manual - This value lets you map the disks manually. • withvm - This value stores the virtual disks in a datastore that you select. The default value is "auto."
`-targetpath`	For VMware Workstation and VirtualBox exports only. This option specifies the local or network path—or Linux path, for VirtualBox only—to the folder where you want to store the virtual machine files
`-pathusername`	For VMware Workstation exports only. It is the user name for the network machine. It is only required when you specify a network path in the `-targetpath` option.
`-pathpassword`	For VMware Workstation exports only. It is the password for the network machine. It is only required when you specify a network path in the `-targetpath` option.

Option	Description
-uselocalmachine	For Hyper-V exports only. Optional. Use this command to connect to the local Hyper-V server. This option ignores the -hostname, -hostport, -hostusername, and -hostpassword options.

Examples:

Export data to an ESXi virtual machine with a specific name and the same amount of RAM and disk size as the source protected server:

```
>cmdutil         /startexport -exporttype esxi -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname
10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram
-diskprovisioning thick
```

Create a VMware Workstation machine file on the local drive with protected data from recovery point #4:

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -
targetpath c:\virtualmachines -ram 4096
```

Create a Hyper-V machine files to be stored on a remote machine:

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-
Bobby\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -
hostpassword 12QWsdxc@# -ram 4096
```

StartExportAzure

You can use the startexportazure command to force the export of data from a protected machine to a Microsoft Azure virtual server.

Usage

The usage for the command is as follows:

```
/startexportazure -core [host name] -user [user name for Core] -password
[password for Core] -protectedserver [name | IP address] -volumes [volume
names | all] -rpn [number | numbers] -time [time string] -cloudaccountname
[Azure account name] -storageaccountname[ storage account name] -containername
[container name] -foldername [folder name] -deploymentname [deployment name] -
destinationcontainer [Azure destination container] -subscriptionid [Azure
subscription ID] -cloudservicename [cloud service name] -vmname [virtual
machine name] -vmsize [virtual machine size] -endpointname [rdp | ssh] -
protocol [tcp | udp] -publicremoteaccessport [public remote access port number]
-privateremoteaccessport [private port number]
```

Command Options

The following table describes the options available for the `startexportzure` command:

Table 72: StartExportAzure command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points that you want to export.
`-volumes`	Optional. List of additional volume names for the deploy. If you use the value `all` or use no value, the all volumes deploy.
`-rpn`	Optional. The sequential number of a recovery point that you want to export (use the `/list` rps command to get the numbers). If neither `-time` nor `-rpn` is specified, then the most recent recovery point is exported.
`-time`	Optional. This option determines the recovery points to select for export. Specify the exact time in the format `mm/dd/yyyy hh:mm tt`; for example, `2/24/2012 09:00 AM`. Keep in mind to specify the date time value of the time zone set on your PC. If neither `-time` nor `-rpn` is specified, then the most recent recovery point is exported.
`-cloudaccountname`	Optional, if the `-storageaccountname` is specified. Specify the Azure cloud account name.
`-storageaccountname`	Optional, if the `-cloudaccountname` is specified. Specify the Azure storage account name.
`-containername`	The name of the Azure container.
`-foldername`	Optional. The name of the Azure folder.
`-deploymentname`	Use this option to specify the name of the deployment. It is required for a deploy after export only.
`-destinationcontainer`	The name of the Azure destination container you want to use for the deploy.
`-subscriptionid`	The Azure subscription ID. It is required for a deploy after export only.
`-cloudservicename`	The name of the Azure cloud service. It is required for a deploy after export only.
`-vmname`	The name of the virtual machine. It is required for a deploy after export only.
`-vmsize`	The size of the virtual machine; for example, `A0`, `Basic_A4`, or `Standard_G1`.
`-endpointname`	The Azure endpoint protocol used only for remote access `rdp` or `ssh`. The

Option	Description
	default value is `rdp`. It is required for a deploy after export only.
`-protocol`	The protocol used only for remote access `tcp` or `udp`. It is required for a deploy after export only. The default value is `tcp`.
`-publicremoteaccessport`	The public port for using remote access. The default value is `3389`.
`-privateremoteaccessport`	The private port for using remote access. The default value is `3389`.
`-privateagentport`	Optional. The Agent port. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter `-publicagentport` nor `-privateagentport` is specified, then no endpoint is added.
`-publicagentport`	Optional. The external Agent port. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter `-publicagentport` nor `-privateagentport` is specified, then no endpoint is added.
`-privatetransferport`	Optional. The TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter `-publictransferport` nor `-privatetransferport` is specified, then no endpoint is added.
`-publictransferport`	Optional. The external TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter `-publictransferport` nor `-privatetransferport` is specified, then no endpoint is added.

Examples:

Export data to Azure:

```
>cmdutil /startexportazure -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -cloudaccountname "Cloud Account 1" -
containername "mycontainer" -foldername "folder" -deploymentname Deploy1 -
destinationcontainer container1 -subscriptionid "111111-22222-33333-4444-555555" -
cloudservicename Service1 -vmname VirtualMachine -vmsize A0
```

Export data to Azure using a specified endpoint:

```
>cmdutil /startexportazure -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -cloudaccountname "Cloud Account 1" -
containername "mycontainer" -foldername "folder" -deploymentname Deploy1 -
destinationcontainer container1 -subscriptionid "111111-22222-33333-4444-555555" -
cloudservicename Service1 -vmname VirtualMachine -vmsize A0 -endpointname ssh -
protocol udp -publicremoteaccessport 1555 -privateremoteaccessport 22
```

Export data to Azure with a specified Agent endpoint when the `-privateagentport` option uses the special value 0, which is taken from the Agent configuration. The `-publicagentport` option has the user-defined value of `1888`:

```
>cmdutil /startexportazure -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -cloudaccountname "Cloud Account 1" -
```

```
containername "mycontainer" -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 0 -publicagentport 1888
```

Export data to Azure with specified Agent and transfer endpoints. The `-privateagentport` option has the user-defined value of `8006`. The parameter for `-publicagentport` uses the special value of `0`, which is copied from the `-privateagentport` option. The parameter for `-privatetransferport` uses the special value of `0`, which is taken from the Agent configuration. The parameter for `-publictransferport` uses the special value `0`, which is copied from the `-privatetransferport` option.:

```
>cmdutil /startexportazure -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -cloudaccountname "Cloud Account 1" -
containername "mycontainer" -foldername "folder" -deploymentname Deploy1 -
destinationcontainer container1 -subscriptionid "111111-22222-33333-4444-555555" -
cloudservicename Service1 -vmname VirtualMachine -vmsize A0 -privateagentport 8006 -
publicagentport 0 -privatetransferport 0 -publictransferport 0
```

StartOracleDBVerifyJob

Use the command `startoracledbverifyjob` to start the DBVerify job for one or more specified recovery points on a protected server.

Usage

The usage for the command is as follows:

```
/startoracledbverifyjob -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -recoverypointnumber [number | numbers]
```

Command Options

The following table describes the options available for the `startoracledbverifyjob` command:

Table 73: StartOracleDBVerifyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle DBVerify nightly job.

Option	Description
-recoverypointnumber	The sequential number of a recovery point that you want to export (use the /list rps command to get the numbers). To start the job on multiple recovery points with one command, separate each recovery point number with a space.

Example:

Start the Oracle DBVerify job for the recovery points on the specified protected server:

```
>cmdutil /startoracledbverifyjob -core 10.10.127.42 -user admin -password 676df#df -protectedserver 10.10.34.88 -recoverypointnumber 1 2
```

StartOracleLogTruncationJob

The command startoraclelogtruncationjob lets you start a log truncation job for a specified Oracle instance on a protected server.

Usage

The usage for the command is as follows:

```
/startaclelogtruncationjob -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -instancename [instance SID] -deletionpolicy [automatic | keepnewest | keepspecificnumber] -retentionduration [duration value] -retentionunit [day | week | month | year] -numberoffiles [number of archive files to create]
```

Command Options

The following table describes the options available for the startoraclelogtruncationjob command:

Table 74: StartOracleLogTruncationJob command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-protectedserver	Use this option to specify the protected machine for which you want to enable Oracle log truncation as a nightly job.

Option	Description
-instancename	The name of the Oracle instance for which you want to start log truncation.
-deletionpolicy	Optional. This option must be represented by one of the following values: • "automatic" • "keepnewest" • "keepspecificnumber"
-retentionduration	Optional. This value determines the length of time to keep a log before truncating and is constrained to positive integer values. If using the "keepnewest" value of the -deletionpolicy option, a retention duration value is required.
-retentionunit	Optional. This option identifies the time unit for the -retentionduration option. It must be represented by one of the following values: • "day" • "week" • "month" • "year"
-numberoffiles	Optional. This option sets the number of recent archive log files to keep. If using the "keepspecificnumber" value of the -deletionpolicy option, a number of files value is required.

Examples:

Start the Oracle log truncation job for the ORCL instance on a specified protected server:

```
>cmdutil /startoraclelogtruncationjob -core 10.10.127.42 -user admin -password
676df#df -protectedserver 10.10.34.88 -instancename ORCL
```

Start the Oracle log truncation job for the ORCL instance on a specified protected server and configure the deletion policy as "keepnewest" with the logs kept for 10 days:

```
>cmdutil /startoraclelogtruncationjob -protectedserver 10.10.34.88 -instancename
ORCL -deletionpolicy keepnewest -retentionduration 10 -retentionunit day
```

StopCoreService

Use this command to stop the Core service on a Core machine.

Usage

The usage for the command is as follows:

```
/stopcoreservice -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false] -wait [time in seconds]
```

Command Options

The following table describes the options available for the `stopcoreservice` command:

Table 75: StopCoreService command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."
`-wait`	Optional. This option indicates that the command should wait until the Core service is fully stopped for the specified period of time in seconds before canceling active jobs.

Example:

Stop the Core service:

```
>cmdutil /stopcoreservice -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true -wait 600
```

SuspendScheduler

This command lets you suspend or pause the task scheduler it has been paused.

Usage

The usage for the command is as follows:

```
/suspendscheduler -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false]
```

Command Options

The following table describes the options available for the `suspendscheduler` command:

Table 76: SuspendScheduler command options

Option	Description
`-?`	Display this help message.
`-restore`	[`snapshots`], [`replication`] or [`vmexport`].
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."

Example:

Pause the task scheduler:

```
>cmdutil /suspendscheduler -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true
```

UpdateRepository

The `updaterepository` command adds a new storage location to an existing DVM repository.

NOTE: This command is deprecated.

Usage

The usage for the command is as follows:

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath
[data path] -metadatapath [metadata path] | [-uncpath [UNC path] -shareusername
[share user name] -sharepassword [share password] -core [host name] -user [user
name] -password [password]
```

Command Options

The following table describes the options available for the `updaterepository` command:

Table 77: UpdateRepository command options

Option	Description
`-?`	Display this help message.
`-name`	Repository name.
`-size`	Size of repository storage location. Available units are b, Kb, Mb, Gb, Tb, and Pb.
`-datapath`	For local location only. Determines data path of repository storage location.
`-metadatapath`	For local location only. Determines metadata path of repository storage location.
`-uncpath`	For share location only. Determines data and metadata paths of repository storage location.
`-shareusername`	For share location only. Determines user name to share location.
`-sharepassword`	For share location only. Determines password to share location.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.

Examples:

Create a new storage location in a local DVM repository:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository
-metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -
password 23WE@#$sdd
```

Create a storage location for a DVM repository at a shared location:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath
\\share\repository -shareusername login -sharepassword 23WE@#$sdd -core
10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

Version

The `version` command displays information about the version of the Rapid Recovery software installed on the specified server. If you do not specify a core or protected server, the information returned applies to the Core on which you are currently working.

Usage

The usage for the command is as follows:

```
/[version | ver] -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `version` command:

Table 78: Version command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Optional. The protected machine for which you want to view version information. If you do not specify a protect machine, the return is information about the Core machine on which you are working.

Example:

Display information about the version of Rapid Recovery installed on the current Rapid Recovery Core:

```
>cmdutil /version
```

VirtualStandby

You can use the `virtualstandby` command to export data from a Rapid Recovery protected machine to a compatible virtual machine.

Usage

The usage for the command is as follows:

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname [virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal machine] -initialexport
```

Command Options

The following table describes the options available for the `virtualstandby` command:

Table 79: VirtualStandby command options

Option	Description
-?	Display this help message.
-exporttype	This option exports data from a protected machine to one of the following specified virtual servers: • esxi (ESXi) • vm (VMware Workstation) • hyperv (Hyper-V) • vb (VirtualBox)
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-protectedserver	Use this option to specify the protected machine whose recovery points you want to export.
-volumes	Optional. Use this option to list the names of the volumes that you want to export. If you do not specify volumes, then all volumes in the recovery point will export. Enclose values in double quotes and separate them with a space; for example: "c:" "d:". Do not use trailing slashes in volumes names.
-ram	Use this option to allocate a specific amount of RAM on the virtual server.
-usesourceram	Optional. Use this option to allocate the same amount of RAM on the virtual server that the source machine contains.
-vmname	The Windows name of the virtual machine.

-gen2	Optional. This option specifies Generation 2 of the VM server. If you do not specify the generation, the command uses Generation 1. The following operating systems support Generation 2:
	• Windows
	  • Windows Server 2012 R2
	  • Windows 8.1
	• Ubuntu Linux
	  • CentOs
	  • RHEL
	  • Oracle Linux 7

-hostname	For ESXi and Hyper-V virtual exports only. The virtual server host name.
-linuxhostname	For VirtualBox exports only. The virtual server host name.

Option	Description
-hostport	For ESXi and Hyper-V virtual exports only. The virtual server port number.
-hostusername	For ESXi and Hyper-V virtual exports only. The user name for the virtual server host.
-hostpassword	For ESXi and Hyper-V virtual exports only. The password for the virtual server host.
-diskprovisioning	For ESXi exports only. Optional. The amount of disk space that you want to allocate on the virtual machine. Use one of the two following specifications: • Thick - This specification makes the virtual disk as large as the original drive on the protected machine. • Thin - This specification allocates the amount of actual disk space occupied on the original drive with a few additional megabytes. The default specification is "thin."
-diskmapping	For ESXi exports only. Optional. This option determines how to map the disks from the protected machine to the virtual machine. Use one of the following values: • auto - This value automatically maps the disks. • manual - This value lets you map the disks manually. • withvm - This value stores the virtual disks in a datastore that you select. The default value is "auto."
-targetpath	For VMware Workstation and VirtualBox exports only. This option specifies the local or network path—or Linux path, for VirtualBox only—to the folder where you want to store the virtual machine files.
-pathusername	For VMware Workstation exports only. It is the user name for the network machine. It is only required when you specify a network path in the -targetpath option.
-pathpassword	For VMware Workstation exports only. It is the password for the network machine. It is only required when you specify a network path in the -targetpath option.
-uselocalmachine	For Hyper-V exports only. Optional. Use this command to connect to the local Hyper-V server. This option ignores the -hostname, -hostport, -hostusername, and -hostpassword options.
-edit	Optional. This option lets you edit existing virtual machines. It ignores the -exporttype and -initialexport options.
-initialexport	Optional. This option specifies whether to start an initial on-demand virtual machine export after you configure a continuous virtual standby.

Examples:

Set up a virtual standby export to an ESXi virtual machine with the name, amount of RAM, and disk size of the source protected server:

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

Set up a virtual standby export to a VMware Workstation machine file on the local drive:

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath
c:\virtualmachines -ram 4096
```

Set up a virtual standby export to a Hyper-V machine files and store them on a remote machine:

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user adminstrator -
password 23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win20008-Smith -vmlocation
\\WIN7-Bobby\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root
-hostpassword 12QWsdxc@# -ram 4096
```

Localization

When running on the same machine on which Rapid Recovery Core is installed, the Rapid Recovery Command Line Management utility bases its display language on the language set for the Rapid Recovery Core. In this release, supported languages include English, Chinese (Simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish.

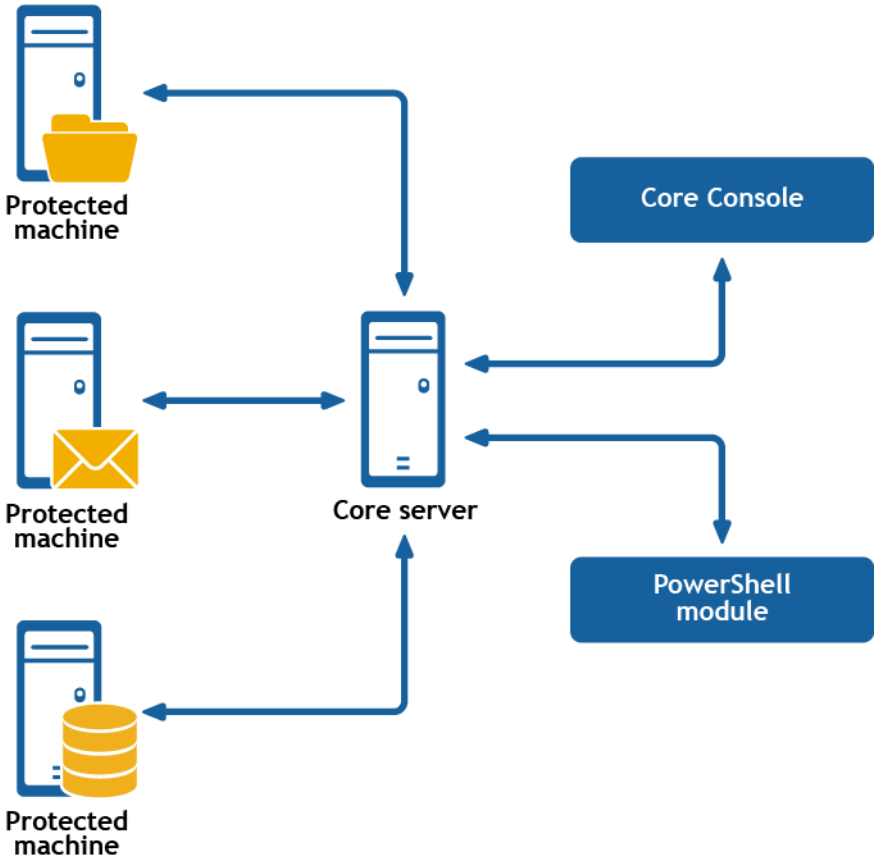
If the Rapid Recovery Command Line Management utility is installed on a separate machine, English is the only language supported.

PowerShell module

Rapid Recovery consists of several software components. Key components relevant to this topic include the following:

- The Rapid Recovery manages authentication for protected machines, schedules for transferring data for backup and replication, export to virtual machines, reporting, and bare metal restore (BMR) to similar or dissimilar hardware.
- The Rapid Recovery Agent is responsible for taking volume snapshots and for fast transfer of the data to the repository managed by the Core.
- The Rapid Recovery PowerShell Module is a Windows utility that lets users interact with the Core server by using Windows PowerShell® scripts. This module offers some of the same functionality that the Rapid Recovery Core Console graphic user interface (GUI) provides. For example, the Rapid Recovery PowerShell Module can mount Rapid Recovery recovery points or force a snapshot of a protected machine.

The PowerShell module interacts with the Rapid Recovery Core



PowerShell is a Microsoft .NET Framework-connected environment designed for administrative automation. This section describes the Rapid Recovery PowerShell module and the cmdlets administrators can use to script certain functions without interaction with the Rapid Recovery Core GUI.

NOTE: You can also run PowerShell scripts as pre and post scripts. For more information and sample scripts, see Scripting.

The Rapid Recovery PowerShell Module is automatically installed and registered when you install the Rapid Recovery Core. The module is installed in your Windows system directory in the path: [Environment.SystemDirectory]\WindowsPowerShell\v1.0\Modules\RapidRecoveryPowerShellModule. For example, for x86 or 32-bit OS, it is installed in C:\Windows\System32\WindowsPowerShell\v1.0\Modules\RapidRecoveryPowerShellModule. When using the module, run PowerShell as an Administrator, and then change the directory to the location of the module.

Prerequisites for using PowerShell

Before using the Rapid Recovery PowerShell module, you must have Windows PowerShell 2.0 or later installed. Due to new features introduced in PowerShell 3.0, including easier access to object properties, PowerShell Web access, and support for REST calls, Quest recommends using PowerShell 3.0 or later.

Note: Make sure to place the powershell.exe.config file in the PowerShell home directory; for example, C:\WindowsPowerShell\powershell.exe.config.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
       <startup useLegacyV2RuntimeActivationPolicy="true">
              <supportedRuntime version="v4.0.30319"/>
              <supportedRuntime version="v2.0.50727"/>
       </startup>
</configuration>
```

Working with commands and cmdlets

Cmdlets are specialized commands in a Windows PowerShell script that perform a single function. A cmdlet is typically expressed as a verb-noun pair. The result returned by a cmdlet is an object.

You can pipeline PowerShell commands, which enables the output of one cmdlet to be piped as input to another cmdlet. As a simple example, you can request the list of commands in the Rapid Recovery PowerShell module, and sort that list by name. The example script for this is:

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

Getting cmdlet help and examples

After you open PowerShell and import the Rapid Recovery PowerShell module, you can request additional information at any time by using the Get-Help <command_name> cmdlet. For example, to get information about the virtual machine export cmdlet, enter the following cmdlet and then press Enter:

```
Get-Help Start-VMExport
```

The object returned includes the command name, synopsis, syntax, and any options you can use with the command.

Another method to get help for a specific cmdlet is to type the command name followed by `-?`. For example:

```
Start-VMExport -?
```

You can also request examples for a cmdlet by executing the following command:

```
>Get-Help Start-VMExport -examples
```

Rapid Recovery PowerShell module cmdlets

This section describes the cmdlets and options available in the Rapid Recovery PowerShell Module. All cmdlets in the Rapid Recovery PowerShell Module support the following common parameters:

- Verbose
- Debug
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

For more information, use `Get-Help about_commonparameters`.

Add-EsxAutoProtectObjects

The `Add-EsxAutoProtectObjects` cmdlet enables auto protection for specified objects on a vCenter or ESXi server.

Usage

The usage for the command is as follows:

```
Add-EsxAutoProtectObjects -core [host name] -user [user name] -password [password] -
repository [name] -protectedserver [name | IP address] -autoprotect [object name
collection]
```

Command Options

The following table describes the options available for the `Add-EsxAutoProtectObjects` command:

Table 80: Add-EsxAutoProtectObjects command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-autoprotect`	Optional. This option lets you list the new virtual machines that you want to automatically protect.

Example:

Put specific objects from a vCenter or ESXi server under auto-protection by the Core:

```
>Add-EsxAutoProtectObjects -protectedserver 10.10.8.150 -add -autoprotect
"Folder1", "Folder2"
```

Add-EsxVirtualMachines

The `Add-EsxVirtualMachines` cmdlet lets you add specific virtual machines (VMs) on vCenter or ESXi server under the protection of a Core.

Usage

The usage for the command is as follows:

```
Add-EsxVirtualMachines -core [host name] -user [user name] -password [password] -
repository [name] -protectedserver [name | IP address] -virtualmachines [virtual
machines collection | all]
```

Command Options

The following table describes the options available for the `Add-EsxVirtualMachines` command:

Table 81: Add-EsxVirtualMachines command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to store the data of the virtual machine. **NOTE:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to edit the vCenter or ESXi objects for a specific protected machine.
`-virtualmachines`	A list of virtual machines each separate by a comma.

Example:

Add two VMs from a vCenter or ESXi server under protection by the Core:

```
>Add-EsxVirtualMachines -repository "repository1" -protectedserver 10.10.10.10 -
virtualmachines "vm1", "vm2"
```

Add-HyperVClusterSharedVirtualDisks

The `Add-HyperVClusterSharedVirtualDisks` cmdlet lets you add shared Hyper-V virtual disks under the protection of a Core.

Usage

The usage for the command is as follows:

```
Add-HyperVClusterSharedVirtualDisks -core [host name] -user [user name] -password
[password] -repository [name] -shareddisks [shared virtual disks name or path
collection | all]
```

Command Options

The following table describes the options available for the `Add-HyperVClusterSharedVirtualDisks` command:

Table 82: Add-HyperVClusterSharedVirtualDisks command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to store the data of the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to edit the shared virtual disks for a specific protected machine.
`-shareddisks`	A list of shared disks each separate by a comma.

Example:

Protect all of the shared virtual disks on a cluster:

```
>Add-HyperVClusterSharedVirtualDisks -protectedserver "HV-2012R2" -repository
"Repository_10.10.55.133"  -shareddisks "all"
```

Add-HyperVClusterVirtualMachines

The `Add-HyperVClusterVirtualMachines` cmdlet lets you add specific virtual machines (VMs) from a Hyper-V cluster under the protection of a Core.

Usage

The usage for the command is as follows:

```
Add-HyperVClusterVirtualMachines -core [host name] -user [user name] -password
[password] -repository [name] -protectedserver [name | IP address] -virtualmachines
[virtual machines collection | all]
```

Command Options

The following table describes the options available for the `Add-HyperVClusterVirtualMachines` command:

Table 83: Add-HyperVClusterVirtualMachines command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to store the data of the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to protect virtual machines.
`-virtualmachines`	A list of the virtual machines that you want to protect, each separated by a comma. The name of the VM must be enclosed in double quotes.

Example:

Add specific VMs of a Hyper-V cluster under protection by the Core:

```
>Add-HyperVClusterVirtualMachines -repository "Repository 1" -protectedserver
hvcluster -virtualmachines "Win8x64-gen1", "Win2012x64-gen2"
```

Add-HyperVVirtualMachines

The `Add-HyperVVirtualMachines` cmdlet lets you add specific virtual machines (VMs) from a Hyper-V cluster under the protection of a Core.

Usage

The usage for the command is as follows:

```
Add-HyperVVirtualMachines -core [host name] -user [user name] -password [password] -
repository [name] -protectedserver [name | IP address] -virtualmachines [virtual
machines collection | all]
```

Command Options

The following table describes the options available for the `Add-HyperVVirtualMachines` command:

Table 84: Add-HyperVVirtualMachines command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that is associated with the Core that you want to use to store the data of the virtual machine. **Note:** You must enclose the name in double quotes.
`-protectedserver`	Use this option to edit Hyper-V objects for a specific virtual machine.
`-virtualmachines`	A list of the virtual machines that you want to protect, each separated by a comma. The name of the VM must be enclosed in double quotes.

Example:

Add specific VMs of a Hyper-V cluster under protection by the Core:

```
>Add-HyperVVirtualMachines -repository "Repository 1" -protectedserver HVServer1 -
virtualmachines "Win8x64-gen1", "Win2012x64-gen2"
```

Disable-HyperVAutoProtection

The `Disable-HyperVAutoProtection` cmdlet lets you disable the auto-protection feature, which automatically protects new virtual machines (VMs), on a Hyper-V host.

Usage

The usage for the command is as follows:

```
Disable-HyperVAutoProtection -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Disable-HyperVAutoProtection` command:

Table 85: Disable-HyperVAutoProtection command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	The display name, host name, or IP address of the protected Hyper-V server.

Example:

Disable auto protection of new virtual machines on the specified Hyper-V host:

```
>Disable-HyperVAutoProtection -protectedserver "10.10.1.1"
```

Edit-AzureVirtualStandby

You can use the `Edit-AzureVirtualStandby` cmdlet to change the parameters of an existing Azure virtual standby continuous export.

Usage

The usage for the command is as follows:

```
Edit-AzureVirtualStandby -core [host name] -user [user name for Core] -password
[password for Core] -protectedserver [name | IP address] -volumes [volume names |
all] -containername [container] -foldername [folder name] -subscriptionid [Azure
subscription ID] -forceedit
```

Command Options

The following table describes the options available for the `Edit-AzureVirtualStandby` command:

Table 86: Edit-AzureVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.

Option	Description
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points that you want to export.
`-volumes`	Optional. List of additional volume names to be exported. If you use the value `all` or use no value, then all volumes export. Values must be enclosed in double quotes and separated by a space. Do not use trailing slashes in volumes names; for example, use `"c:" "d:"`.
`-containername`	The name of the container in the Azure storage account (classic). The name must container between three and 63 characters (lowercase letters, numbers, and hyphens only), and start with a letter or a number. Every hyphen must be preceded and followed by a letter or number.
`-foldername`	Optional. The name of a folder inside of the Azure storage container. A folder name cannot contain any of the following characters: `\ / : * ? " < > |`.
`-subscriptionid`	The identifier of a previously added Azure subscription.
`-forceedit`	Optional. This option lets you delete existing export files when you change an export location.

Example:

Edit an Azure virtual standby export:

```
>Edit-AzureVirtualStandby -protectedserver 10.10.5.22 -subscriptionid "111111-22222-33333-4444-555555" -containername container1 -foldername folder2
```

Edit-EsxiVirtualStandby

The `Edit-EsxiVirtualStandby` command lets you use PowerShell to make changes to an existing virtual export to an ESXi virtual machine (VM).

Usage

The usage for the command is as follows:

```
Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-ErroAction<ActionPreference>] [-WarningAction<ActionPreference>] [-ErrorVariable String>] [-WarningVariable <String> [-OutVariable <String>] [-OutBuffer <Int32>]
```

Command Options

The following table describes the options available for the `Edit-EsxiVirtualStandby` command: Updated option descriptions TK.

Table 87: Edit-EsxiVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create boot CDs), `'diagnostics'` (upload logs), `'exchange'` (Exchange Server files check), `'export'` (recovery point export), `'pushinstall'` (deploy agents), `'rollback'` (restoring from a recovery point), `'rollup'` (recovery point rollups), `'sqlattach'` (agent attachability checks), and `'mount'` (mount repository). By default, all jobs of the specified type are returned.
`-time`	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all active jobs on the local Core:

```
>Get-activejobs -all
```

Edit-HyperVVirtualStandby

The `Edit-HyperVVirtualStandby` command lets you use PowerShell to make changes to an existing virtual export to a Hyper-V virtual machine (VM).

Usage

The usage for the command is as follows:

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName
<String>] [-HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2]
[-UseVhdx] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-
UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>]
[-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-ErrorVariable <String>] [-WarningVariable <String>] [-
OutVariable <String>] [-OutBuffer <Int32>] -exportvmconfigfiles
```

Command Options

The following table describes the options available for the `Edit-HyperVVirtualStandby` command:

Table 88: Edit-HyperVVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-hostname`	Virtual server host name.
`-hostport`	Virtual server port number.
`-hostusername`	Login to the virtual server host.
`-hostpassword`	Password to the virtual server host.
`-vmlocation`	Location of the virtual machine.
`-uselocalmachine`	Optional. Connect to the local Hyper-V server. In this case, the command ignores the following options: 'hostname', 'hostport', 'hostusername', and 'hostpassword'.
`-gen2`	Optional. The virtual machine generation. If not specified, the command uses generation 1. Windows Server 2012 R2 and
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Option	Description
-all	Show all jobs, including those performed by the Core and all protected servers.
-number	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
-jobtype	Optional. Specifies the job type filter. Available values are: 'transfer' (data transfer), 'repository' (repository maintenance), 'replication' (local and remote replications), 'backup' (backup and restore), 'bootcdbuilder' (create boot CDs), 'diagnostics' (upload logs), 'exchange' (Exchange Server files check), 'export' (recovery point export), 'pushinstall' (deploy agents), 'rollback' (restoring from a recovery point), 'rollup' (recovery point rollups), 'sqlattach' (agent attachability checks), and 'mount' (mount repository). By default, all jobs of the specified type are returned.
-time	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).
-exportvmconfigfiles	Optional. Specify whether to export virtual machine configuration files. This option is available only both when the source is a virtual protected agentlessly and when the target hpyervisor is the same as the source hypervisor.

Example:

Lists all active jobs on the local Core:

```
>Get-activejobs -all
```

Edit-OracleDBVerifyNightlyJob

Use the command `Edit-OracleDBVerifyNightlyJob` to enable or disable this nightly job for specific Oracle machines that are under protection.

Usage

The usage for the command is as follows:

```
Edit-OracleDBVerifyNightlyJob -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] [-enable | -disable] [-global]
```

Command Options

The following table describes the options available for the `Edit-OracleDBVerifyNightlyJob` command:

Table 89: Edit-OracleDBVerifyNightlyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle DBVerify nightly job.
`-enable`	Use this option to enable the DBVerify nightly job for the specified protected machine.
`-disable`	Use this option to disable the DBVerify nightly job for the specified protected machine.
`-global`	Use this option to apply the specified setting as the default for this Core.

Examples:

Enable the Oracle DBVerify nightly job for a protected server:

```
Edit-OracleDBVerifyNightlyJob -core 10.10.127.42 -user admin -password 676df#df -
protectedserver 10.10.34.88 -enable
```

Disable the Oracle DBVerify nightly job for a protected server:

```
Edit-OracleDBVerifyNightlyJob -core 10.10.127.42 -user admin -password 676df#df -
protectedserver 10.10.34.88 -disable
```

Edit-OracleLogTruncationNightlyJob

Use the command `Edit-OracleLogTruncationNightlyJob` to enable or disable this nightly job for specific Oracle machines that are under protection and to set the deletion policy and retention duration for the logs.

Usage

The usage for the command is as follows:

```
Edit-OracleLogTruncationNightlyJob -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] [-enable | -disable] [-global] [-
usedefault] -deletionpolicy [automatic | keepnewest | keepspecificnumber] -
retentionduration [duration value] -retentionunit [day | week | month | year] -
numberoffiles [number of archive files to create]
```

Command Options

The following table describes the options available for the `Edit-OracleLogTruncationNightlyJob` command:

Table 90: Edit-OracleLogTruncationNightlyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable Oracle log truncation as a nightly job.
`-enable`	Use this option to enable log truncation for the specified protected machine. This is the default option and can be omitted.
`-disable`	Use this option to disable log truncation for the specified protected machine.
`-global`	Use this option to apply the specified setting as the default for this Core.
`-all`	This option applies the specified changes for every protected machine that has at least one Oracle instance installed.
`-usedefault`	Optional. Use this option to apply the default Core settings to the specified machine, which may also be set by using the `-global` option.
`-deletionpolicy`	Optional. This option must be represented by one of the following values: • `"automatic"` • `"keepnewest"` • `"keepspecificnumber"`
`-retentionduration`	Optional. This value determines the length of time to keep a log before truncating and is constrained to positive integer values. If using the `"keepnewest"` value of the `-deletionpolicy` option, a retention duration value is required.
`-retentionunit`	Optional. This option identifies the time unit for the `-retentionduration` option. It must be represented by one of the following values: • `"day"` • `"week"` • `"month"` • `"year"`
`-numberoffiles`	Optional. This option sets the number of recent archive log files to keep. If using the `"keepspecificnumber"` value of the `-deletionpolicy` option, a number of files value is required.

Examples:

Edit the Oracle log truncation nightly job settings for the Core globally:

```
Edit-OracleLogTruncationNightlyJob -core 10.10.127.42 -user admin -password 676df#df
-protectedserver 10.10.34.88 -global -deletionpolicy keepspecificnumber -
numberoffiles 15
```

Disable the Oracle log truncation nightly job for a specified protected server:

```
Edit-OracleLogTruncationNightlyJob -core 10.10.127.42 -user admin -password 676df#df
-protectedserver 10.10.34.88 -disable
```

Edit-Replication

Use the `Edit-Replication` to make changes to an existing replication relationship between two Cores.

Usage

The usage for the command is as follows:

```
Edit-Replication -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -incoming [host name] -outgoing [host name] -add
```

Command Options

The following table describes the options available for the `Edit-Replication` command:

Table 91: Edit-Replication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
`-protectedserver`	Use this option to specify the protected machine for which you want to enable Oracle log truncation as a nightly job.
`-add`	Add protected servers to an existing replication.
`-scheduletype`	The type of replication schedule. This option should be specified by one of the following values: • 1. "`atalltimes`" - to automatically replicate at all times.

Option	Description
	• 2. "daily" - to automatically replicate once each day, with specific "-dailystarttime" and "-dailyendtime" parameters. • 3. "custom" - to automatically replicate on specified weekdays or weekends designated by "-weekdaystarttime," "-weekdayendtime," "-weekendstarttime," and "-weekendendtime" parameters.
-dailystarttime	Use only for the daily value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the earliest time of day when you want replication to start.
-dailyendtime	Use only for the daily value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of day when you want replication to start.
-weekdaystarttime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the earliest time of a weekday when you want replication to start.
-weekdayendtime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of a weekday when you want replication to start.
-weekendstarttime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the earliest time of the weekend when you want replication to start.
-weekendendtime	Use only for the custom value of the -scheduletype option. It is used to establish a window of time for when replication should occur. Use this option to specify the latest time of the weekend when you want replication to start.

Examples:

Edit the replication schedule by specifying weekdays and weekends:

```
>Edit-Replication -id RemoteServerHostName -scheduletype custom -weekdaystarttime
"9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime
"6:00 PM"
```

Add protected servers to existing replication:

```
>Edit-Replication -id RemoteServerHostName -protectedserver
"10.10.1.1","Repository1"
```

Edit-ScheduledArchive

The Edit-ScheduledArchive command lets you use PowerShell to make changes to an existing scheduled archive.

Usage

The usage for the command is as follows:

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP
address2]"] -path [location] -cloudaccountname [name] -cloudcontainer [name] -
recycleaction [type] -scheduletype [type] -dayofweek [name] -dayofmonth [number] -
time [time] -initialpause -id archiveretention [months]
```

Command Options

The following table describes the options available for Edit-ScheduledArchive command:

Table 92: Edit-ScheduledArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	The protected machine with recovery points that you want to archive. You can specify multiple machine names enclosed in double quotes and separated by commas.
`-all`	Archive recovery points for all protected machines.
`-path`	The path to where to save the archived data. For example: • Local machine: "d:\work\archive" • Network path: "\\servername\sharename" • Folder in a cloud account: "Folder Name" **Note:** The number of symbols should not be greater than 100 for local and network locations, and should not be greater than 150 for a cloud location.
`-cloudaccountname`	Optional. Use only for cloud archiving. The name of the cloud account where you want to save the archive.
`-cloudcontainer`	Optional. Use only for cloud archiving. The name of the cloud container in the chosen cloud account, where the archive will be saved. When you use this option, you should also specify the "-cloudaccountname" parameter.
`-recycleaction`	The type of recycle action. Specified by using one of the following four values: • "replacethiscore" - Overwrites any pre-existing archived data pertaining to this Core, but leaves the data for other Cores intact. • "erasecompletely" - Clears all archived data from the directory before writing the new archive.

Option	Description
	• "incremental" - Lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.
`-scheduletype`	Type of schedule interval. Specified the option with one of the following four values: • "daily" - For a daily automatically created archive. • "weekly" - For a weekly automatically created archive. You must specify the "-dayofweek" parameter. • "monthly" - For a monthly automatically created archive. You must specify the "-dayofmonth" parameter. If a month does not have the day specified—for example, "31"—then the archive will not occur for that month. • "lastdayofmonth" - For automatically creating an archive on the last day of each month.
`-dayofweek`	Use only for the "weekly" option of the "-scheduletype" parameter. The day of the week on which to automatically create the archive (for example, "Monday").
`-dayofmonth`	Use only for the "month" option of the "-scheduletype" parameter. The day (number) of the month on which to automatically create the archive (for example, "15").
`-time`	The hour of the day when you want to create an archive.
`-initialpause`	Optional. Specify this option if you want to initially pause archiving after you configure the archiving schedule.
`-id`	The identifier of the scheduled archive that you want to edit.
`-archiveretention`	Optional. Specifies the number of months to retain archived recovery points. Archived recovery points older than the specified number of months will be automatically removed.

Example:

Edit a scheduled archive on the local Core:

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -
scheduletype daily -time 12:00 AM -initialpause -i
    d archiveid
```

Edit-VBVirtualStandby

The `Edit-VBVirtualStandby` command lets you use PowerShell to make changes to an existing virtual export to a VirtualBox virtual machine (VM).

Usage

The usage for the command is as follows:

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword
<String>] [-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>]
[-AccountPassword <String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-
VMName <String>] [-UseSourceRam] [-Ram <String>] [-User <String>] [-Core <String>]
[-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-
WarningAction <ActionPreference>] [-ErrorVariable <String>] [-WarningVariable
<String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Command Options

The following table describes the options available for the `Edit-VBVirtualStandby` command:
Updated option descriptions TK.

Table 93: Edit-VBVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create boot CDs), `'diagnostics'` (upload logs), `'exchange'` (Exchange Server files check), `'export'` (recovery point export), `'pushinstall'` (deploy agents), `'rollback'` (restoring from a recovery point), `'rollup'` (recovery point rollups), `'sqlattach'` (agent attachability checks), and `'mount'` (mount repository). By default, all jobs of the specified type are returned.
`-time`	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all active jobs on the local Core:

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

The `Edit-VMVirtualStandby` command lets you use PowerShell to make changes to an existing virtual export to a VMware Workstation virtual machine (VM).

Usage

The usage for the command is as follows:

```
 Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-
PathPassword <String>] [-ProtectedServer <S
    tring>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>]
[-User <String>] [-Core <String>]
    [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-
WarningAction <ActionPreference>] [-Er
    rorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-
OutBuffer <Int32>]
```

Command Options

The following table describes the options available for the `Edit-VMVirtualStandby` command:

Table 94: Edit-VMVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-targetpath`	The local or network path (or Linux path, only for VirtualBox export) to the folder for storing the virtual machine files.
`-pathusername`	The credentials for the target path when it is located on a network share and you specified it with the `-targetpath` option.
`-pathpassword`	The password for the target path when it is located on a network share and you specified it with the `-targetpath` option.

Option	Description
-protectedserver	The protected machine with recovery points that you want to export, indicated by IP address.
-volumes	Optional. A list of volume names that you want to export. When not specified, all volumes export. Values must be separated by a comma. Do not use trailing slashes in volume names. For example: C, F, E.
-vmname	The Windows name of the virtual machine.
-ram	Use this option to allocate a specific amount of RAM on the virtual server.
-usesourceram	Optional. Allocate all of the amount of RAM on the target virtual server that is used on the source virtual server.

Example:

Edit a specific amount of RAM on the existing Virtual Standby:

```
>Edit-VMVirtualStandby -targetpath "\\servername\sharename" -pathusername "login" -
pathpassword "password" -protectedserver 10.10.11.245 -vmname "name" -ram 2048
```

Edit the list of volume names to be exported to the existing Virtual Standby:

```
>Edit-VMVirtualStandby -targetpath "\\servername\sharename" -pathusername "login" -
pathpassword "password" -protectedserver 10.10.11.245 -vmname "name" -volumes C,F
```

Enable-HyperVAutoProtection

The `Enable-HyperVAutoProtection` cmdlet lets you enable the auto-protection of new virtual machines (VMs) on a Hyper-V host.

Usage

The usage for the command is as follows:

```
Enable-HyperVAutoProtection -core [host name] -user [user name] -password [password]
-repository [name] -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Enable-HyperVAutoProtection` command:

Table 95: Enable-HyperVAutoProtection command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.

Option	Description
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-repository	Required. The name of the repository that is associated with the Core that you want to use to store the data of the virtual machine. **Note:** You must enclose the name in double quotes.
-protectedserver	Use this option to protect virtual machines.

Example:

Enable auto-protection of new VMs on a Hyper-V host:

```
>Enable-HyperVAutoProtection -protectedserver 10.10.1.1 -repository "Repository 1"
```

Enable-OracleArchiveLogMode

Use the command `Enable-OracleArchiveLogMode` to enable or disable this mode for specific Oracle machines that are under protection.

Usage

The usage for the command is as follows:

```
Enable-OracleArchiveLogMode -core [host name] -user [user name] -password [password]
-protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Enable-OracleArchiveLogMode` command:

Table 96: Enable-OracleArchiveLogMode command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password,

Option	Description
	you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle archive log mode.

Example:

Enable the Oracle archive log mode for a protected server:

```
>Enable-OracleArchiveLogMode -core 10.10.127.42 -user admin -password 676df#df -
protectedserver 10.10.34.88
```

Get-ActiveJobs

The `Get-ActiveJobs` command returns all active jobs from the Core. The `-jobtype` parameter could be used to observe specific jobs.

Usage

The usage for the command is as follows:

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |  -
protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Command Options

The following table describes the options available for the `Get-ActiveJobs` command:

Table 97: Get-ActiveJobs command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Option	Description
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create boot CDs), `'diagnostics'` (upload logs), `'exchange'` (Exchange Server files check), `'export'` (recovery point export), `'pushinstall'` (deploy agents), `'rollback'` (restoring from a recovery point), `'rollup'` (recovery point rollups), `'sqlattach'` (agent attachability checks), and `'mount'` (mount repository). By default, all jobs of the specified type are returned.
`-time`	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all active jobs on the local Core:

```
>Get-activejobs -all
```

Get-CloudAccounts

The `Get-CloudAccounts` command lets you get information about the cloud accounts that have been added to the Core.

Usage

The usage for the command is as follows:

```
Get-CloudAccounts -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Get-CloudAccounts` command:

Table 98: Get-CloudAccounts command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Get information about cloud accounts:

```
>Get-CloudAccounts -core 10.10.10.10 -user administrator -password 23WE@#$sdd
```

Get-Clusters

The `Get-Clusters` command returns information about server clusters protected in the Core.

Usage

The usage for the command is as follows:

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Get-Clusters` command:

Table 99: Get-Clusters command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

List server clusters protected on the local Core:

```
>Get-Clusters
```

Get-CompletedJobs

The `Get-CompletedJobs` command returns a list of jobs completed on the Core. The `-jobtype` parameter could be used to observe specific jobs.

Usage

The usage for the command is as follows:

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |
  -protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Command Options

The following table describes the options available for the `Get-CompletedJobs` command:

Table 100: Get-CompletedJobs command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create

Option	Description
	boot CDs), 'diagnostics' (upload logs), 'exchange' (Exchange Server files check), 'export' (recovery point export), 'pushinstall' (deploy agents), 'rollback' (restoring from a recovery point), 'rollup' (recovery point rollups), 'sqlattach' (agent attachability checks), and 'mount' (mount repository). By default, all jobs of the specified type are returned.
-time	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all active jobs on the local Core:

```
>Get-CompletedJobs -all
```

Lists all completed create repository jobs on the local Core:

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

The Get-ExchangeMailStores command returns information about male stores on Exchange servers Protected by the Core.

Usage

The usage for the command is as follows:

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]  -protectedserver [server name or IP address]
```

Command Options

The following table describes the options available for the Get-ExchangeMailStores command:

Table 101: Get-ExchangeMailStores command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.

Option	Description
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Show jobs for a specific protected machine, indicated by IP address.

Example:

Lists Exchange mail stores for Exchange server for the local Core:

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

The `Get-Failed` command returns information about failed recovery points on the local Core.

Usage

The usage for the command is as follows:

```
Get-Failed -core [host name] -user [user name] -password [password] -all | -protectedserver [server name or IP address] -number [all | f[number] |l [number] | number]
```

Command Options

The following table describes the options available for the `Get-Failed` command:

Table 102: Get-Failed command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-protectedserver	Show jobs for a specific protected machine, indicated by IP address.
-number	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.

Example:

Lists all failed recovery points:

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

The `Get-FailedJobs` command returns all failed jobs from the local Core.

Usage

The usage for the command is as follows:

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |  -
protectedserver [server name or IP address] -number [all | f[number] |l[number] |
number] -jobtype [type] -time [time]
```

Command Options

The following table describes the options available for the `Get-FailedJobs` command:

Table 103: Get-FailedJobs command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Show jobs for a specific protected machine, indicated by IP address.

Option	Description
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create boot CDs), `'diagnostics'` (upload logs), `'exchange'` (Exchange Server files check), `'export'` (recovery point export), `'pushinstall'` (deploy agents), `'rollback'` (restoring from a recovery point), `'rollup'` (recovery point rollups), `'sqlattach'` (agent attachability checks), and `'mount'` (mount repository). By default, all jobs of the specified type are returned.
`-time`	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all failed jobs on the local Core:

```
>Get-FailedJobs -all
```

Lists all failed create backup jobs on the local Core:

```
>Get-FailedJobs -type backup
```

Get-HyperVClusterSharedVirtualDisks

The `Get-HyperVClusterSharedVirtualDisks` command provides information about machines protected on the local Core.

Usage

The usage for the command is as follows:

```
Get-HyperVClusterSharedVirtualDisks -protectedserver [name | IP address] -shareddisk
[shared virtual disk name (path)]
```

Command Options

The following table describes the options available for the `Get-HyperVClusterSharedVirtualDisks` command:

Table 104: Get-HyperVClusterSharedVirtualDisks command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	This option shows all of the shared virtual disks for a specific protected cluster.
`-shareddisk`	The name of a specific shared disk.

Example:

Retrieve a collection of all shared disks:

```
>Get-HyperVClusterSharedVirtualDisks -protectedserver "HV-2012R2" -shareddisk
"Shared Disk 1"
```

Get-ListAzureVMSizes

The `Get-ListAzureVMSizes` command provides a list of the available virtual machines sizes for deploying to Azure.

Usage

The usage for the command is as follows:

```
Get-ListAzureVMSizes -core [host name] -user [user name] -password [password] -
cloudaccountname [Azure account name] -storageaccountname [Azure storage account
name] -subscriptionid [subscription ID] -cloudservicename [service name]
```

Command Options

The following table describes the options available for the `Get-ListAzureVMSizes` command:

Table 105: Get-ListAzureVMSizes command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number).

Option	Description
	By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-cloudaccountname`	Optional when specifying `-storageaccountname`. Specify the name of the Azure cloud account.
`-storageaccountname`	Optional when specifying `-cloudaccountname`. Specify the name of the Azure storage account.
`-subscriptionid`	The Azure subscription ID.
`-cloudservicename`	The name of the Azure cloud service.

Example:

View a list of the available virtual machine sizes for the cloud account Account1:

```
>Get-CloudAccounts -cloudaccountname Account1 -cloudservicename Service
```

View a list of the available virtual machine sizes for the storage account named "teststorage:"

```
>Get-CloudAccounts -storageaccountname teststorage -cloudservicename Service
```

Get-Mounts

The `Get-Mounts` command returns all recovery points mounted on the local Core.

Usage

The usage for the command is as follows:

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver
[server name or IP address]
```

Command Options

The following table describes the options available for the `Get-Mounts` command:

Table 106: Get-Mounts command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Example:

Show all mounted recovery points:

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Get-OracleInstances

The `Get-OracleInstances` command lists the Oracle instances that are running a specified protected server.

Usage

The usage for the command is as follows:

```
Get-OracleInstances -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Get-OracleInstances` command:

Table 107: Get-OracleInstances command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the

Option	Description
	logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-protectedserver	The name or IP address of the protected machine.

Example:

List the Oracle instances running on a specified protected server:

```
Get-OracleInstances -core 10.10.127.42 -user admin -password -676df#df -
protectedserver 10.10.34.88
```

Get-Passed

The `Get-Passed` command returns information about recovery points that have passed verification checks on the Core.

Usage

The usage for the command is as follows:

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver
[server name or IP address] -number [all | f[number] |l[number] | number]
```

Command Options

The following table describes the options available for the `Get-Passed` command:

Table 108: Get-Passed command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Lists all recovery points on the local Core the passed verification checks:

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

The `Get-ProtectedServers` command provides information about machines protected on the local Core.

Usage

The usage for the command is as follows:

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Get-ProtectedServers`command:

Table 109: Get-ProtectedServers command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-withclusters`	Optional. If they exist, include clusters and cluster nodes in the resulting protected server list.

Example:

Lists all machines, including clusters and cluster nodes, protected by the specified Core:

```
>Get-ProtectedServers -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
withclusters
```

Get-ProtectionGroups

The `Get-ProtectionGroups` command returns information about protection groups on the local Core.

Usage

The usage for the command is as follows:

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |
  -protectedserver [server name or IP address]
```

Command Options

The following table describes the options available for the `Get-ProtectionGroups` command:

Table 110: Get-ProtectionGroups command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Example:

Lists protection groups on the local Core:

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

The `Get-QueuedJobs` command returns all jobs waiting to begin from the Core.

Usage

The usage for the command is as follows:

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address] -nu
    mber [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

Command Options

The following table describes the options available for the `Get-ActiveJobs` command:

Table 111: Get-ActiveJobs command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-all`	Show all jobs, including those performed by the Core and all protected servers.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.
`-jobtype`	Optional. Specifies the job type filter. Available values are: `'transfer'` (data transfer), `'repository'` (repository maintenance), `'replication'` (local and remote replications), `'backup'` (backup and restore), `'bootcdbuilder'` (create boot CDs), `'diagnostics'` (upload logs), `'exchange'` (Exchange Server files check), `'export'` (recovery point export), `'pushinstall'` (deploy agents), `'rollback'` (restoring from a recovery point), `'rollup'` (recovery point rollups), `'sqlattach'` (agent attachability checks), and `'mount'` (mount repository). By default, all jobs of the specified type are returned.
`-time`	Optional. Filter output by date and time for the job started. Available types of input include: #d or DD (where # is a number for the period of time of days before now until now) #h or #H (where # is number for the period of hours before now until now) “time date 1”, “time date 2” (to show a custom range of time from a specific date appearing before the comma to a specific date following the comma).

Example:

Lists all queued jobs on the local Core:

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

The `Get-RecoveryPoints` command returns information about recovery points for machines protected on the local Core.

Usage

The usage for the command is as follows:

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address] -number [all | f[number] |l [number] | number]
```

Command Options

The following table describes the options available for the `Get-RecoveryPoints` command:

Table 112: Get-RecoveryPoints command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-number`	Optional. Determine how many records to display. available values are: all (display all jobs); l[number] or [number] (fetches ## most recent jobs sorted by execution and time); f[number] (displays first ## recovery jobs sorted by execution and time). By default, the 20 most recent jobs are shown.

Example:

Lists recovery points for machines protected on the local Core:

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

The `Get-ReplicatedServers` command returns information about machines replicated on the Core.

Usage

The usage for the command is as follows:

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

Quest recommends you consider security when using commands to return values. For example, this command returns the administrator password for each replicated server. If used in an MSP environment from the target Core, this can potentially expose the login password of the administrator user. For environments with encrypted repository data, this does not pose substantial security issues.

Command Options

The following table describes the options available for the `Get-ReplicatedServers` command:

Table 113: Get-ReplicatedServers command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Lists all replicated servers on the local Core:

```
>Get-ReplicatedServers
```

Get-Repositories

The `Get-Repositories` command returns information about repositories on the Core.

Usage

The usage for the command is as follows:

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Get-Repositories` command:

Table 114: Get-Repositories command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Lists repositories on the local Core:

```
>Get-Repositories
```

Get-ScheduledArchives

The `Get-ScheduledArchives` command lets you use PowerShell to view information about the existing Rapid Recovery scheduled archives associated with this Core.

Usage

The usage for the command is as follows:

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

Command Options

The following table describes the options available for the `Get-ScheduledArchives` command:

Table 115: Get-ScheduledArchives command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have

Option	Description
	to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Get information about the scheduled archives on this Core:

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

The `Get-SqlDatabases` command returns a list of SQL databases from the specified protected machine.

Usage

The usage for the command is as follows:

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]  -
protectedserver [server name or IP address]
```

Command Options

The following table describes the options available for the `Get-SqlDatabases` command:

Table 116: Get-SqlDatabases command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Example:

Lists all SQL databases jobs on the local Core:

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-TransferQueueEntries

The `Get-TransferQueueEntries` command shows a list of the transfer jobs that are still in the queue and have yet to occur.

Usage

The usage for the command is as follows:

```
Get-TransferQueueEntries -core [host name] -user [user name] -password [password] -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Get-TransferQueueEntries` command:

Table 117: Get-TransferQueueEntries command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.

Example:

View the transfer queue entries on Core "10.10.10.10" for Agent "10.10.5.22:"

```
Get-TransferQueueEntries -core 10.10.10.10 -user administrator -password -23WE@#$sdd -protectedserver 10.10.5.22
```

Get-UnprotectedVolumes

The `Get-UnprotectedVolumes` command returns information about volumes that are available for protection but not currently protected on the Core.

Usage

The usage for the command is as follows:

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server
name or IP address]
```

Command Options

The following table describes the options available for the `Get-UnprotectedVolumes` command:

Table 118: Get-UnprotectedVolumes command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on.

Option	Description
	If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Example:

Lists all volumes available for protection (but not get protected) on the specified agent machine:

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-Version

The `Get-Version` command retrieves the product version of a Core or Agent software installation.

Usage

The usage for the command is as follows:

```
Get-Version -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Get-Version` command:

Table 119: Get-Versioncommand options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password,

Option	Description
	you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.

Example:

Retrieve the product version of the present Core installation:

```
Get-Version
```

Get-VirtualizedServers

The `Get-VirtualizedServers` command returns information about virtualized servers.

Usage

The usage for the command is as follows:

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Get-VirtualizedServers` command:

Table 120: Get-VirtualizedServers command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User

Option	Description
	name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Example:

Lists all virtualized servers on the local Core:

```
>Get-VirtualizedServers
```

Get-Volumes

The `Get-Volumes` command returns information about volumes on a specified machine that is protected by the Core.

Usage

The usage for the command is as follows:

```
Get-Volumes -core [host name] -user [user name] -password [password]  -
protectedserver [server name or IP address]
```

Command Options

The following table describes the options available for the `Get-Volumes` command:

Table 121: Get-Volumes command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.

Example:

Lists all volumes on the specified machine:

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-AzureVirtualStandby

You can use the `New-AzureVirtualStandby` command to export a virtual machine (VM) to a Microsoft Azure cloud account as a virtual standby machine.

Usage

The usage for the command is as follows:

```
New-AzureVirtualStandby -core [host name] -user [user name for Core] -password
[password for Core] -protectedserver [name | IP address] -volumes [volume names |
all] -initialexport -cloudaccountname [cloud account name]      -storageaccountname
[storage account name]-containername [container name] -foldername [folder name] -
subscriptionid [Azure subscription ID]
```

Command Options

The following table describes the options available for the `New-AzureVirtualStandby` command:

Table 122: New-AzureVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points that you want to export.
`-volumes`	Optional. List of additional volume names to be exported. If you use the value `all` or use no value, then all volumes export. Values must be enclosed in double quotes and separated by a space. Do not use trailing slashes in volumes names; for example, use `"c:" "d:"`.
`-initialexport`	Optional. Include this option if you need to start an initial ad-hoc virtual machines export to configure the virtual standby.
`-cloudaccountname`	Optional. You can use this option if you do not specify the `-storageaccountname`. It is the display name for the cloud account previously registered on the Core.
`-storageaccountname`	Optional. You can use this option if you do not specify the `-cloudaccountname`. It is the name of the storage account in Azure Classic.
`-containername`	The name of the container in the Azure storage account (classic). The name must container between three and 63 characters (lowercase letters, numbers, and hyphens only), and start with a letter or a number. Every hyphen must be preceded and followed by a letter or number.
`-foldername`	Optional. The name of a folder inside of the Azure storage container. A folder name cannot contain any of the following characters: `\ / : * ? " < > |`.
`-subscriptionid`	The identifier of a previously added Azure subscription.

Example:

Create a new Azure virtual standby:

```
>New-AzureVirtualStandby -protectedserver Win2008R2 -storageaccountname exports3 -containername container1 -foldername Win2008R2 -subscriptionid 4db3a063-0d9c-42d8-a994-d5e5c4b82c0
```

New-Base

The `New-Base` command forces a new base image resulting in a data transfer for the current protected machine. When you force a base image, the transfer will start immediately or will be added to the queue. Only the data that has changed from a previous recovery point will be transferred. If there is no previous recovery point, all data on the protected volumes will be transferred.

Usage

The usage for the command is as follows:

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `New-Base` command:

Table 123: New-Base command options

Option	Description
`-?`	Display this help message.
`-all`	Base image for all agents.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Force for the current protected machine's name.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Force base image for all protected machines:

```
>New-Base -all
```

New-BootCD

This command lets you create a bare metal restore (BMR) boot CD without using the Rapid Recovery Core Console.

Usage

The usage for the command is as follows:

```
New-BootCD -core [host name] -user [user name] -password [password] -ip [IP address] -mask [mask] -defaultgateway [defaultgateway] -dnsserver [dnsserver] -vncpassword [vncpassword] -vncport [vncport] -isofilepath [destination for the boot image] -driverspath [drivers path]
```

Command Options

The following table describes the options available for the `New-BootCD` command:

Table 124: New-BootCD command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-ip`	Optional. This option specifies the IP address of the target BMR machine. By default, it generates automatically.
`-mask`	Optional. This option specifies the subnet mask of the target BMR machine. By default, it generates automatically.
`-defaultgateway`	Optional. This option specifies the default gateway of the target BMR machine. By default, it generates automatically.
`-dnsserver`	Optional. This option specifies the DNS server for the target BMR machine. By default, it generates automatically.
`-vncpassword`	Optional. This option specifies the user password for an existing UltraVNC account. By default, this option is empty.
`-vncport`	Optional. This option specifies the port to use for UltraVNC. You can change it only if you used the `-vncpassword` option. By default, the port is 5900.
`-isofilepath`	Optional. This option specifies the patch to the boot CD file. The default path is C:\ProgramData\AppRecovery\Boot CDs.
`-driverspath`	Optional. This option specifies the path to the archive of drivers.

Example:

Create a boot CD:

```
>New-BootCD -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -
dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

New-CloudAccount

The `New-CloudAccount` command lets you add a new cloud account to the Rapid Recovery Core.

Usage

The usage for the command is as follows:

```
New-CloudAccount -core [host name] -user [login] -password [password] -
displayname [display name] -type [cloud acco
      unt type] -username [user name] - key [secret key] -region [region] -
tenantid [tenant Id] -authurl [authorization
      url]
```

Command Options

The following table describes the options available for the `New-CloudAccount` command:

Table 125: New-CloudAccount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-displayname`	The name of the cloud account to display.
`-type`	The type of cloud account you want to add. Supported values include: • amazon • openstack • rackspace • windowsazure • "windows azure" • azure
`-username`	The user name for the cloud account that you want to add. It is used in the authentication process. This property resolves as "Access Key" for Amazon™ cloud, "User Name" for Rackspace and OpenStack, and "Storage Account Name" for Windows Azure cloud accounts.
`-key`	The key for the cloud account you want to add. It is used in the authentication process. This property resolves as "Secret Key" for Amazon™ cloud, "Api Key" for Rackspace and OpenStack, and "Access Key" for a Windows Azure cloud accounts.

Option	Description
-region	The region of the cloud account that you want to add. This property is required only for RackSpace and OpenStack cloud accounts.
-tenantid	The identifier that is used in the authentication process of an OpenStack cloud account. This option is required only for OpenStack cloud accounts.
-authurl	The URL that is used in the authentication process of an OpenStack cloud account. This option is required only for OpenStack cloud accounts.

Example:

Create a new Amazon™ S3 cloud account named "Amazon S3 Account" with the access key "akey" and the secret key "skey."

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey
-key skey
```

New-EncryptionKey

The `New-EncryptionKey` command lets you create a new encryption key for securing your Rapid Recovery backed up data.

Usage

The usage for the command is as follows:

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name
[encryption key name] -passphrase [pas
    sphrase] -comment [comment]
```

Command Options

The following table describes the options available for the `New-EncryptionKey` command:

Table 126: New-EncryptionKey command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-name	The name of the encryption key that you want to create.
-passphrase	The passphrase to the encryption key that you want to create.
-comment	Optional. The description of the encryption key.

Example:

Create an encryption key on the local Core:

```
>New-EncryptionKey –name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

The `New-EsxiVirtualStandby` PowerShell command lets you create a new ESXi virtual standby machine using Rapid Recovery.

Usage

The usage for the command is as follows:

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

Command Options

The following table describes the options available for the `New-EsxiVirtualStandby` command:

Table 127: New-EsxiVirtualStandby command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Show jobs for a specific protected machine, indicated by IP address.
-volumes	Optional. List the volume names you want to export. If not specified, all volumes in the recovery point(s) are exported. Values must be enclosed in double quotes and separated by space; for example, "c:", "d:". **Note:** Do not use trailing slashes in volume names.
-vmname	The Microsoft Windows name of the virtual machine.
-hostname	The name of the virtual server host.
-hostport	The port number to use for communicating with the virtual server.
-hostusername	The user name for logging in to the virtual server host.
-hostpassword	The password for logging in to the virtual server host.
-ram	Allocate a specific amount of RAM on the virtual server.
-usesourceram	Optional. Allocate the same amount of RAM on the virtual server that the source protected machine has.
-diskprovisioning	Optional. The amount of disk space to allocate on the virtual machine. Available values include: • Thick - Specify 'thick' to make the virtual disk as large as the original drive on the protected server. • Thin - Specify 'thin' to allocate the amount of actual disk space occupied on the original drive plus some additional megabytes. The default disk provisioning is 'thin'.
-diskmappinjg	Optional. It determines how to map the disks from the recovery point to the virtual machine. Available values include: • 'auto' • 'manual' • 'withvm' The default setting is 'auto'.
-initialexport	Optional. Specify this option if you need to start an initial on-demand virtual machine export after configuring the virtual standby.

Example:

Create a new ESXi virtual standby:

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -
hostname 10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -
usesourceram -diskprovisioning thin -diskmapping auto
```

New-FileSearch

The `New-FileSearch` command lets you search for a specific file among the recovery points in a repository, which helps you determine which recovery point you need to mount for a restore.

Usage

The usage for the command is as follows:

```
New-FileSearch -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -startdate [start date] -enddate [end date]
-filemasks [file masks] -paths [paths] -subdiroff -ntfsfastoff -limitsearch
[limit search]
```

Command Options

The following table describes the options available for the `New-FileSearch` command:

Table 128: New-FileSearch command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle archive log mode.
`-startdate`	The earliest date of a period within you want to conduct your search. Use the date pattern "MM/DD/YYYY HH:mm:ss AM."
`-enddate`	The latest date of a period within you want to conduct your search. Use the date pattern "MM/DD/YYYY HH:mm:ss AM."
`-filemasks`	A combination of fixed and wildcard characters to search for the file. It can be one string or an array of strings. All masks should be separated by a space; for example: `-filemasks "first" "second."`
`-paths`	Optional. If there are specific directories in which you want to search, use this option to list the paths. It can be one string or an array of strings. All directories should be separated by a space; for example: `-paths "E:\" "C:\Program Files."`
`-subdiroff`	Optional. By default, the file search is performed in subdirectories. Use this option if you want to turn this feature off and not search in subdirectories.
`-ntfsfastoff`	Optional. By default, the file search is performed using the NTFS fast algorithm. If you

Option	Description
	want to perform the search without this feature, specify this option.
`-limitsearch`	Optional. Use this option to limit the number of search results. The default value is 1000.

Examples:

Perform a file search with one file mask:

```
New-FileSearch -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.10 -filemasks "sample"
```

Perform a file search with multiple file masks in specified directories and without the NTFS fast algorithm:

```
New-FileSearch -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.10 -filemasks "sample" "second" -paths "C:\dir" -
ntfsfastoff
```

New-HyperVVirtualStandby

The `New-HyperVVirtualStandby` PowerShell command lets you create a new Hyper-V virtual machine (VM) using Rapid Recovery.

Usage

The usage for the command is as follows:

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -
protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-
uselocalmachine] | -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login]
-hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -
initialexport -exportvmconfigfiles
```

Command Options

The following table describes the options available for the `New-HyperVVirtualStandby` command:

Table 129: New-HyperVVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.

Option	Description
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Show jobs for a specific protected machine, indicated by IP address.
-volumes	Optional. List the volume names you want to export. If not specified, all volumes in the recovery point(s) are exported. Values must be enclosed in double quotes and separated by space; for example, "c:", "d:". **Note:** Do not use trailing slashes in volume names.
-vmname	The Microsoft Windows name of the virtual machine.
-gen2	Optional. Specify to use the second VM generation. If not specified, generation 1 is used. Rapid Recovery supports generation 2 from Windows Server 2012 R2 through Windows 8.1.
-usevhdx	Optional. If you specify this option, Rapid Recovery uses the VHDX disk format to create the VM. If you do not, it uses the VHD disk format. Generation 2 uses only the VHDX format.
-uselocalmachine	Optional. Connect to the local Hyper-V server. When you specify this value, Rapid Recovery ignores the following options: • hostname • hostport • hostusername • hostpassword
-hostname	The name of the virtual server host.
-hostport	The port number to use for communicating with the virtual server.
-hostusername	The user name for logging in to the virtual server host.
-hostpassword	The password for logging in to the virtual server host.
-vmlocation	Local or network path to the folder where you want to store the virtual machine files.
-ram	Allocate a specific amount of RAM on the virtual server.
-usesourceram	Optional. Allocate the same amount of RAM on the virtual server that the source protected machine has.
-initialexport	Optional. Specify this option if you need to start an initial on-demand virtual machine export after configuring the virtual standby.
-exportvmconfigfiles	Optional. Specify whether to export virtual machine configuration files. This option is available only both when the source is a virtual protected agentlessly and when the target hpyervisor is the same as the source hypervisor.

Example:

Create a new Hyper-V virtual standby machine:

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -
protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-
uselocalmachine] | -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login]
-hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -
initialexport
```

New-Mount

The `New-Mount` command mounts a snapshot of one or more drives.

Usage

The usage for the command is as follows:

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver
[machine name] -mounttype [read | write | readonlywithpreviouswrites] -drives
[drive names] -path [location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -
rpn [number]
```

Command Options

The following table describes the options available for the `New-Mount` command:

Table 130: New-Mount command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-protectedserver`	The protected server IP address or machine name (depends on how the particular machine was protected.
`-time`	Optional. The timestamp of the Recovery Point to mount. This should be in the format that is specified by the OS on the current PC. The administrator is able to get the latest recovery point by specifying latest or last checked recovery point by passed parameter value. By default the latest time option is chosen.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you

Option	Description
	also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-path`	Path on the Core machine to which recovery points will be mounted.
`-mounttype`	Optional. Specifies a mount mode. Available options are `'read'`, `'readOnlyWithPreviousWrites'` (read-only with previous writes), `'write'` (writable). Default mode is `read-only`.
`-volumes`	Optional. Space-separated list of volume names to mount. If the volume's name contains spaces or special characters, it has to be specified using double quotes. If not specified, all volumes will be mounted.
`-rpn`	Optional. Recovery point number for the mount. You can obtain this using the `get-mounts` command. Specify several numbers for the `rpn` parameter to mount different points with a single command. **Note:** If you set an array of points to mount, each point will be located in a separate child directory. The name describes the time when the recovery point was created. When you call dismount, all child directories will be removed. You should remove the parent directory manually.

Example:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c "d, ko"
```

Mount an array of recovery points:

```
>New-Mount –rpn 10 52 41 -protectedserver localhost –path "D:/Folder for mount"
```

Mount a recovery point with certain time created:

```
>New-Mount -protectedserver 10.10.5.56 –path "D:/Folder for mount" –time "8/24/2012 11:46 AM"
```

New-Replication

The `New-Replication` command lets you set up and force replication for a protected server or servers.

Usage

The usage for the command is as follows:

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `New-Replication` command:

Table 131: New-Replication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-replicationname`	Name of the replication configuration on the target Core.
`-targetserver`	The host name, user name, and password for the target Core.
`-protectedserver`	The name of the protected machine and repository on the target Core for setting up replication.

Example:

Create new replication for the protected machine with IP 10.10.10.4:
Pending examples from QA.

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

The `New-Repository` command creates a new DVM repository in the Rapid Recovery Core. The size specified must be between 250MB and 16TB.

Usage

The usage for the command is as follows:

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

Command Options

The following table describes the options available for the `New-Repository` command:

Table 132: New-Repository command options

Option	Description
`-?`	Display this help message.

Option	Description
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
-name	Repository name.
-size	Size of repository extent. Available units are: b, Kb, MB, GB, TB, PB.
-datapath	For local location only. Determines data path of repository extent.
-metadatapath	For local location only. Determines metadata path of repository extent.
-uncpath	For share location only. Determines data and metadata paths of repository extent.
-shareusername	For share location only. Determines login to share location.
-sharepassword	For share location only. Determines password to share location.
-comment	Optional. Description of repository.
-concurrent Operations	Optional. Maximum number of operations that can be pending at one time. Value by default: 64.

Example:

Create new DVM repository of minimum size in local drive E:

```
>New-Repository –name Repository2 -size 250Mb -datapath e:\Repository\Data -
metadatapath e:\Repository\Metadata
```

New-ScheduledArchive

The `New-ScheduledArchive` command lets you use PowerShell to make changes to an existing scheduled archive.

Usage

The usage for the command is as follows:

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address] -path [location] -archiveusername [name] -
archivepassword [password] -cloudaccountname [name] -cloudcontainer [name] -
recycleaction [type] -schdeuletype [type] -dayofweek [name] -dayofmonth [number] -
time [time] -archiveretention [months] -initialpause -useglacierfordatafiles
```

Command Options

The following table describes the options available for the `New-ScheduledArchive` command:

Table 133: New-ScheduledArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	The protected machine with recovery points that you want to archive. You can specify multiple machine names enclosed in double quotes and separated by commas.
`-all`	Archive recovery points for all protected machines.
`-path`	The path to where to save the archived data. For example: • Local machine: "d:\work\archive" • Network path: "\\servername\sharename" • Folder in a cloud account: "Folder Name" **Note:** The number of symbols should not be greater than 100 for local and network locations, and should not be greater than 150 for a cloud location.
`-archiveusername`	Optional. The user name for logging in to the remote machine. It is required for a network path only.
`-archivepassword`	Optional. The password for logging in to the remote machine. It is required for a network path only.
`-cloudaccountname`	Optional. Use only for cloud archiving. The name of the cloud account where you want to save the archive.
`-cloudcontainer`	Optional. Use only for cloud archiving. The name of the cloud container in the chosen cloud account, where the archive will be saved. When you use this option, you should also specify the "-cloudaccountname" parameter.
`-recycleaction`	The type of recycle action. Specified by using one of the following four values: • "replacethiscore" - Overwrites any pre-existing archived data pertaining to this Core, but leaves the data for other Cores intact.

Option	Description
	• "erasecompletely" - Clears all archived data from the directory before writing the new archive. • "incremental" - Lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.
-scheduletype	Type of schedule interval. Specified the option with one of the following four values: • "daily" - For a daily automatically created archive. • "weekly" - For a weekly automatically created archive. You must specify the "-dayofweek" parameter. • "monthly" - For a monthly automatically created archive. You must specify the "-dayofmonth" parameter. If a month does not have the day specified—for example, "31"—then the archive will not occur for that month. • "lastdayofmonth" - For automatically creating an archive on the last day of each month.
-dayofweek	Use only for the "weekly" option of the "-scheduletype" parameter. The day of the week on which to automatically create the archive (for example, "Monday").
-dayofmonth	Use only for the "month" option of the "-scheduletype" parameter. The day (number) of the month on which to automatically create the archive (for example, "15").
-time	The hour of the day when you want to create an archive.
-initialpause	Optional. Specify this option if you want to initially pause archiving after you configure the archiving schedule.
-useglacierfordatafiles	Only for cloud archiving to Amazon. Use Glacier for data files.
-archiveretention	Optional. Specifies the number of months to retain archived recovery points. Archived recovery points older than the specified number of months will be automatically removed.

Examples:

Archive all recovery points with creation dates starting from 04/30/2012 02:55 PM for all machines on the Core, and replace pre-existing archived data pertaining to this Core:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
path "d:\work\archive" -s
    tartdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

Archive recovery points that fall within a date range for two protected machines, and clear all archived data from the directory before writing the new archive:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate
"04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

Create an incremental archive for all recovery points with creation dates starting from 04/30/2012 02:55 PM for all machines on the Core to the cloud account with the name "Amazon S3" and a container named "Container":

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
path "ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -
startdate "04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

The `New-Snapshot` command forces a snapshot resulting in a data transfer for the current protected machine. When you force a snapshot, the transfer will start immediately or will be added to the queue. Only the data that has changed from a previous recovery point will be transferred. If there is no previous recovery point, all data on the protected volumes will be transferred.

Usage

The usage for the command is as follows:

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user
name] -password [password]
```

Command Options

The following table describes the options available for the `New-Snapshot` command:

Table 134: New-Snapshot command options

Option	Description
`-?`	Display this help message.
`-all`	Force all protected machines.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Force for the current protected machine's name.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Force a snapshot for all protected machines:

```
>New-Snapshot -all
```

New-VBVirtualStandby

The `New-VBVirtualStandby` command lets you use PowerShell to create a new virtual export to a VirtualBox virtual machine (VM).

Usage

The usage for the command is as follows:

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -
protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual
machine name] [-ram [total megabytes] | -usesourceram]  -linuxhostname [linux
hostname] -hostport [linux port] -targetpath [location] -pathusername [login] -
pathpassword [password] -initialexport
```

Command Options

The following table describes the options available for the `New-VBVirtualStandby` command:

Table 135: New-VBVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-volumes`	Optional. List the volume names you want to export. If not specified, all volumes in the recovery point(s) are exported. Values must be enclosed in double quotes and separated by space; for example, "c:", "d:". **Note:** Do not use trailing slashes in volume names.
`-vmname`	The Microsoft Windows name of the virtual machine.
`-ram`	Allocate a specific amount of RAM on the virtual server.

Option	Description
-usesourceram	Optional. Allocate the same amount of RAM on the virtual server that the source protected machine has.
-linuxhostname	The Linux VirtualBox server host name.
-hostport	The Linux VirtualBox server port.
-targetpath	The local, network, or Linux path to the folder where you want to store the virtual machine files.
-pathusername	The user name for logging in to the network machine. It is only required when you specify a network location for the target path.
-pathpassword	The password for logging in to the network machine. It is only required when you specify a network location for the target path.
-accountusername	Optional. You can specify a user account with which to register the exported virtual machine. It is the user name for logging in to the user account. Use this option for a local or network machine only.
-accountpassword	Optional. You can specify a user account with which to register the exported virtual machine. It is the password for logging in to the user account. Use this option for a local or network machine only.
-initialexport	Optional. Specify this option if you need to start an initial on-demand virtual machine export after configuring the virtual standby.

Example:

Create a VirtualBox virtual standby machine named ExportedMachine1 in a specified location:
Pending example from QA.

```
>New-VBVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname
ExportedMachine1 -usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

The `New-VMVirtualStandby` PowerShell command lets you create a new VMware Workstation virtual standby machine using Rapid Recovery.

Usage

The usage for the command is as follows:

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -
protectedserver [name | IP address] -volumes [volumes names] -vmname [virtual
machine name] [-ram [total megabytes] | -usesourceram] -targetpath [location] -
pathusername [login] -pathpassword [password] -initialexport
```

Command Options

The following table describes the options available for the `New-VMVirtualStandby` command:

Table 136: New-VMVirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Show jobs for a specific protected machine, indicated by IP address.
`-volumes`	Optional. List the volume names you want to export. If not specified, all volumes in the recovery point(s) are exported. Values must be enclosed in double quotes and separated by space; for example, "c:", "d:". **Note:** Do not use trailing slashes in volume names.
`-vmname`	The Microsoft Windows name of the virtual machine.
`-ram`	Allocate a specific amount of RAM on the virtual server.
`-usesourceram`	Optional. Allocate the same amount of RAM on the virtual server that the source protected machine has.
`-pathusername`	The user name for logging in to the network machine. It is only required when you specify a network location for the target path.
`-pathpassword`	The password for logging in to the network machine. It is only required when you specify a network location for the target path.
`-initialexport`	Optional. Specify this option if you need to start an initial on-demand virtual machine export after configuring the virtual standby.

Example:

Create a new VMware Workstation virtual standby:

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname
ExportedMachine1 -usesourceram -targetpath I:\VMExport
```

Script pauses, requiring user to specify an index number for the appropriate workstation. Enter the index number for the script to complete (in this case, 2). Example continues:

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

The `Push-Replication` command forces replication for one or more protected machines.

Usage

The usage for the command is as follows:

```
Push-Replication -core [host name] -user [user name] -password [password] -
targetcore [host name] -all | -protectedserver [machine name | IP address]
```

Command Options

The following table describes the options available for the `Push-Replication` command:

Table 137: Push-Replication command options

Option	Description
`-?`	Display this help message.
`-all`	Force replication for all machines being replicated to the target Core.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Protected machine name on the target Core against which to force replication.
`-user`	Optional. Login for the remote Core host machine. If you specify a login, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Push replication for a single protected machine:

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
  -targetcore 10.10.10.20:8006 –protectedserver 10.10.5.22
```

Push replication for all protected machines:

```
>Push-Replication -all
```

Push-Rollup

The `Push-Rollup` command forces rollup for a protected machine.

Usage

The usage for the command is as follows:

```
Push-Rollup -core [host name] -user [user name] -password [password] -
protectedserver [machine name | IP address]
```

Command Options

The following table describes the options available for the `Push-Rollup` command:

Table 138: Push-Rollup command options

Option	Description
`-?`	Display this help message.
`-all`	Force all protected machines.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Force for the current protected machine's name.
`-user`	Optional. Login for the remote Core host machine. If you specify a login, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Push rollup for a single protected machine:

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Push rollup for all protected machines:

```
>Push-Rollup -all
```

Remove-Agent

The `Remove-Agent` PowerShell command lets you remove a machine from Rapid Recovery Core protection.

Usage

The usage for the command is as follows:

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -deleterecoverypoints -all
```

Command Options

The following table describes the options available for the `Remove-MountAgent` command:

Table 139: Remove-Agent command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Dismount all mounted recovery points for the current protected machine.
`-deleterecoverypoints`	Optional. Delete all recovery points for this protected machine.
`-all`	Optional. Delete all protected machines from the Core.

Example:

Dismount all protected machines and their recovery points:

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
deleterecoverypoints -all
```

Remove-EsxAutoProtectObjects

The `Remove-EsxAutoProtectObjects` cmdlet lets you remove specific objects on vCenter or ESXi server from protection by a Core.

Usage

The usage for the command is as follows:

```
Remove-EsxAutoProtectObjects -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -autoprotectobjects
```

Command Options

The following table describes the options available for the `Remove-EsxAutoProtectObjects` command:

Table 140: Remove-ESXAutoProtectObjects command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number).

Option	Description
	By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Use this option to edit the vCenter or ESXi objects for a specific protected machine.
`-autoprotectobjects`	A list of vCenter or ESXi objects each enclosed in double quotes and separated by a comma.

Example:

Remove specific vCenter or ESXi objects from protection auto-protection by the Core:

```
>Remove-EsxAutoProtectObjects -protectedserver 10.10.8.150 -autoprotectobjects
"vm1", "vm2"
```

Remove-HyperVClusterSharedVirtualDisks

The `Remove-HyperVClusterSharedVirtualDisks` cmdlet lets you remove shared Hyper-V virtual disks from protection of a Core.

Usage

The usage for the command is as follows:

```
Remove-HyperVClusterSharedVirtualDisks -core [host name] -user [user name] -password
[password] -shareddisks [shared virtual disks name or path collection | all]
```

Command Options

The following table describes the options available for the `Remove-HyperVClusterSharedVirtualDisks` command:

Table 141: Remove-HyperVClusterSharedVirtualDisks command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.

Option	Description
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Use this option to edit the shared virtual disks for a specific protected machine.
-shareddisks	A list of shared disks each separate by a comma.

Example:

Remove one shared virtual disk from protection:

```
>Remove-HyprVClusterSharedVirtualDisks -protectedserver "HV-2012R2" -shareddisks
"Shared Disk 1"
```

Remove-HyperVClusterVirtualMachines

The `Remove-HyperVClusterVirtualMachines` cmdlet lets you remove specific virtual machines (VMs) of a Hyper-V cluster from protection of a Core.

Usage

The usage for the command is as follows:

```
Remove-HyperVClusterVirtualMachines -core [host name] -user [user name] -password
[password] -repository [name] -protectedserver [name | IP address] -virtualmachines
[virtual machines collection | all]
```

Command Options

The following table describes the options available for the `Remove-HyperVClusterVirtualMachines` command:

Table 142: Remove-HyperVClusterVirtualMachines command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Use this option to protect virtual machines.
-virtualmachines	A list of the virtual machines that you want to protect, each separated by a comma. The name of the VM must be enclosed in double quotes.
-deleterecoverypoints	Optional. Include this option if you want to delete all of the recovery points for this VM.

Example:

Remove specific virtual machines of a Hyper-V cluster from protection by the Core and delete its recovery points:

```
>Remove-HyperVClusterVirtualMachines -protectedserver hvcluster -virtualmachines
"Win8x64-gen1", "Win2012x64-gen2" -deleterecoverypoints
```

Remove-HyperVVirtualMachines

The `Remove-HyperVVirtualMachines` cmdlet lets you remove specific Hyper-V virtual machines (VMs) from the protection of a Core.

Usage

The usage for the command is as follows:

```
Remove-HyperVVirtualMachines -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -virtualmachines [virtual machines
collection | all] -deleterecoverypoints
```

Command Options

The following table describes the options available for the `Remove-HyperVVirtualMachines` command:

Table 143: Remove-HyperVVirtualMachines command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Use this option to edit Hyper-V objects for a specific virtual machine.
-virtualmachines	A list of the virtual machines that you want to protect, each separated by a comma. The name of the VM must be enclosed in double quotes.
-deleterecoverypoints	Optional. Include this option if you want to delete all of the recovery points for this VM.

Example:

Remove specific Hyper-V VMs from protection and delete its recovery points:

```
>Remove-HyperVVirtualMachines -protectedserver HVServer1 -virtualmachines "Win8x64-gen1", "Win2012x64-gen2" -deleterecoverypoints
```

Remove-Mount

The Remove-Mount command dismounts a mounted recovery point specified by the /Path. Dismount points for the selected machine using the -protectedserver parameter or dismount points for all the mounted recovery points by using the -all parameter.

Usage

The usage for the command is as follows:

```
Remove-Mount -core [host name] -user [user name] -password [password] [-protectedserver [machine name] | -path [mount path]]
```

Command Options

The following table describes the options available for the Remove-Mount command:

Table 144: Remove-Mount command options

Option	Description
-?	Display this help message.
-all	Dismount all mounted recovery points.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on.

Option	Description
	If none are provided, then the logged-on user's credentials will be used.
`-path`	Dismount selected mount point.
`-protectedserver`	Dismount all mounted recovery points for the current protected machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Dismount the recovery point specified by the path:

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -path
C:\mountedRecoveryPoint
```

Remove-Mounts

The `Remove-Mounts` command dismounts all mounted recovery points.

Usage

The usage for the command is as follows:

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Remove-Mounts` command:

Table 145: Remove-Mounts command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Dismount all recovery points on the specified Core:

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Remove-RecoveryPoints

The `Remove-RecoveryPoints` PowerShell command lets you delete recovery points for a specific machine.

Usage

The usage for the command is as follows:

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range |
chain | all] -protectedserver
    [name | IP address] -rpn [number | numbers] | -time [time string | time interval
specified by two time strings]
```

Command Options

The following table describes the options available for the `Remove-RecoveryPoints` command:

Table 146: Remove-RecoveryPoints command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Dismount all mounted recovery points for the current protected machine.
`-rpn`	Optional. Only for chain deletion (base image with chain of incrementals or orphaned points). The sequential number of a recovery point to be deleted (use the Get-RecoveryPoints command to obtain the numbers). You can specify several space-separated numbers to delete multiple recovery points with a single command.
`-time`	Use this option to delete a chain of recovery points. Optional. To delete a single recovery point, select the recovery point by its creation time. Specify the exact time in the format "mm/dd/yyyy hh:mm tt" (for example, "2/24/2012 09:00 AM"). Keep in mind to specify date and time values of the time zone set on your computer.

Option	Description
	Required. For a date range, specify a time interval using two time strings separated by coma and space to select the range of recovery points to delete.
`-range`	Optional. The range of recovery points to delete by time interval.
`-chain`	Optional. A base image with sequential incrementals or a sequential set of orphaned points to delete selected by recovery point number or time of recovery point creation.
`-all`	Optional. Delete all protected machines from the Core.

Example:

Delete the recovery point specified by the date:

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd -time "2/24/2012 09:00 AM"
```

Remove-RemoteMount

The `Remove-RemoteMount` command dismounts a remotely mounted recovery point.

Usage

The usage for the command is as follows:

```
Remove-RemoteMount -core [host name] -user [user name] -password [password] [-
protectedserver [machine name] | -path [mount path]]
```

Command Options

The following table describes the options available for the `Remove-RemoteMount` command:

Table 147: Remove-Mount command options

Option	Description
`-?`	Display this help message.
`-all`	Dismount all mounted recovery points.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-path`	Dismount selected mount point.

Option	Description
-protectedserver	Dismount all mounted recovery points for the current protected machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Examples:

Dismount the remotely mounted recovery point by a specified path:

```
>Remove-RemoteMount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-path C:\mountedRecoveryPoint
```

Dismount all remotely mounted recovery points for a specified protected server:

```
>Remove-RemoteMount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "11.11.11.11"
```

Remove-RemoteMounts

The `Remove-RemoteMounts` command dismounts all remotely mounted recovery points.

Usage

The usage for the command is as follows:

```
Remove-RemoteMounts -core [host name] -user [user name] -password [password]
```

Command Options

The following table describes the options available for the `Remove-RemoteMounts` command:

Table 148: Remove-RemoteMounts command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.

Example:

Dismount all remotely mounted recovery points:

```
>Remove-RemoteMounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Remove-Replication

This command lets you remove a replication configuration from a source Core or target Core, as well as remove replicated recovery points.

Usage

The usage for the command is as follows:

```
Remove-Replication -core [host name] -user [user name] -password [password] -
incoming [host name] -outgoing [host name] -deletepoints
```

Command Options

The following table describes the options available for the `Remove-Replication` command:

Table 149: Remove-Replication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-incoming`	The identifier (ID) of the incoming replication that should be deleted. It could be a remote Core ID or a host name. Use the word "all" to delete all replications. **Note:** You can specify different protected machines for different replications by using the following pattern: `Replication1:Agent1,Agent2;Replication2:Agent2,Agent3`. If you do not specify a machine after the colon (:), the replication is deleted for all replicated machines.
`-outgoing`	The identifier (ID) of the outgoing replication that should be deleted. It could be a remote Core ID or a host name. Use the word "all" to delete all replications. **Note:** You can specify different protected machines for different replications by using the following pattern: `Replication1:Agent1,Agent2;Replication2:Agent2,Agent3`. If you do not specify a machine after the colon (:), the replication is deleted for all replicated machines.

Option	Description
-deletepoints	Specify which recovery points, if any, of the replicated machine that you want to remove.

Example:

Delete all incoming and all outgoing replications:

```
>Remove-Replication -incoming all -outgoing all
```

Delete two outgoing replications with all machines:

```
>Remove-Replication -outgoing TargetCore1;TargetCore2
```

Delete one protected machine from incoming replication and delete recovery points:

```
>Remove-Replication -incoming TargetCore1:10.10.10.10 -deletepoints
```

Remove-Repository

The `Remove-Repository` PowerShell command deletes a Rapid Recovery repository and its contents from the Core.

Usage

The usage for the command is as follows:

```
Remove-Repository -core [host name] -user [login] -password [password] -name
[repository name] -all
```

Command Options

The following table describes the options available for the `Remove-Repository` command:

Table 150: Remove-Repository command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-name	The name of the repository that you want to delete.
-all	Delete all repositories associated with this Core.

Example:

Remove all repositories on the local Core:

```
>Remove-repository -all
```

Remove-ScheduledArchive

If you scheduled Rapid Recovery to regularly archive recovery points for a specific machine, you can use the `Remove-ScheduledArchive` PowerShell command to remove that scheduled archive from the Core.

Usage

The usage for the command is as follows:

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `Remove-ScheduledArchive` command:

Table 151: Remove-ScheduledArchive command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
-all	Remove all archives associated with this Core.
-id	The identifier of the archive that you want to remove. To list more than one archive, separate each ID with a space.

Example:

Remove several scheduled archives from the local Core:

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-
47f5-b5a8-dffc49f50e25
```

Remove-VirtualStandby

If you scheduled Rapid Recovery to continuously export data to a virtual machine, then you can use the `Remove-VirtualStandby` PowerShell command to cancel and delete this scheduled job.

Usage

The usage for the command is as follows:

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP ad
    dress]
```

Command Options

The following table describes the options available for the `Remove-VirtualStandby` command:

Table 152: Remove-VirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Remove all virtual standby jobs associated with this Core.
`-protectedserver`	The name or IP address for the protected machine for which you want to remove virtual standby.

Example:

Remove all virtual standby jobs associated with this Core:

```
>Remove-VirtualStandby -all
```

Restart-CoreService

If the Core service on the Core machine is stopped, use the `Restart-CoreService` command to start it again.

Usage

The usage for the command is as follows:

```
Restart-CoreService -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false] -wait [time in seconds]
```

Command Options

The following table describes the options available for the `Restart-CoreService` command:

Table 153: Restart-CoreService command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."
`-wait`	Optional. This option indicates that the command should wait until the Core service is fully restarted for the specified period of time in seconds before canceling active jobs.

Example:

Restart the Core service:

```
>Restart-CoreService -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true -wait 600
```

Resume-Replication

The `Resume-Replication` command lets you resume replication. See Suspend-Replication for more details.

Usage

The usage for the command is as follows:

```
Resume-Replication -core [host name] -user [user name] -password [password] -all
| -protectedserver [machine name | IP address] -incoming [host name] | -
outgoing [host name]
```

Command Options

The following table describes the options available for the `Resume-Replication` command:

Table 154: Resume-Replication command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-all`	All protected servers.
`-protectedserver`	Resume replication for the specified machine.
`-incoming`	Host name of the remote Core that replicates to the Core machine. Replication is resumed for all protected machines on the remote Core.
`-outgoing`	Host name of the remote target core to which data is replicating. Replication is resumed for all protected machines on the remote core.

Example:

Resume replication for the protected machine with IP 10.10.10.128 for the local Core, specifying the repository being used:

```
>Resume-Replication replicationname Replication1 -targetserver
10.10.10.128,Administrator,123asdQ -protectedserver 10.10.10.4

# Repository
- ----------

1 Repository A
2 Repository B
Please, input number of Repository from the list above or type 'exit' to exit:
```

Script pauses, requiring user to specify an index number for the appropriate repository. Enter the index number for the script to complete (in this case, 2). Example continues:

```
2
Replication job was started.
```

```
True
PS C:\Users\Administrator>
```

Resume-ScheduledArchive

The `Resume-ScheduledArchive` command lets you resume a scheduled archive that had been paused or stopped.

Usage

The usage for the command is as follows:

```
Resume-ScheduledArchive -core [host name] -user [user name] -password [password] -
all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `Resume-ScheduledArchive` command:

Table 155: Resume-ScheduledArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Use this option to force all scheduled archives.
`-ids`	The identifier (ID) or IDs separated by spaces of the scheduled archives that you want to force.

Examples:

Resume all scheduled archives:

```
>Resume-ScheduledArchive -all
```

Resume one scheduled archive:

```
>Resume-ScheduledArchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

Resume multiple scheduled archives:

```
>Resume-ScheduledArchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Resume-Snapshot

An administrator is able to resume snapshots, export to virtual machines, and perform replication. See Start-VMExport for more details.

Usage

The usage for the command is as follows:

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Resume-Snapshot` command:

Table 156: Resume-Snapshot command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-all`	All protected servers.
`-protectedserver`	Resume snapshot for the specified machine.

Example:

Resume snapshots for the protected machine with IP 10.10.10.4 for the local Core:

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

The `Resume-VirtualStandby` PowerShell command lets you resume the suspended export of data to a Rapid Recovery virtual standby machine.

Usage

The usage for the command is as follows:

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Command Options

The following table describes the options available for the `Resume-VirtualStandby` command:

Table 157: Resume-VirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Resume exports for all virtual standby machines.
`-protectedserver`	The name or names—separated by a comma and space—of the protected machines with virtual standby machines that you want to resume.

Example:

Resume virtual standby exports for a protected machine:

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22
```

Set-AgentMetadataCredentials

The `Set-AgentMetadataCredentials` command sets the metadata credentials for a specified protected machine.

Usage

The usage for the command is as follows:

```
Set-AgentMetadataCredentials -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -target [default | SQL | Exchange] -
```

```
metadatausername [user name] -metadatapassword [password] -sqlinstancename [SQL
instance name] -usewindowsauthentication
```

Command Options

The following table describes the options available for the `Set-AgentMetadataCredentials` command:

Table 158: Set-AgentMetadataCredentials command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.
`-target`	Optional. The type of metadata, such as SQL, Exchange, or default.
`-metadatausername`	Optional. The metadata-related login.
`-metadatapassword`	Optional. The metadata-related password.
`-sqlinstancename`	Optional. The specific SQL instance name. Use this option in conjunction with the `-target` "sql."
`-usewindowsauthentication`	Optional. Use this option if your SQL credentials are also used for Windows authentication.

Example:

Set credentials for Exchange metadata:

```
>Set-AgentMetadataCredentials -core 10.10.10.10 -user administrator -password -
23WE@#$sdd -protectedserver 10.10.20.20 -target exchange -metadatausername
administrator -metadatapassword 123#
```

Set-DedupCacheConfiguration

This command lets you used the Command Line Utility to set the location, size, and metadata location for the primary and secondary cache of a DVM repository.

Usage

The usage for the command when creating a DVM repository is as follows:

```
Set-DedupCacheConfiguration -core [host name] -user [user name] -password [password]
-primary [cache location] -secondary [cache location] -metadata [metadata location]
-size [cache size] -restoredefault
```

Command Options

The following table describes the options available for the `Set-DedupCacheConfiguration` command:

Table 159: Set-DedupCacheConfiguration command options

Option	Description
`-?`	Display help on the command.
`-core`	Optional. Remote core host machine IP address (with an optional port number). By default, the connection is made to the core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-primary`	Optional. Primary cache location.
`-secondary`	Optional. Secondary cache location.
`-metadata`	Optional. Metadata cache location.
`-size`	Optional. Deduplication cache size in GB.
`-restoredefault`	Optional. Restore to default deduplication cache configuration. If this parameter is specified, all other parameters are ignored.

Examples:

Set primary deduplication cache location and deduplication cache size:

```
>Set-DedupCacheConfiguration -primary D:\primary -size 6
```

Set secondary and metadata deduplication location:

```
>Set-DedupCacheConfiguration -secondary D:\secondary -metadata D:\metadata
```

Restore default deduplication configuration:

```
>Set-DedupCacheConfiguration -restoredefault
```

Set-License

There may be times when you need to change the Rapid Recovery license applied to a machine, such as when moving from a trial license to a subscription or perpetual license. In such instances, you can change the license in the Command Prompt by using the `Set-License` command.

Usage

The usage for the command is as follows:

```
Set-License -core [host name] -user [user name] -password [password] -licensekey [license key] -licensepath [license file path] -licensenumber [license number] -email [email address]
```

Command Options

The following table describes the options available for the `Set-License` command:

Table 160: Set-License command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-licensekey`	Optional. A 30-character key comprising six groups of five alphanumeric characters, each separate by a hyphen. Use this key when a license file is not available.
`-licensepath`	Optional. The path to the file that ends with the .lic extension. If a license file is available, you can use this option instead of the `-licensekey`.
`-licensenumber`	Optional. You may have received this nine-digit license number in an order confirmation email. If you provide this number, use the email address that received it for verification.
`-email`	Optional. If you use the `-licensenumber`, you must include the email address that received it for verification.

Examples:

Change the license key associated with this Core to JL09F-89FSD-6THFS-DSE34-KS3D5-65DF2:

```
>Set-License -core 10.10.10.10 -user admin -password 676df#df -licensekey JL09F-89FSD-6THFS-DSE34-KS3D5-65DF2
```

Change the license key associated with this Core to the key contained in the license file:

```
>Set-License -core 10.10.10.10 -user admin -password 676df#df -licensepath C:\MyLicenseFile.lic
```

Change the license number associated with this Core to 111-111-111 using john.doe@example.com to verify the license:

```
>Set-License -core 10.10.10.10 -user admin -password 676df#df -licensenumber 111-111-111 -email john.doe@example.com
```

Set-OracleMetadataCredentials

The `Set-OracleMetadataCredentials` command lets you set the metadata credentials for a specified Oracle instance.

Usage

The usage for the command is as follows:

```
Set-OracleMetadataCredentials -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -instancename [Oracle instance SID] -connectiontype [-basic | TNS] -hostname [host name | IP address] -port [port number] [-usesid] -instanceservicename [service name] -tnsnetworkalias [TNS alias] [-usewindowsauthentication] -oracleusername [user name] -oraclepassword [password] [-edit]
```

Command Options

The following table describes the options available for the `Set-OracleMetadataCredentials` command:

Table 161: Set-OracleMetadataCredentialscommand options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the protected machine.
`-instancename`	The Oracle SID from which you want to fetch metadata.
`-connectiontype`	Use this option to identify the connection type. It must be represented by either `basic` or `TNS`.
`-hostname`	Optional. The name of the Oracle host. Use it for the `basic` connection type.
`-port`	Optional. A port number. Use it for the `basic` connection type.
`-usesid`	Optional. This option uses the `-instancename` to identify the Oracle

Option	Description
	instance. Use it for the `basic` connection type.
`-instanceservicename`	Optional. The Oracle instance service name. Use it when the `-usesid` is not specified and for the `basic` connection type.
`-tnsnetworkalias`	Optional. Use this option to identify the TNS network alias when using the `TNS` connection type.
`-usewindowsauthentication`	Optional. This option lets you authenticate with your Windows credentials.
`-oracleusername`	Optional. The user name for the Oracle instance.
`-oraclepassword`	Optional. The password for the Oracle instance.
`-edit`	Optional. This option lets you omit any number of options.

Examples:

Set the metadata credentials for the ORCL instance on a protected server using the `basic` connection type:

```
>Set-OracleMetadataCredentials -core 10.10.127.42 -user admin -password -676df#df -
protectedserver 10.10.34.88 -instancename ORCL -connectiontype basic -hostname
localhost -port 1521 -usesid -oracleusername User-ORA -oraclepassword 676df#df
```

Set the metadata credentials for the ORCL instance on a protected server using the `TNS` connection type and Windows authentication:

```
>Set-OracleMetadataCredentials -core 10.10.127.42 -user admin -password -676df#df -
protectedserver 10.10.34.88 -instancename ORCL -connectiontype TNS -tnsnetworkalias
ORCL_ALIAS -usewindowsauthentication
```

Start-Archive

Businesses often use long-term storage to archive both compliant and non-compliant data. The archive feature in Rapid Recovery is used to support the extended retention for compliant and non-compliant data. The administrator can save an archive on the local storage or network location by specifying the `/Path` command and credentials.

Usage

The usage for the command is as follows:

```
Start-Archive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP
address2]"] -path [location] -startdate [time string] -enddate [time string] -
archiveusername [name] -archivepassword [password] -comment [text]  -
cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -legalhold -
retentionmode [mode] -retain [days] -usecompatibleformat -useglacierfordatafiles
```

Command Options

The following table describes the options available for the `Start-Archive` command:

Table 162: Start-Archive command options

Option	Description
`-?`	Displays this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-all`	Archive all recovery points for all protected machines on the Core.
`-protectedserver`	Protected machine with recovery points to be archived. You can specify several machine names enclosed in double quotes and separated by spaces.
`-path`	Path where archived data should be placed; for example: d:\work\archive or network path \\servername\sharename.
`-startdate`	Start date for selecting recovery points by creation date. The value must be enclosed in double quotes; for example, `04/30/2012 02:55 PM`.
`-enddate`	Optional. End date for

Option	Description
	selecting recovery points by creation date. Value must be enclosed in double quotes; for example, `05/31/2012 11:00 AM`. The current time system is used by default.
`-archiveusername`	Optional. User name for the remote machine. Required for network path only.
`-archivepassword`	Optional. Password to the remote machine. Required for network path only.
`-comment`	Optional. Comment text must be enclosed in double quotes; for example: `-comment "comment goes here..."`.
`-usecompatibleformat`	Not supported for scheduled archives. The new format has improved performance, but it is not compatible with Cores older than release 6.2. Use this flag to create an archive that can be used with the old format.
`-cloudaccountname`	Optional. The name of the cloud account to which you want to save the archive.
`-cloudcontainer`	Optional. The name of the cloud container in the specified cloud account to which you want to save the archive.
`-recycleaction`	Specifies one of the following recycle action types: • `donotreuse` - This type is not supported for scheduled archive. It does not overwrite or clear any existing archived data from the location. If the location is not empty, the archive write fails.

Option	Description
	• `replacethiscore` - This type overwrites any pre-existing archived data that pertains to this Core, but leaves the data for other Cores intact. • `erasecompletely` - This type clears all archived data from the directory before writing the new archive. • `incremental` - This type lets you add recovery points to an existing archive. It compares recovery points to avoid duplicating data that already exists in the archive.
`-initialpause`	Optional. Specify whether you want to initially pause the archive job when you create it.
`-useglacierfordatafiles`	Optional. Only when archiving to an Amazon cloud. Specify this option if you want to use Amazon Glacier for archiving data files.
`-legalhold`	Optional. Supported only for Amazon S3 and S3-compatible cloud storage. Provides the same protection as a retention period, but it has no expiration date. Instead, a legal hold remains in place until you explicitly remove it. Legal holds are independent from retention periods.
`-retentionmode`	Optional. Supported only for Amazon S3 and S3-compatible cloud storage. Retention period and retention mode are always configured in tandem, unlike legal holds, which are configured independently. S3 Object Lock provides two retention

Option	Description
	modes that apply different levels of protection to your archives: • governance mode - In governance mode, users can't overwrite or delete an object version or alter its lock settings unless they have special permissions. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. • compliance mode - In compliance mode, a protected object version can't be overwritten or deleted by any user, including the root user in your AWS account. When an object is locked in compliance mode, you cannot change the retention mode, and you cannot shorten the retention period. Compliance mode helps ensure that an object version can't be overwritten or deleted for the duration of the retention period.
`-retain`	Optional. Supported only for Amazon S3 and S3-compatible cloud storage. Specifies a fixed period of time during which an object remains locked. During this period, your object is WORM-protected and can't be overwritten or deleted.

Option	Description
`-vaultelegalhold`	Optional. Supported only for Amazon Glacier! "Legal hold" vault locking mode. Provides the same protection as a retention period, but it has no expiration date.
`-vaultretain`	Optional. Supported only for Amazon Glacier! Specifies a fixed period of time during which an vault remains locked. During this period, your vault is WORM-protected and can't be overwritten or deleted.

Example:

Example 1 : Start archive of a particular protected machine to local target:

```
>Start-Archive -user administrator -password qwerty123 -protectedserver 10.23.20.186
-path E:\Archives\W7AGENT -startdate "6/12/2015 12:00:00 AM" -enddate "6/13/2015
12:00:00 AM" -recycleaction "incremental"
```

Example 2 - Start archive of a particular protected machine to network target:

```
>Start-Archive -user administrator -password qwerty123 -protectedserver 10.23.20.186
-path \\10.23.20.137\share -archiveusername administrator -archivepassword 321ytrewq
-startdate "6/12/2015 12:00:00 AM" -enddate "6/13/2015 12:00:00 AM" -recycleaction
"incremental"
```

Example 3 - Start archive of a particular protected machine to cloud target (Note: Configured cloud account is required):

```
>Start-Archive -user administrator -password qwerty123 -protectedserver 10.23.20.186
-path W7AGENT -cloudaccountname "Cloud Account 1" -cloudcontainer Archive -startdate
"6/12/2015 12:00:00 AM" -enddate "6/13/2015 12:00:00 AM" -recycleaction
"incremental"
```

Example 4 - Start archive all recovery points to Amazon S3 cloud storage with creation dates starting from 12/31/2023 12:00:00 PM for specified machine on the core, set object lock mode "Legal hold" and retention mode "Governance" with retain period of 5 days:

```
>Start-Archive -protectedserver localhost -cloudaccountname "storage account name" -
cloudcontainer "bucket-01" -path "Archive-0000001" -startdate "12/31/2023 12:00:00
PM" -recycleaction donotreuse -legalhold -retentionmode governance -retain 5
```

Set-ReplicationResponse

Use the `Set-ReplicationResponse` command to manage pending replication requests.

Usage

The usage for the command is as follows:

```
Set-ReplicationResponse -core [host name] -user [user name] -password [password] -id
[replication ID] -accept | -deny | -ignore -protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Set-ReplicationResponse` command:

Table 163: Set-ReplicationResponse command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used
`-id`	The identifier for the replication job or pending replication request. It can be a remote Core ID, host name, customer ID, email address, or pending replication request ID.
`-accept`	Accepts the replication request.
`-deny`	Denies the replication request.
`-ignore`	Ignores the replication request.
`-protectedserver`	When responding to a replication request, use this option to apply your response to list of protected servers with a repository name or ID. Use the parameter "all" to apply response to all requested machines.

Examples:

Accept a pending replication request for one protected machines:

```
>Set-ReplicationResponse -id customer@email.address -accepted -protectedserver
10.10.1.1 Repository1 10.10.1.2 Repository2 -responsecomment A response comment
```

Deny a pending replication request:

```
>Set-ReplicationResponse -id customer@email.address -deny
```

Start-AttachabilityCheck

The `Start-AttachabilityCheck` command forces an attachability check for all SQL Server databases protected by the Core.

Usage

The usage for the command is as follows:

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
  - protectedserver [machine name | IP address] -rpn [number | numbers] | -time
[time string]
```

Command Options

The following table describes the options available for the `Start-AttachabilityCheck` command:

Table 164: Start-AttachabilityCheck command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	The protected machine on which to perform the SQL attachability check.
`-rpn`	Optional. The sequential number of a recovery point on which to perform the SQL attachability check. You can use the `-GetRecoveryPoints` command to obtain recovery point numbers. You can specify several space-separated numbers to perform the checks against multiple recovery points with a single command. **Note:** If neither 'time' nor 'rpn' option is specified in this command, than the most recent recovery point is used for the attachability check.
`-time`	Optional. Determines recovery point to be selected for SQL attachability check. You need to specify exact time in the format "MM/DD/YYYY hh:mm tt" (for example: "04/24/2015 09:00 AM")." Specify date time values of the time zone set on your local machine. **Note:** If neither 'time' nor 'rpn' option is specified in this command, than the most recent recovery point will be exported.

Example:

Perform a SQL attachability check on the most recent recovery point for the specified protected SQL server:

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-AzureDeploy

You can use the `Start-AzureDeploy` command to export a virtual machine (VM) to a Microsoft Azure cloud account.

Usage

The usage for the command is as follows:

```
Start-AzureDeploy -core [host name] -user [user name for Core]
                -password [password for Core] -protectedserver [name | IP
address] -volumes
                [volume names | all] -destinationcontainer [Azure destination
container]
                -deploymentname [name of deployment] -subscriptionid [Azure
subscription ID]
                -cloudservicename [cloud service name] -vmname [virtual machine
name] -vmsize
                [virtual machine size] -endpointname [rdp | ssh] -protocol [tcp
| udp]
                -publicremoteaccessport [public port number] -
privateremoteaccessport [private
                port number]
```

Command Options

The following table describes the options available for the `Start-AzureDeploy` command:

Table 165: Start-AzureDeploy command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Protected machine with recovery points that you want to export.
`-volumes`	Optional. List of additional volume names for the deploy. If you use the value `all` or use no value, then all volumes deploy.
`-destinationcontainer`	The name of the Azure destination container you want to use for the deploy.

Option	Description
-deploymentname	The name of the deployment.
-subscriptionid	The Azure subscription ID.
-cloudservicename	The name of the Azure cloud service.
-vmname	The name of the virtual machine.
-vmsize	The size of the virtual machine; for example, A0, Basic_A4, or Standard_G1.
-endpointname	The Azure endpoint protocol used only for remote access rdp or ssh. The default value is rdp.
-protocol	The protocol used only for remote access tcp or udp. The default value is tcp.
-publicremoteaccessport	The public port for using remote access. The default value is 3389.
-privateremoteaccessport	The private port for using remote access. The default value is 3389.
-privateagentport	Optional. The Agent port. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-publicagentport	Optional. The external Agent port. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-privatetransferport	Optional. The TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.
-publictransferport	Optional. The external TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **Note:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.

Examples:

Deploy data to Azure:

```
>Start-AzureDeploy -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0
```

Deploy data to Azure using a specified endpoint:

```
>Start-AzureDeploy -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
```

```
VirtualMachine -vmsize A0 -endpointname ssh -protocol udp -publicremoteaccessport
1555 -privateremoteaccessport 22
```

Deploy data to Azure with specified Agent and transfer endpoint when the `-privateagentport` option has a user-defined value of `8006`. The parameter for `-publicagentport` uses the special value `0`, which is copied from `-privateagentport`. The parameter for `-privatetransferport` uses the special value `0`, which is taken from the Agent configuration. The parameter for `-publictransferport` uses the special value `0`, which is copied from `-privatetransferport`:

```
>Start-AzureDeploy -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 8006 -publicagentport 0 -
privatetransferport 0 -publictransferport 0
```

Deploy data to Azure using all available disks:

```
>Start-AzureDeploy -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -deploymentname Deploy1 -destinationcontainer container1
-subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 8006 -publicagentport 0 -
privatetransferport 0 -publictransferport 0 -Volumes all
```

Start-AzureExport

You can use the `Start-AzureExport` command to force the export of data from a protected machine to a Microsoft Azure virtual server.

Usage

The usage for the command is as follows:

```
Start-AzureExport -core [host name] -user [user name for Core] -password
[password for Core] -protectedserver [name | IP address] -volumes [volume
names | all] -rpn [number | numbers] -time [time string] -cloudaccountid
[Azure account ID] -storageaccountname[ storage account name] -containername
[container name] -foldername [folder name] -deploymentname [deployment name] -
destinationcontainer [Azure destination container] -subscriptionid [Azure
subscription ID] -cloudservicename [cloud service name] -vmname [virtual
machine name] -vmsize [virtual machine size] -endpointname [rdp | ssh] -
protocol [tcp | udp] -publicremoteaccessport [public remote access port number]
-privateremoteaccessport [private port number]
```

Command Options

The following table describes the options available for the `Start-AzureExport` command:

Table 166: Start-AzureExport command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
-protectedserver	Protected machine with recovery points that you want to export.
-volumes	Optional. List of additional volume names for the deploy. If you use the value `all` or use no value, the all volumes deploy.
-rpn	Optional. The sequential number of a recovery point that you want to export (use the `/list` rps command to get the numbers). If neither `-time` nor `-rpn` is specified, then the most recent recovery point is exported.
-time	Optional. This option determines the recovery points to select for export. Specify the exact time in the format `mm/dd/yyyy hh:mm tt`; for example, `2/24/2012 09:00 AM`. Keep in mind to specify the date time value of the time zone set on your PC. If neither `-time` nor `-rpn` is specified, then the most recent recovery point is exported.
-cloudaccountid	Optional, if the `-storageaccountname` is specified. Specify the Azure cloud account ID.
-storageaccountname	Optional, if the `-cloudaccountname` is specified. Specify the Azure storage account name.
-containername	The name of the Azure container.
-foldername	Optional. The name of the Azure folder.
-deploymentname	Use this option to specify the name of the deployment. It is required for a deploy after export only.
-destinationcontainer	The name of the Azure destination container you want to use for the deploy.
-subscriptionid	The Azure subscription ID. It is required for a deploy after export only.
-cloudservicename	The name of the Azure cloud service. It is required for a deploy after export only.
-vmname	The name of the virtual machine. It is required for a deploy after export only.
-vmsize	The size of the virtual machine; for example, `A0`, `Basic_A4`, or `Standard_G1`.
-endpointname	The Azure endpoint protocol used only for remote access `rdp` or `ssh`. The default value is `rdp`. It is required for a deploy after export only.
-protocol	The protocol used only for remote access `tcp` or `udp`. It is required for a deploy after export only. The default value is `tcp`.
-publicremoteaccessport	The public port for using remote access. The default value is `3389`.

Option	Description
-privateremoteaccessport	The private port for using remote access. The default value is 3389.
-privateagentport	Optional. The Agent port. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-publicagentport	Optional. The external Agent port. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publicagentport nor -privateagentport is specified, then no endpoint is added.
-privatetransferport	Optional. The TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.
-publictransferport	Optional. The external TCP port upon which to accept connections from the Core for the transfer of data from the Agent. If the port value is 0, then the value is determined by the Agent configuration. **NOTE:** If neither the parameter -publictransferport nor -privatetransferport is specified, then no endpoint is added.
-hypervgenerationtype	Specifies virtual machine generation. Azure supports two generations of Hyper-V virtual machines: 1 and 2.

Examples:

Export data to Azure:

```
>Start-AzureExport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -cloudaccountid "Cloud Account 1" -containername
"mycontainer" -foldername "folder" -deploymentname Deploy1 -destinationcontainer
container1 -subscriptionid "111111-22222-33333-4444-555555" -cloudservicename
Service1 -vmname VirtualMachine -vmsize A0
```

Export data to Azure using a specified endpoint:

```
>Start-AzureExport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -cloudaccountid "Cloud Account 1" -containername
"mycontainer" -foldername "folder" -deploymentname Deploy1 -destinationcontainer
container1 -subscriptionid "111111-22222-33333-4444-555555" -cloudservicename
Service1 -vmname VirtualMachine -vmsize A0 -endpointname ssh -protocol udp -
publicremoteaccessport 1555 -privateremoteaccessport 22
```

Export data to Azure with a specified Agent endpoint when the -privateagentport option uses the special value 0, which is taken from the Agent configuration. The -publicagentport option has the user-defined value of 1888:

```
>Start-AzureExport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -cloudaccountid "Cloud Account 1" -containername
"mycontainer" -deploymentname Deploy1 -destinationcontainer container1 -
subscriptionid "111111-22222-33333-4444-555555" -cloudservicename Service1 -vmname
VirtualMachine -vmsize A0 -privateagentport 0 -publicagentport 1888
```

Export data to Azure with specified Agent and transfer endpoints. The `-privateagentport` option has the user-defined value of `8006`. The parameter for `-publicagentport` uses the special value of `0`, which is copied from the `-privateagentport` option. The parameter for `-privatetransferport` uses the special value of `0`, which is taken from the Agent configuration. The parameter for `-publictransferport` uses the special value `0`, which is copied from the `-privatetransferport` option.:

```
>Start-AzureExport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -cloudaccountid "Cloud Account 1" -containername
"mycontainer" -foldername "folder" -deploymentname Deploy1 -destinationcontainer
container1 -subscriptionid "111111-22222-33333-4444-555555" -cloudservicename
Service1 -vmname VirtualMachine -vmsize A0 -privateagentport 8006 -publicagentport 0
-privatetransferport 0 -publictransferport 0
```

Start-ChecksumCheck

The `Start-ChecksumCheck` PowerShell command lets you force a checksum check of Exchange Server recovery points.

Usage

The usage for the command is as follows:

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -
protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Command Options

The following table describes the options available for the `Start-ChecksumCheck` command:

Table 167: Start-ChecksumCheck command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-protectedserver	The name of the protected machine.
-rpn	Optional. Only for chain deletion (base image with chain of incrementals or orphaned points). The sequential number of a recovery point to check (use the Get-RecoveryPoints command to obtain the numbers). You can specify several space-separated numbers to delete multiple recovery points with a single command.
-time	Optional. Select the recovery point to check by its creation time, instead of its sequential number. Specify the exact time in the format "mm/dd/yyyy hh:mm tt" (for example, "2/24/2012 09:00 AM"). Keep in mind to specify date and time values of the time zone set on your computer.

Example:

Start a checksum check on two recovery points.:

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

Start-ConsumeSeedDrive

Use `Start-ConsumeSeedDrive` for the initial data transfer when you establish Rapid Recovery replication.

Usage

The usage for the command is as follows:

```
Start-ConsumeSeedDrive -path [local | network path] -seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] -protectedserver [name] | -all]
```

Command Options

The following table describes the options available for the `Start-ConsumeSeedDrive` command:

Table 168: Start-ConsumeSeedDrive command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
-user	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
-password	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the

Option	Description
	credentials for the logged-on user are used.
-path	The local or network path of the seed drive.
-seeddriveusername	Optional. The user name for the network location of the seed drive.
-seeddrivepassword	Optional. The password for the network location of the seed drive.
-remotecore	Use only with the -consume option. It is the name of the remote Core from which the seed drive recovery points are created or consumed.
-protectedserver	The name or IP address of the protected machine you are using to create or consume the seed drive of recovery points. For example: -protectedserver "10.10.60.48" "10.10.12.101."
-all	This option specifies whether to consume or copy all of the available protected machines.

Examples:

Starting consuming a seed drive located on a network share:

```
>Start-ConsumeSeedDrive -path \\10.10.1.1\Share\Seed\ -seeddriveusername
Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName -all
```

Start consuming the data from two protected machines from a seed drive located on the local system:

```
>Start-ConsumeSeedDrive -path C:\Seed\ -remotecore TargetCoreHostName -
protectedserver "10.10.1.1","10.10.1.2"
```

Start-CopySeedDrive

You can use a seed drive for the initial data transfer when you establish Rapid Recovery replication.

Usage

The usage for the command is as follows:

```
Start-CopySeedDrive -path [local | network path] -seeddriveusername [user name] -
seeddrivepassword [password] [-targetcore [name or IP] | -protectedserver [name] | -
all] -usecompatibleformat
```

Command Options

The following table describes the options available for the Start-CopySeedDrive command:

Table 169: Start-CopySeedDrive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-path`	The local or network path of the seed drive.
`-seeddriveusername`	Optional. The user name for the network location of the seed drive.
`-seeddrivepassword`	Optional. The password for the network location of the seed drive.
`-targetcore`	Optional. Use only with the `-copy` option. It is the name or IP address of the remote Core. All protected machines replicating to this Core receive seed drive recovery points.
`-protectedserver`	The name or IP address of the protected machine you are using to create or consume the seed drive of recovery points. For example: -protectedserver "10.10.60.48" "10.10.12.101."
`-all`	This option specifies whether to consume or copy all of the available protected machines.
`-usecompatibleformat`	The new archiving format offers improved performance, however it is not compatible with older Cores. Use this option when working with a legacy AppAssure Core. Confirm with dev.

Examples:

Start copying data from protected machines to a seed drive located on the local system:

```
>Start-CopySeedDrive -path C:\Seed\ -usecompatibleformat -targetcore
TargetCoreHostName
```

Start copying two protected machines to the seed drive on the network share:

```
>Start-CopySeedDrive -path \\10.10.1.1\Share\Seed\ -seeddriveusername Administrator
-seeddrivepassword 12345 -usecompatibleformat -protectedserver
"10.10.60.48","10.10.12.101"
```

Start-EsxiExport

The `Start-EsxiExport` PowerShell command initiates the launch of a virtual export from the selected Rapid Recovery recovery point to an ESX(i) server virtual machine.

Required parameters include the name of the protected machine containing recovery points to export; the name of the virtual machine you are exporting to; the amount of RAM to be allocated on the virtual machine; the host name

and port of the Linux server host, and the path to the local, network, or Linux folder where the resulting virtual machine files will be stored.

Usage

The usage for the command is as follows:

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -
protectedserver [machine name | IP address] -volumes [volume names] -rpn [number |
numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual host port number] -hostusername [virtual host user
name] hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram]
-diskprovisioning [thin | thick] -diskmapping [automatic | manual | withvm]
```

Command Options

The following table describes the options available for the `Start-EsxiExport` command:

Table 170: Start-EsxiExport command options

Option	Description
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Protected machine with recovery points to be exported.
`-volumes`	Optional. List of volume names to be exported. If not specified, all volumes in the specified recovery points will be exported. Values must be enclosed in double quotes, each separated by a space. do not use trailing slashes in volume names. For example, specify “C:” not “C:/”
`-rpn`	Optional. The sequential number of a recovery point to be exported. (You can use the `Get-RecoveryPoints` command to obtain recovery point numbers. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-time`	Optional. Determines recovery point to be selected for export. You need to specify exact time in the format “MM/DD/YYYY hh:mm tt” (for example: “04/24/2015 09:00 AM”).” Specify date time values of the time zone set on your local machine. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-vmname`	Windows name of the virtual machine.
`-hostname`	The virtual server host name.
`-hostport`	The virtual server port number.

Option	Description
-hostusername	The user name to the virtual server host.
-hostpassword	The password to the virtual server host.
-ram	Allocate specific amount of RAM on the virtual server.
-usesourceram	Optional. Allocate the same amount of RAM on the virtual server as the source protected machine.
-diskprovisioning	Optional. The amount of disk space that will be allocated on the virtual machine. Specify 'thick' to make the virtual disk as large as the original drive on the protected server, or 'thin' to allocate the amount of actual disk space occupied on the original drive, plus some extra space in megabytes. By default, 'thin' provisioning is selected.
-diskmapping	Optional. Select either 'auto,' 'manual,' or 'withvm'. By default, auto-mapping is enabled.
-resetup	Optional. Recreates virtual machine if it is already presented at the specified location.
-datacenter	Optional. Specifies which datacenter to use.
-resourcepool	Optional. Specifies which resource pool to use.
-datastore	Optional. Specifies which datastore to use.
-computeresource	Optional. Specifies which compute resource to use.
-version	Optional. Specifies which version of ESXi to use.

Start-HypervExport

The `Start-HypervExport` PowerShell command initiates the launch of a virtual export from the selected Rapid Recovery recovery point to a Hyper-V server virtual machine.

Usage

The usage for the command is as follows:

```
Start-HypervExport -core [host name] -user [user name] -password [password] -
protectedserver [[machine name] or [IP address]] -volumes [volume names] -rpn
[number | numbers] | -time [time string] [-vmname [uselocalmachine] | -hostname
[virtual host name] -hostport [virtual host port number] -hostusername [virtual host
user name] -hostpassword [virtual host password] -vmlocation [location]] [-ram
[total megabytes] | -usesourceram] -diskformat [VHD | VHDX] -exportvmconfigfiles
```

Command Options

The following table describes the options available for the `Start-HypervExport` command:

Table 171: Start-HypervExport command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Protected machine with recovery points to be exported.
`-volumes`	Optional. List of volume names to be exported. If not specified, all volumes in the specified recovery points will be exported. Values must be enclosed in double quotes, each separated by a space. do not use trailing slashes in volume names. For example, specify “C:” not “C:/”
`-rpn`	Optional. The sequential number of a recovery point to be exported. (You can use the `Get-RecoveryPoints` command to obtain recovery point numbers. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-time`	Optional. Determines recovery point to be selected for export. You need to specify exact time in the format “MM/DD/YYYY hh:mm tt” (for example: “04/24/2015 09:00 AM”).” Specify date time values of the time zone set on your local machine. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-vmname`	Windows name of the virtual machine.
`-gen2`	Optional. Specify to use the second VM generation. If not specified, generation 1 is used. Rapid Recovery supports generation 2 from Windows Server 2012 R2 through Windows 8.1.
`-usevhdx`	Optional. If you specify this option, Rapid Recovery uses the VHDX disk format to create the VM. If you do not, it uses the VHD disk format. Generation 2 uses only the VHDX format.
`-uselocalmachine`	Optional. Connect the local Hyper-V server. If this parameter is used, the following options are ignored: hostname, host port, host username, host password.
`-hostname`	The virtual server host name.
`-hostport`	The virtual server port number.
`-hostusername`	The user name to the virtual server host.
`-hostpassword`	The password to the virtual server host.
`-vmlocation`	Local or network path to the folder where you want to store the virtual machine files.
`-ram`	Allocate specific amount of RAM on the virtual server.
`-usesourceram`	Optional. Allocate the same amount of RAM on the virtual server as the source

Option	Description
	protected machine.
-exportvmconfigfiles	Optional. Specify whether to export virtual machine configuration files. This option is available only both when the source is a virtual protected agentlessly and when the target hpyervisor is the same as the source hypervisor.

Example:

Create a Hyper-V machine file to be stored on a remote machine:

```
>Start-HypervExport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname
10.10.10.23 -hostport 443 –hostusername root –hostpassword 12QWsdxc@# -ram 4096
```

Start-LogTruncation

The `Start-LogTruncation` command forces log truncation for the specified protected SQL Server or Microsoft Exchange server.

Usage

The usage for the command is as follows:

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -
protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

Command Options

The following table describes the options available for the `Start-LogTruncation` command:

Table 172: Start-LogTruncation command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
-user	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
-password	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
-protectedserver	Archive of recovery points for the specified machine.
-target	Specify the type of log truncation (either ‘sql’ or ‘exchange’). If not specified, logs are truncated on all databases.

Example:

Truncate SQL logs:

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Truncate Exchange server logs: all recovery points for all machines on the Core:

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

The `Start-MountabilityCheck` command forces a mountability check for protected Microsoft Exchange mail stores.

Usage

The usage for the command is as follows:

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -
protectedserver [[machine name] or [IP address]] -rpn [number | numbers] |   -time
[time string]
```

Command Options

The following table describes the options available for the `Start-MountabilityCheck` command:

Table 173: Start-MountabilityCheck command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Archive of recovery points for the specified machine.
`-rpn`	Optional. The sequential number of a recovery point to be exported. (You can use the `-GetRecoveryPoints` command to obtain recovery point numbers. **Note:** If neither 'time' nor 'rpn' option is specified in this command, than the most recent recovery point will be exported.
`-time`	Optional. Determines recovery point to be selected for export. You need to specify exact time in the format "MM/DD/YYYY hh:mm tt" (for example: "04/24/2015 09:00 AM")." Specify date time values of the time zone set on your local machine.

Option	Description
	Note: If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.

Example:

Start a mountability check for oall recovery points for all machines on the Core:

```
> Start-MountabilityCheck -protected EX01
```

Start-MigrateAgent

The `Start-MigrateAgent` command migrates the protected server with it's recovery points to another DVM repository.

Usage

The usage for the command is as follows:

```
Start-MigrateAgent -core [host name] -user [login] -password [password] -
protectedserver [name | IP address] -targetrepository [name]
```

Command Options

The following table describes the options available for the `Start-MigrateAgent` command:

Table 174: Start-MountabilityCheck command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. Login ID to the remote Core host machine. If you specify a login you also have to provide a password. If none are provided the logged-in user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Name or IP of the protected machine.
`-targetrepository`	Name of the target repository.

Example:

Migrates protected server "10.10.10.10" with it's recovery points to DVM repository "Repository 2":

```
>Start-MigrateAgent -protectedserver "10.10.10.10" -targetrepository "Repository 2"
```

Start-OptimizationJob

The `Start-OptimizationJob` command lets you perform optimize a repository on demand.

Usage

The usage for the command is as follows:

```
Start-OptimizationJob -core [host name] -user [user name] -password [password] -
repository [repository name] | -all
```

Command Options

The following table describes the options available for the `Start-OptimizationJob` command:

Table 175: Start-OptimizationJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	The name of the repository that you want to optimize.
`-all`	Use this option to perform the optimization job on all repositories for this Core.

Example:

Start a repository optimization job:

```
>Start-OptimizationJob -repository "Repository 1" -core 10.10.10.10 -user
administrator -password 23WE@#$sdd
```

Start-OracleDBVerifyJob

Use the command `Start-OracleDBVerifyJob` to start the DBVerify job for one or more specified recovery points on a protected server.

Usage

The usage for the command is as follows:

```
Start-OracleDBVerifyJob -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address] -recoverypointnumber [number | numbers]
```

Command Options

The following table describes the options available for the `Start-OracleDBVerifyJob` command:

Table 176: Start-OracleDBVerifyJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable the Oracle DBVerify nightly job.
`-recoverypointnumber`	The sequential number of a recovery point that you want to export (use the `/list rps` command to get the numbers). To start the job on multiple recovery points with one command, separate each recovery point number with a space.

Example:

Start the Oracle DBVerify job for the recovery points on the specified protected server:

```
>Start-OracleDBVerifyJob -core 10.10.127.42 -user admin -password 676df#df -
protectedserver 10.10.34.88 -recoverypointnumber 1 2
```

Start-OracleLogTruncationJob

The command `Start-OracleLogTruncationJob` lets you start a log truncation job for a specified Oracle instance on a protected server.

Usage

The usage for the command is as follows:

```
Start-OracleLogTruncationJob -core [host name] -user [user name] -password
[password] -protectedserver [name | IP address] -instancename [instance SID] -
```

```
deletionpolicy [automatic | keepnewest | keepspecificnumber] -retentionduration
[duration value] -retentionunit [day | week | month | year] -numberoffiles [number
of archive files to create]
```

Command Options

The following table describes the options available for the `Start-OracleLogTruncationJob` command:

Table 177: Start-OracleLogTruncationJob command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	Use this option to specify the protected machine for which you want to enable Oracle log truncation as a nightly job.
`-instancename`	The name of the Oracle instance for which you want to start log truncation.
`-deletionpolicy`	Optional. This option must be represented by one of the following values: • `"automatic"` • `"keepnewest"` • `"keepspecificnumber"`
`-retentionduration`	Optional. This value determines the length of time to keep a log before truncating and is constrained to positive integer values. If using the `"keepnewest"` value of the `-deletionpolicy` option, a retention duration value is required.
`-retentionunit`	Optional. This option identifies the time unit for the `-retentionduration` option. It must be represented by one of the following values: • `"day"` • `"week"` • `"month"` • `"year"`
`-numberoffiles`	Optional. This option sets the number of recent archive log files to keep. If using the `"keepspecificnumber"` value of the `-deletionpolicy` option, a number of files value is required.

Examples:

Start the Oracle log truncation job for the ORCL instance on a specified protected server:

```
>Start-OracleLogTruncationJob -core 10.10.127.42 -user admin -password 676df#df -
protectedserver 10.10.34.88 -instancename ORCL
```

Start the Oracle log truncation job for the ORCL instance on a specified protected server and configure the deletion policy as "keepnewest" with the logs kept for 10 days:

```
>Start-OracleLogTruncationJob -protectedserver 10.10.34.88 -instancename ORCL -
deletionpolicy keepnewest -retentionduration 10 -retentionunit day
```

Start-Protect

The `Start-Protect` command lets an administrator add a server under protection by a Core.

Usage

```
Start-Protect -core [host name] -user [user name] -password [password] -repository
[repository name] -agent [name | IP address] -agentusername [user name]   -
agentpassword [password] -agentport [port] -volumes [volume names]
```

Command Options

The following table describes the options available for the `Start-Protect` command:

Table 178: Start-Protect command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Name of a repository on the Core where the protected machine's data is stored.
`-agentname`	Protected machine name or IP address.
`-agentusername`	Log on to the server to be protected.
`-agentpassword`	Password to the server to be protected.
`-agentport`	Protected server port number.
`-volumes`	List of volumes to protect. Values must be enclosed in double quotes and separated by a space. Do not use trailing slashes in volume names. For example, "c:" or "d:".

Example:

Put volumes of a server under protection:

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername
administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

The `Start-ProtectCluster` command lets an administrator add a server cluster under protection by a Core.

Usage

Usage for the command is as follows:

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -
repository [repository name] -clustername [name | IP address] -clusterusername [user
name for cluster] -clusterpassword [password for cluster] -clusterport [port] -
clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

Command Options

The following table describes the options available for the `Start-ProtectCluster` command:

Table 179: Start-ProtectCluster command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Name of a repository on the Core where the protected machine's data is stored. The name must be enclosed in double quotes.
`-clustername`	The name of the cluster to protect.
`-clusterusername`	User name for the cluster to be protected.
`-clusterpassword`	Password to the cluster to be protected.
`-clusterport`	Port number for the cluster to be protected.
`-clustervolumes`	List of volumes to protect. Values must be in double quotes and separated by a space. Do not use trailing slashes in volume names. For example, “c:”, “d”.

Option	Description
`-clusternodes`	List of cluster nodes with volumes to protect. First specify label “nodename” and then type the name of the node. Then, specify label “volumes” and then type a list of volumes for the node. For example: `“nodename”, “10.10.10.10”, “volumes”, “c:”, “e:”, “nodename”, “10.10.10.11,” “volumes”, “c:”`

Example:

Put volumes of a server under protection:

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -
clusterusername administrator -clusterpassword 12345 -clusterport 5002 -
clustervolumes "c:" "d:" -clusternodes nodename 10.10.10.10 volumes “c:” “e:”
```

Start-ProtectEsxServer

You can use the `Start-ProtectEsxServer` command whenever you want to add a VMware ESX(i) virtual machine to protection.

Usage

The usage for the command is as follows:

```
Start-ProtectEsxServer -core [host name] -user [user name] -password [password] -
repository [repository name] -server [name | IP address] -serverusername [user name]
-serverpassword [password for server login] -serverport [port] -virtualMachines
[virtual machines collection | all] -autoProtect [object ID or name collection]
```

Command Options

The following table describes the options available for the `Start-ProtectEsxServer` command:

Table 180: Start-ProtectEsxServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. The user name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. The password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.

Option	Description
-repository	Required. The name of the repository that is associated with the Core that you want to use to protect the virtual machine. **Note:** You must enclose the name in double quotes.
-server	The name or IP address for the vCenter or ESXi server you want to protect.
-serverusername	The user name for logging in to the vCenter or ESXi server that you want to protect.
-serverpassword	The password for logging in to the vCenter or ESXi server that you want to protect.
-serverport	Optional. The port number for the vCenter or ESXi server that you want to protect.
-virtualmachines	Optional. This option lets you list the virtual machines that you want to protect.
-autoprotect	Optional. This option lets you list new virtual machines that you want to automatically protect.

Example:

Protect specific virtual machines from a vCenter or ESXi server with the Core:

```
>Start-ProtectEsxServer -core 10.10.10.10 -user admin -password password -repository
"Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -
serverpassword password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

Start-ProtectHyperVCluster

The `Start-ProtectHyperVCluster` command adds a Hyper-V cluster under protection by a Core using agentless protection.

Usage

The usage for the command is as follows:

```
Start-ProtectHyperVCluster -core [host name] -user [user name] -password [password]
-repository [name] -server [name | IP address] -serverusername [user name] -
serverpassword [password] -serverport [port] -virtualmachines [virtual machines
collection | all] -isagentprotection
```

Command Options

The following table describes the options available for the `Start-ProtectHyperVCluster` command:

Table 181: Start-ProtectHyperVCluster command options

Option	Description
-?	Display this help message.
-core	Optional. Remote Core host machine IP address (with an optional port number). By

Option	Description
	default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
`-server`	Name or IP address of the Hyper-V server that you want to protect.
`-serverusername`	User name for the Hyper-V server to be protected.
`-serverpassword`	Password for the Hyper-V server to be protected.
`-serverport`	Optional. Protected Hyper-V server port number.
`-virtualmachines`	Optional. List of virtual machines to protect. Values must be enclosed in double quotes and separated by a space. If you exclude this parameter, only the Hyper-V cluster container is protected.
`-isagentprotection`	Optional. Use this option to protect a cluster with an Agent in each guest virtual machine, which is false by default.
`-autoprotect`	Optional. This option enables the autoprotect feature for the Hyper-V server. It is not compatible with the `-isagentprotection` option.

Example:

Protect specific virtual machines of a Hyper-V cluster:

```
>Start-ProtectHyperVCluster -core 10.10.10.10 -username admin -password password -
repository "Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root
clusterpassword password -virtualmachines "VM1" "VM2" -autoprotect
```

Start-ProtectHyperVServer

The `Start-ProtectHyperVServer` command adds a Hyper-V server under protection by a Core using agentless protection.

Usage

The usage for the command is as follows:

```
Start-ProtectHyperVServer -core [host name] -user [user name] -password [password] -
repository [name] -server [name | IP address] -serverusername [user name] -
serverpassword [password] -serverport [port] -virtualmachines [virtual machines
collection | all] -isagentprotection
```

Command Options

The following table describes the options available for the `Start-ProtectHyperVServer` command:

Table 182: Start-ProtectHyperVServer command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-repository`	Name of a repository on the Core to which the protected machine data should be stored. The name must be enclosed in double quotes.
`-server`	Name or IP address of the Hyper-V server that you want to protect.
`-serverusername`	User name for the Hyper-V server to be protected.
`-serverpassword`	Password for the Hyper-V server to be protected.
`-serverport`	Optional. Protected Hyper-V server port number.
`-virtualmachines`	Optional. List of virtual machines to protect. Values must be enclosed in double quotes and separated by a space. If you exclude this parameter, only the Hyper-V cluster container is protected.

Example:

Protect specific virtual machines of a Hyper-V server:

```
>Start-ProtectHyperVServer -core 10.10.10.10 -username admin -password password -
repository “Repository 1” -server 10.10.8.150 -serverport 443 -serverusername root
clusterpassword password -virtualmachines “VM1” "VM2"
```

Start-RepositoryCheck

The `Start-RepositoryCheck` PowerShell command lets you check the integrity of a repository.

Usage

The usage for the command is as follows:

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -
password [password] -force
```

Command Options

The following table describes the options available for the `Start-RepositoryCheck` command:

Table 183: Start-RepositoryCheck command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-repository`	Required. The name of the repository that you want to check.
`-all`	Optional. Check all repositories associated with this Core.
`-force`	Optional. Perform the repository check without confirmation.

Example:

Start checking a repository:

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Start-RestoreAgent

The `Start-RestoreAgent` command lets you restore a protected machine or volume from a specific Rapid Recovery recovery point.

Usage

The usage for the command is as follows:

```
Start-RestoreAgent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

Command Options

The following table describes the options available for the `Start-RestoreAgent` command:

Table 184: Start-RestoreAgent command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-protectedserver`	The name or IP address of the server you want to restore.
`-rpn`	The identification number of the recovery point you want to use to restore the machine. To find the correct number, use the command `/list rps`.
`-volumes`	The IDs or names of the volumes you want to restore. To restore all protected volumes, use `-volumes all`.
`-targetmacchine`	The name of the machine to which you want to restore the protected machine.
`-targetvolume`	The name or ID of the volume to which you want to restore the machine.
`-forcedismount`	Optional. Use this option to force the dismount of the database on demand.
`-autorestart`	Optional. Use this command if restarting an Exchange Server machine is necessary.

Example:

Restore a machine to a protected machine with the IP address 192.168.20.130, including the force database dismount option:

```
>Start-RestoreAgent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:"
-targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

Start-RestoreArchive

Businesses often use long-term storage to archive both compliant and non-compliant data. The archive feature in Rapid Recovery is used to support the extended retention for compliant and non-compliant data. The administrator can save an archive on the local storage or network location by specifying the `-Path` command and credentials.

Usage

The usage for the command is as follows:

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP
address2]"] -repository [name] -archiveusername [name] -archivepassword [password] -
path [location]  -cloudaccountname [name] -cloudcontainer [name]
```

Command Options

The following table describes the options available for the `Start-RestoreArchive` command:

Table 185: Start-RestoreArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Archive recovery points for all protected machines.
`-protectedserver`	The protected machine with recovery points that you want to archive. You can specify multiple machine names enclosed in double quotes and separated by commas.
`-repository`	The name of the repository where you want to place restored recovery points. You must enclose the name in double quotes; for example, "Repository1."
`-archiveusername`	Optional. The user name for logging in to the remote machine. It is required for a network path only.
`-archivepassword`	Optional. The password for logging in to the remote machine. It is required for a network path only.
`-path`	The path to where to save the archived data. For example: • Local machine: "d:\work\archive" • Network path: "\\servername\sharename" • Folder in a cloud account: "Folder Name" **Note:** The number of symbols should not be greater than 100 for local and network locations, and should not be greater than 150 for a cloud location.
`-cloudaccountname`	Optional. Use only for cloud archiving. The name of the cloud account where you want to save the archive.
`-cloudcontainer`	Optional. Use only for cloud archiving. The name of the cloud container in the chosen cloud account, where the archive will be saved. When you use this option, you should also specify the "-cloudaccountname" parameter.
`-manifestcore`	Optional. Specify the Core that you want to use from the manifest of the restored archive.

Example:

Archive all recovery points for all machines on the Core and store them on the local machine:

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

The `Start-ScheduledArchive` PowerShell command lets you force a Rapid Recovery scheduled archive to begin on demand, regardless of the pre-established schedule.

Usage

The usage for the command is as follows:

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `Start-ScheduledArchive` command:

Table 186: Start-ScheduledArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Force all scheduled archives.
`-id`	The identification number or space-separated identifiers of the scheduled archives that you want to force.

Example:

Start multiple scheduled archive jobs:

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

The `start-VBExport` command initiates the launch of a virtual export from the selected recovery point to an Oracle VirtualBox server virtual machine.

Required parameters include the name of the protected machine containing recovery points to export; the name of the virtual machine you are exporting to; the amount of RAM to be allocated on the virtual machine; the host name and port of the Linux server host, and the path to the local, network, or Linux folder where the resulting virtual machine files will be stored.

Usage

The usage for the command is as follows:

```
Start-VBExport -core -user [user name] -password [password] -protectedserver
[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] |
  -time [time string] -vmname [virtual machine name] [-ram [total megabytes] |   -
usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath
[location] pathusername [user name] - pathpassword [password]
```

Command Options

The following table describes the options available for the `Start-VBExport` command:

Table 187: Start-VBExport command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Protected machine with recovery points to be exported.
`-volumes`	Optional. List of volume names to be exported. If not specified, all volumes in the specified recovery points will be exported. Values must be enclosed in double quotes, each separated by a space. do not use trailing slashes in volume names. For example, specify “C:” not “C:/”
`-rpn`	Optional. The sequential number of a recovery point to be exported. (You can use the `Get-RecoveryPoints` command to obtain recovery point numbers.) **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-time`	Optional. Determines recovery point to be selected for export. You need to specify exact time in the format “MM/DD/YYYY hh:mm tt” (for example: “04/24/2015 09:00 AM”).” Specify date time values of the time zone set on your local machine. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-vmname`	Windows name of the virtual machine.
`-ram`	Allocate specific amount of RAM on the virtual server.

Option	Description
-usesourceram	Optional. Allocate the same amount of RAM on the virtual server as the source protected machine.
-linuxhostname	Linux VirtualBox server hostname.
-hostport	Linux VirtualBox server port.
-targetpath	Local or network or Linux path to the folder where the virtual machine files are to be stored.
-pathusername	User name for network machine. Only required when you specify network path in parameter -targetpath.
-pathpassword	Password for network machine. Only required when you specify network path in parameter -targetpath.
-accountusername	Optional. Use if you can specify a user account to register the exported virtual machine. For local or network machine only.
-accountpassword	Optional. Use only when you specify a user account to register the exported virtual machine using parameter -accountusername. For local or network machine only.

Example:

Export all volumes from the latest recovery point on machine 10.10.12.97 to a VM called NewVirtualBoxVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram
usesourceram -targetpath D:/exports
```

Start-VirtualStandby

The Start-VirtualStandby PowerShell command lets you force a Rapid Recovery a data export to a virtual standby machine. This on-demand export can occur outside of the regularly scheduled virtual standby exports.

Usage

The usage for the command is as follows:

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Command Options

The following table describes the options available for the Start-VirtualStandby command:

Table 188: Start-VirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Force an export for all virtual standby

Option	Description
	machines.
-protectedserver	The name or names—separated by a comma and space—of the protected machines that you want to force to export.

Example:

Force a virtual standby export for a protected machine:

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22
```

Start-VMExport

The `Start-VMExport` command initiates the launch of a virtual export from the selected recovery point to a VMware Workstaation server virtual machine.

Required parameters include the name of the protected machine containing recovery points to export; the name of the virtual machine you are exporting to; the amount of RAM to be allocated on the virtual machine; and the path to the local or network, folder where the resulting virtual machine files will be stored.

Usage

The usage for the command is as follows:

```
Start-VMExport -core -user [user name] -password [password] -protectedserver
[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] |
  -time [time string] -vmname [virtual machine name] [-ram [total megabytes] |   -
usesourceram] -linuxhostnme [linux hostname] -hostport [linux port] -targetpath
[location] pathusername [user name] - pathpassword [password]
```

Command Options

The following table describes the options available for the `Start-VMExport` command:

Table 189: Start-VMExport command options

Option	Description
-?	Display this help message.

Option	Description
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Protected machine with recovery points to be exported.
`-volumes`	Optional. List of volume names to be exported. If not specified, all volumes in the specified recovery points will be exported. Values must be enclosed in double quotes, each separated by a space. do not use trailing slashes in volume names. For example, specify “C:” not “C:/”
`-rpn`	Optional. The sequential number of a recovery point to be exported. (You can use the `Get-RecoveryPoints` command to obtain recovery point numbers. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-time`	Optional. Determines recovery point to be selected for export. You need to specify exact time in the format “MM/DD/YYYY hh:mm tt” (for example: “04/24/2015 09:00 AM”).” Specify date time values of the time zone set on your local machine. **Note:** If neither ‘time’ nor ‘rpn’ option is specified in this command, than the most recent recovery point will be exported.
`-vmname`	Windows name of the virtual machine.
`-ram`	Allocate specific amount of RAM on the virtual server.
`-usesourceram`	Optional. Allocate the same amount of RAM on the virtual server as the source protected machine.
`-targetpath`	Local or network or Linux path to the folder where the virtual machine files are to be stored.
`-pathusername`	User name for network machine. Only required when you specify network path in parameter `-targetpath`.
`-pathpassword`	Password for network machine. Only required when you specify network path in parameter `-targetpath`.
`-version`	Version of VMware Tools to use. Valid versions are: 7, 8, 9, and 10.

Example:

Export all volumes from the latest recovery point on machine 10.10.12.97 to a VM called NewVMwareVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -
targetpath D:/exports
```

Stop-ActiveJobs

The `Stop-ActiveJobs` cancels active jobs for a specified protected machine.

Usage

The usage for the command is as follows:

```
Stop-ActiveJobs [-protectedserver [machine name | IP address] | -core [host name]] -
user [user name] -password [password] -jobtype [jobtype]
```

Command Options

The following table describes the options available for the `Stop-ActiveJobs` command:

Table 190: Stop-ActiveJobs command options

Option	Description
`-?`	Display this help message.
`-all`	Select and cancel events of the specified type for all protected machines.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Determines protected machine on which jobs should be canceled.
`-jobtype`	Optional. Specifies job type filter. Available values are: ‘transfer’ (data transfer), ‘repository’ (repository maintenance), ‘replication’ (local and remote replications), ‘backup’ 9backup and restore), ‘bootcdbuilder’ (create boot CDs), ‘diagnostics’(upload logs), ‘exchange’ (Exchange Server files check), ‘export (recovery point export), ‘pushinstall’ (deploy Agent software to protected machines), ‘rollback’ (restore data from recovery point), ‘rollup’ (recovery point rollup’s), ‘sqlattach’ (agent attachability checks), ‘mount’ (not repository). By default, all jobs of the specified type are canceled.

Example:

Stop transfer job in protected machine:

```
>Stop-ActiveJobs –protectedserver 10.10.1.76 -jobtype transfer
```

Stop all jobs for a specific protected machine:

```
>Stop-ActiveJobs –protectedserver 10.10.1.76 -all
```

Stop-CoreService

Use this command to stop the Core service on a Core machine.

Usage

The usage for the command is as follows:

```
Stop-CoreService -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false] -wait [time in seconds]
```

Command Options

The following table describes the options available for the `Stop-CoreService` command:

Table 191: Stop-CoreService command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."
`-wait`	Optional. This option indicates that the command should wait until the Core service is fully stopped for the specified period of time in seconds before canceling active jobs.

Example:

Stop the Core service:

```
>Stop-CoreService -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true -wait 600
```

Suspend-Replication

The `Suspend-Replication` command lets an administrator pause replication.

A user can pause replication in three ways:

- Pause replication on the source Core for all protected machines (`-outgoing parameter`)
  The administrator must specify the remote machine name with outgoing replication pairing to pause outgoing replication on the source Core.

```
>Suspend-replication -outgoing 10.10.12.10
```

- Pause replication on the source Core for a single protected machine (`-protectedserver` parameter)

```
>Suspend-replication -protectedserver 10.10.12.97
```

- Pause replication on the target Core (`-incoming parameter`)
  If the local Core is a target Core, the administrator can pause replication by specifying the source Core using the –incoming parameter.

Command Options

The following table describes the options available for the `Suspend-Replication` command:

Table 192: Suspend-Replication command options

Option	Description
`-?`	Display this help message.
`-all`	Pauses all protected machines on the selected Core.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-pause`	`[snapshots]`, `[replication]` or `[vmexport]`.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-protectedserver`	Pause the current protected server.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-incoming`	Host name of the remote Core that replicates to the Core machine. Replication is suspended for all protected machines on the remote Core.
`-outgoing`	Host name of the remote target core to which data is replicating. Replication is suspended for all protected machines on the remote core.

Example:

Pause outgoing replication on the remote Core with the IP address: 10.10.1.15, for the single protected machine with the IP address: 10.10.1.76:

```
>Suspend-replication –core 10.10.1.15 –protectedserver 10.10.1.76
```

Pause outgoing replication from the local Core to remote target with the IP address: 10.10.1.63 for all protected machines:

```
>Suspend-replication –outgoing 10.10.1.63
```

Pause incoming replication from 10.10.1.82 on the remote Core with the IP address: 10.10.1.15 (Administrator is able to pause incoming replication only for whole machine):

```
>Suspend-replication –core 10.10.1.15 –incoming 10.10.1.82
```

Suspend-ScheduledArchive

The `Suspend-ScheduledArchive` PowerShell command lets you pause a Rapid Recovery scheduled archive. This command prevents the archive from occurring as scheduled until you reactivate it.
If the topic is relevant, include and re-link:
For more information, see Resume-ScheduledArchive.
.

Usage

The usage for the command is as follows:

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Command Options

The following table describes the options available for the `Suspend-ScheduledArchive` command:

Table 193: Suspend-ScheduledArchive command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-all`	Pauses all scheduled archives.
`-id`	The identification number or space-separated numbers of scheduled archives to suspend.

Example:

Suspend multiple scheduled archives:

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Scheduler

This command lets you suspend or pause the task scheduler it has been paused.

Usage

The usage for the command is as follows:

```
Suspend-Scheduler -core [host name] -user [user name] -password [password] -
cancelactivejobs [true | false]
```

Command Options

The following table describes the options available for the `Suspend-Scheduler` command:

Table 194: Suspend-Scheduler command options

Option	Description
`-?`	Display this help message.
`-restore`	[`snapshots`], [`replication`] or [`vmexport`].
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default, the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you must also provide a password. If none is provided, then the credentials for the logged-on user are used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none is provided, then the credentials for the logged-on user are used.
`-cancelactivejobs`	Optional. Use this option to cancel all active jobs on the Core. The default setting is "false."

Example:

Pause the task scheduler:

```
>Suspend-Scheduler -core 10.10.127.42 -user admin -password 676df#df -
cancelactivejobs true
```

Suspend-Snapshot

The `Suspend-Snapshot` command lets an administrator pause snapshots.

Usage

The usage for the command is as follows:

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |   -
protectedserver [name | IP address] -time [time string]
```

Command Options

The following table describes the options available for the `Suspend-Snapshot` command:

Table 195: Suspend-Snapshot command options

Option	Description
`-?`	Display this help message.
`-all`	Pauses all protected machines on the selected Core.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-time`	The time in the format `'Day-Hours-Minutes'` when the snapshots will be resumed (only for snapshots pause).

Example:

Pause snapshots for the protected machine with IP 10.10.10.4 for the local Core with a certain time to resume:

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

The `Suspend-VirtualStandby` PowerShell command lets you pause the export of data to a Rapid Recovery virtual standby machine.

Usage

The usage for the command is as follows:

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Command Options

The following table describes the options available for the `Suspend-VirtualStandby` command:

Table 196: Suspend-VirtualStandby command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a log on. If none are provided, then the logged-on user's credentials will be used.
`-all`	Pause exports for all virtual standby machines.
`-protectedserver`	The name or names—separated by a comma and space—of the protected machines with virtual standby machines that you want to suspend.

Example:

Suspend virtual standby exports for a protected machine:

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22
```

Suspend-VMExport

The `Suspend-VMExport` command lets an administrator pause exports to virtual machines.

Usage

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Command Options

The following table describes the options available for the `Suspend-VMExport` command:

Table 197: Suspend-VMExport command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name,

Option	Description
	you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.
`-all`	Pauses all protected machines on the selected Core.
`-protectedserver`	Pause the current protected server.

Example:

Suspend VM export for the protected machine with IP 10.10.10.4 for the local Core:

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

The `Update-Repository` command adds an extent to an existing DVM repository. The size specified must be between 250MB and 16TB.

Usage

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]  -metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -sharepassword [share password]]] -core [host name] -user [user name]  -password [password]
```

Command Options

The following table describes the options available for the `Update-Repository` command:

Table 198: Update-Repository command options

Option	Description
`-?`	Display this help message.
`-core`	Optional. Remote Core host machine IP address (with an optional port number). By default the connection is made to the Core installed on the local machine.
`-user`	Optional. User name for the remote Core host machine. If you specify a user name, you also have to provide a password. If none are provided, then the logged-on user's credentials will be used.
`-password`	Optional. Password to the remote Core host machine. If you specify a password, you also have to provide a user name. If none are provided, then the logged-on user's credentials will be used.

Option	Description
-name	DVM repository name.
-size	Size of DVM repository extent. Available units are: b, Kb, MB, GB, TB, PB.
-datapath	For local location only. Determines data path of DVM repository extent.
-metadatapath	For local location only. Determines metadata path of DVM repository extent.
-uncpath	For share location only. Determines data and metadata paths of DVM repository extent.
-shareusername	For share location only. Determines login to share location.
-sharepassword	For share location only. Determines password to share location.

Example:

Add an extent to the DVM repository of the minimum size:

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -
metadatapath C:\repository\Metadata
```

Localization

When running on the same machine on which Rapid Recovery Core is installed, the Rapid Recovery PowerShell module bases its display language on the language set for the Core. Localized Rapid Recovery versions such as this one support English, Chinese (Simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish.

For Non-English releases, use: Rapid Recovery Core release 6.1.1 is an English-only release. As a result, English is the only language supported for the PowerShell Module. AppAssure release 6.0.2 is the most recent localized version of the Core software. In that release, supported languages include English, Chinese (Simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish.

If the Rapid Recovery PowerShell module is installed on a separate machine, English is the only language supported.

Qualifiers

The following table describes the qualifiers available for Rapid Recovery PowerShell Module.

Table 199: Rapid Recovery PowerShell module qualifiers

Qualifier	Usage
-core <Rapid Recovery Core Name>	Host name of the Core. Default: Localhost
-ProtectedServer <Protected Server Name>	Host name/IP address of the Rapid Recovery Agent.

Qualifier	Usage
	Default: `Localhost` if multiple servers protected, otherwise the single server protected.
`-Mode <READ, READWRITE, WRITE>`	Recovery Point Mount mode. Default: `Read`.
`-Volumes <Snapshot Volume Letter>`	Snapshot volume letter from Rapid Recovery Agent. Default: `All`.
`-User <User Name>`	User name used to connect to the Rapid Recovery Core. This is typically the service user.
`-Domain <Domain Name>`	Domain to which the user defined in /User belongs.
`-Password <Password>`	Password of the user defined in `/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	For example: `C:\RapidRecoveryMount`.

Scripting

Rapid Recovery enables administrators to automate the administration and management of resources at certain occurrences through the execution of commands and scripts. The Rapid Recovery software supports the use of PowerShell scripting for Windows and Bourne shell and Bash scripting for Linux.

Core jobs are automatically created whenever you initiate operations on the Rapid Recovery Core such as replication, virtual export, or a backup transfer. You can extend these jobs by running a script before it or after it. These are known as pre and post scripts.

This section describes the scripts that can be used by administrators at designated occurrences in Rapid Recovery for Windows and Linux.

Caution: The sample PowerShell and shell scripts provided in this document will function when run as designed by qualified administrators. Take precautions when modifying functioning scripts to retain working versions. Any modifications to the script samples included here, or any scripts you create, are considered customization, which is not typically covered by Quest Support.

Using PowerShell scripting with Rapid Recovery

Windows PowerShell is a Microsoft .NET Framework-connected environment designed for administrative automation. Rapid Recovery includes comprehensive client software development kits (SDKs) for PowerShell scripting that lets administrative users run user-provided PowerShell scripts at designated occurrences; for example, before or after a snapshot, attachability and mountability checks, and so on. Administrators can run scripts from both the Rapid Recovery Core and the protected machine. Scripts can accept parameters, and the output of a script is written to Core and protected machine log files.

Note: For nightly jobs, preserve one script file and the JobType input parameter to distinguish between nightly jobs. Script files are located in the %ALLUSERSPROFILE%\AppRecovery\Scripts folder.

- In Windows 7, the path to locate the %ALLUSERSPROFILE% folder is: C:\ProgramData.
- In Windows 2003, the path to locate the folder is: Documents and Settings\All Users\Application Data\.
  Note: Windows PowerShell is required and must be installed and configured before running Rapid Recovery scripts.

For more information on how using PowerShell scripts see Sample PowerShell scripts, Input Parameters for PowerShell Scripting, Input parameters for shell scripting, and Sample shell scripts.

Prerequisites for PowerShell scripting

Before running PowerShell scripts for Rapid Recovery, you must have Windows PowerShell 2.0 or later installed. Due to new features introduced in PowerShell 3.0, including easier access to object properties, PowerShell Web access, and support for REST calls, Quest recommends using PowerShell 3.0 or later.

Note: Place the powershell.exe.config file in the PowerShell home directory. For example, C:\WindowsPowerShell\powershell.exe.config.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
       <startup useLegacyV2RuntimeActivationPolicy="true">
              <supportedRuntime version="v4.0.30319"/>
              <supportedRuntime version="v2.0.50727"/>
       </startup>
</configuration>
```

Testing PowerShell Scripts

If you want to test the scripts you plan to run, you can do so by using the PowerShell graphical editor, *powershell_is*. You also need to add the configuration file *powershell_ise.exe.config* to the same folder as the configuration file *powershell.exe.config.*

Note: The configuration file *powershell_ise.exe.config* must have the same content as the *powershell.exe.config* file.

Caution: If the pre-PowerShell or post-PowerShell script fails, the job also fails.

Localization

When running on the same machine on which Rapid Recovery Core is installed, the Rapid Recovery PowerShell module bases its display language on the language set for the Core. Localized Rapid Recovery versions such as this one support English, Chinese (Simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish.

For Non-English releases, use: Rapid Recovery Core release 6.1.1 is an English-only release. As a result, English is the only language supported for the PowerShell Module. AppAssure release 6.0.2 is the most recent localized version of the Core software. In that release, supported languages include English, Chinese (Simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish.

If the Rapid Recovery PowerShell module is installed on a separate machine, English is the only language supported.

Qualifiers

The following table describes the qualifiers available for Rapid Recovery PowerShell Module.

Table 200: Rapid Recovery PowerShell module qualifiers

Qualifier	Usage
`-core <Rapid Recovery Core Name>`	Host name of the Core. Default: `Localhost`
`-ProtectedServer <Protected Server Name>`	Host name/IP address of the Rapid Recovery Agent. Default: `Localhost` if multiple servers

Qualifier	Usage
	protected, otherwise the single server protected.
`-Mode <READ, READWRITE, WRITE>`	Recovery Point Mount mode. Default: `Read`.
`-Volumes <Snapshot Volume Letter>`	Snapshot volume letter from Rapid Recovery Agent. Default: `All`.
`-User <User Name>`	User name used to connect to the Rapid Recovery Core. This is typically the service user.
`-Domain <Domain Name>`	Domain to which the user defined in /User belongs.
`-Password <Password>`	Password of the user defined in `/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	For example: `C:\RapidRecoveryMount`.

Input Parameters for PowerShell Scripting

All available input parameters are used in sample scripts. The parameters are described in the following tables.
Note: Script files must possess the same name as the sample script files.

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

The following table presents the available objects for the AgentProtectionStorageConfiguration parameter.

Table 201: Objects for the AgentProtectionStorageConfiguration parameter

Method	Description
public Guid RepositoryId { get; set; }	Gets or sets the ID of the repository where the agent recovery points are stored.
public string EncryptionKeyId { get; set; }	Gets or sets the ID of the encryption key for this agent's recovery points. An empty string means no encryption.

AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

The following table presents the available objects for the AgentTransferConfiguration parameter.

Table 202: Objects for the AgentTransferConfiguration parameter

Method	Description
public uint MaxConcurrentStreams { get; set; }	Gets or sets the maximum number of concurrent TCP connections the Core establishes to the agent for transferring data.
public uint MaxTransferQueueDepth { get; set; }	Gets or sets the maximum number of block extents which can be queued for writing. When a range of blocks are read from a transfer stream, that range is placed on a producer or consumer queue, where a consumer thread reads it and writes it to the epoch object. If the repository writes slower than the network reads, this queue fills up. The point at which the queue is full and reads stop is the maximum transfer queue depth.
public uint MaxConcurrentWrites { get; set; }	Gets or sets the maximum number of block write operations to have outstanding on an epoch at any given time. If additional blocks are received beyond the maximum number of write operations specified in this parameter, those additional blocks are ignored until one of the outstanding writes finishes.
public ulong MaxSegmentSize { get; set; }	Gets or sets the maximum number of contiguous blocks to transfer in a single request. Depending on testing, higher or lower values may be optimal.
public Priority Priority { get; set; }	Gets or sets the priority for transfer request.
public uint GetChangedBlocksRetries { get; set; }	Gets or sets the count of retries if initial retrieval of changed blocks from the agent failed.
public int MaxRetries { get; set; }	Gets or sets the maximum number of times a failed transfer should be retried before it is presumed failed.
public bool UseDefaultMaxRetries { get; set; }	If included, the default maximum number of retries (specified in transfer configuration) will be used.
public Guid ProviderId{ get; set; }	Gets or sets the GUID of the VSS provider to use for snapshots on this host. Administrators typically accept the default.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Gets or sets the collection of VSS writer IDs that should be excluded from this snapshot. The writer ID is determined by the name of the writer. This name is for documentation purposes only, and does not necessarily provide an exact match of the writer name.
public ushort TransferDataServerPort { get; set; }	Gets or sets a value containing the TCP port upon which to accept connections from the Core for the actual transfer of data from the protected machine to the Core. The Agent attempts to listen on this port, but if the port is in use, the protected machine can use a different port instead. The Core should use the port number specified in the BlockHashesUri and BlockDataUri properties of the VolumeSnapshotInfo object for each snapped volume.
public TimeSpan CleanSnapshotTimeout { get; set;	Gets or sets the amount of time to wait for cleaning up the snapshot after transfer is finished.

Method	Description
}	
public TimeSpan SnapshotTimeout { get; set; }	Gets or sets the amount of time to wait for a VSS snapshot operation to complete before giving up and timing out.
public TimeSpan TransferTimeout { get; set; }	Gets or sets the amount of time to wait for further contact from the Core before abandoning the snapshot.
public TimeSpan NetworkReadTimeout { get; set; }	Gets or sets the timeout for network read operations related to this transfer.
public TimeSpan NetworkWriteTimeout { get; set; }	Gets or sets the timeout for network write operations related to this transfer.
public uint InitialQueueSize { get; set; }	Gets or sets a size of initial queue or requests.
public uint MinVolumeFreeSpacePercents { get; set; }	Gets or sets a minimal amount of free space on a volume, measured by percentage. If free space is lower than the amount specified in this parameter, then all change logs are deleted and a base image is forced.
public uint MaxChangeLogsSizePercents { get; set; }	Gets or sets a maximum size of driver change logs as part of volume capacity, measured by percentage. If part of change logs is bigger than this value, then all change logs are deleted and a base image is forced.
public bool EnableVerification { get; set; }	Gets or sets a value indicating whether diagnostic verification of each block sent to Core should be performed.

BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

The following table presents the available objects for the BackgroundJobRequest parameter.

Table 203: Objects for the BackgroundJobRequest parameter

Method	Description
public AgentIdsCollection AgentIds { get; set; }	Gets or sets the IDs of the protected machines.
public bool IsNightlyJob { get; set; }	Gets or sets the value indicating whether the background job is a nightly job.
public Guid NightlyJobTransactionId { get; set; }	Gets or sets the ID of nightly job transaction.
public Guid JobId { get; set; }	Gets or sets the ID of background job.
public bool Force { get; set; }	Gets or sets the value indicating if a job was forced.
public uint JobStartsCount { get; set; }	Gets or sets the number of attempts to start a job.
public virtual bool InvolvesAgentId(Guid agentId)	Determines the value indicating whether the concrete agent is involved in job.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Inherits its values from the parameter, DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Inherits its values from the parameter, BackgroundJobRequest.

Table 204: Objects for the DatabaseCheckJobRequestBase parameter

Method	Description
public string RecoveryPointId { get; set; }	Gets or sets the ID of the recovery point for which databases will be checked.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Inherits its values from the parameter, BackgroundJobRequest.

The following table presents the available objects for the ExportJobRequest parameter.

Table 205: Objects for the ExportJobRequest parameter

Method	Description
public uint RamInMegabytes { get; set; }	Gets or sets the memory size for the exported VM. Set to zero (0) to use the memory size of the source machine.
public ushort CpuCount { get; set; }	Gets or sets the CPU count for the exported VM. Set to 0 to use the CPU count of the source machine.
public ushort CoresPerCpu { get; set; }	Gets or sets the Cores per CPU count for the exported VM. Set to 0 to use the Cores per CPU count of the source machine.
public VirtualMachineLocation Location { get; set; }	Gets or sets the target location for this export. This is an abstract base class.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Gets or sets the volume images to include in the VM export.
public ExportJobPriority Priority { get; set; }	Gets or sets the priority for export request.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Inherits its values from the parameter, BackgroundJobRequest.

Table 206: Objects for the NightlyAttachabilityJobRequest parameter

Method	Description
public int SimultaneousJobsCount { get; set; }	Gets or sets count of jobs that can be run simultaneously.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Inherits its values from the parameter, BackgroundJobRequest.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

The following table presents the available objects for the TakeSnapshotResponse parameter.

Table 207: Objects for the TakeSnapshotResponse parameter

Method	Description
public Guid SnapshotSetId { get; set; }	Gets or sets the GUID assigned by VSS to this snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Gets or sets the collection of snapshot info for each volume included in the snap.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Inherits its values from the parameter, BackgroundJobRequest.

The following table presents the available objects for the TransferJobRequest parameter.

Table 208: Objects for the TransferJobRequest parameter

Method	Description
public VolumeNameCollection VolumeNames { get; set; }	Gets or sets the collection of names for transfer. VolumeNames is a data structure that contains the following data: • GuidName. The Guid associated with the volume, used as the name if a DisplayName is not set. • DisplayName. The displayed name of the volume.
public VolumeNameCollection TransferredVolumes { get; set; }	Gets or sets the collection of transferred volumes.
public VolumeNameCollection DependentVolumeNames { get; set; }	Gets or sets the collection of dependent volumes.
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	Gets or sets quotas that are enabled on a volume.

Method	Description
public ShadowCopyType ShadowCopyType { get }	Gets the type of copying for transfer. The available values are: • Copy • Full

public AgentTransferConfiguration TransferConfiguration { get; set; }	Gets or sets the transfer configuration. AgentTransferConfiguration is an object which will have the following data:
	• MaxConcurrentStreams. The maximum number of concurrent TCP connections the core will establish to the agent for transferring data
	• MaxTransferQueueDepth. The maximum number of block extents which can be queued up for writing
	• MaxConcurrentWrites. The maximum number of block write operations to have outstanding on an epoch at any given time. If additional blocks are received when this many block writes are outstanding, those additional blocks will be ignored until one of the outstanding blocks gets written.
	• MaxSegmentSize. The maximum number of contiguous blocks to transfer in a single request
	• Priority. An object which will have the following data:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (which is equal to One)
	  • Lowest (which is equal to Ten)
	  • Default (which is equal to Five)
	• MaxRetries. The maximum number of times a failed transfer should be retried before it is presumed failed
	• UseDefaultMaxRetries. A value indicating that the maximum number of retries is the default value

Method	Description
	• ProviderId. The GUID of the VSS provider to use for snapshots on this host. Users typically use the default setting.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Gets or sets the storage configuration.
public string Key { get; set; }	Generates a pseudorandom (but not cryptographically secure) key, which can be used as a one-time password to authenticate transfer requests.
public bool IsBaseImage { get; set; }	Gets or sets value indicating whether base image will be taken.
public bool IsForced { get; set; }	Gets or sets value indicating whether transfer has been forced.
public Guid ProtectionGroupId { get; set; }	Gets or sets the ID of the protection group.
public TargetComponentTypes LogTruncationTargets { get; set; }	Gets or sets value that indicates for which databases log truncation will be performed (SQL or Exchange).
public bool ForceBaseImage { get }	Gets the value indicating whether the base image was forced or not.
public bool IsLogTruncation { get }	Gets the value indicating whether the log truncation job is performing or not.

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Inherits its values from the TransferScriptParameterBase parameter.

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

The following table presents the available objects for the TransferPostscript parameter. Inherits its value from the TransferScriptParameterBase parameter.

Table 209: Objects for the TransferPostscript parameter

Method	Description
public VolumeNameCollection VolumeNames (get; set;)	Gets or sets the collection of volume names for transfer. VolumeNames is a data structure that contains the following data: • GuidName. The Guid associated with the volume, used as the name if a DisplayName is not set. • DisplayName. The displayed name of the volume.
public ShadowCopyType ShadowCopyType { get; set; }	Gets or sets the type of copying for transfer.ShadowCopyType is an enumeration with values. The available values are:

Method	Description
	• Unknown • Copy • Full
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Gets or sets the storage configuration.

public AgentTransferConfiguration TransferConfiguration { get; set; }	Gets or sets the transfer configuration. AgentTransferConfiguration is an object which will have the following data:
	• MaxConcurrentStreams. The maximum number of concurrent TCP connections the core will establish to the agent for transferring data
	• MaxTransferQueueDepth. The maximum number of block extents which can be queued up for writing
	• MaxConcurrentWrites. The maximum number of block write operations to have outstanding on an epoch at any given time. If additional blocks are received when this many block writes are outstanding, those additional blocks will be ignored until one of the outstanding blocks gets written.
	• MaxSegmentSize. The maximum number of contiguous blocks to transfer in a single request
	• Priority. An object which has the following data:
	  • "Undefined
	  • "One
	  • "Two
	  • "Three
	  • "Four
	  • "Five
	  • "Six
	  • "Seven
	  • "Eight
	  • "Nine
	  • "Ten
	  • "Highest (which is equal to One)
	  • "Lowest (which is equal to Ten)
	  • "Default (which is equal to Five)
	• MaxRetries. The maximum number of times a failed transfer should be retried before it is presumed failed

Method	Description
	• UseDefaultMaxRetries. A value indicating that the maximum number of retries is the default value • ProviderId. The GUID of the VSS provider to use for snapshots on this host. Administrators typically accept the default.
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• ExcludedWriterIds. Collection of VSS writer IDs which should be excluded from this snapshot. The writer ID is keyed by the name of the writer. This name is for documentation purposes only and does not have to exactly match the actual name of the writer. • TransferDataServerPort. A value containing the TCP port upon which to accept connections from the core for the actual transfer of data from the agent to the core. • SnapshotTimeout. The amount of time to wait for a VSS snapshot operation to complete before giving up and timing out. • TransferTimeout. The amount of time to wait for further contact from the core before abandoning the snapshot. • NetworkReadTimeout. The timeout for network read operations related to this transfer. • NetworkWriteTimeout. The timeout for network write operations related to this transfer. • InitialQueueSize. A size of initial queue of requests. • MinVolumeFreeSpacePercents. A minimal amount of free space on a volume in percent. • MaxChangeLogsSizePercents. A maximum size of driver change logs as part of volume capacity measured in percent. • EnableVerification. A value indicating whether diagnostic verification of each block sent to Core should be performed.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Gets or sets the storage configuration The AgentProtectionStorageConfiguration object contains the following data: • RepositoryId. The name of the repository where this agent's recovery points will be stored • EncryptionKeyId. The ID of the encryption key for this agent's recovery points. An empty string means no encryption
public string Key { get; set; }	The Key method generates a pseudorandom (but not

Method	Description
	cryptographically secure) key, which can be used as a one-time password to authenticate transfer requests.
public bool ForceBaseImage { get; set; }	Gets or sets the value indicating whether the transfer was a forced base image capture.
public bool IsLogTruncation { get; set; }	Gets or sets the value indicating whether logging is being truncated.
public uint LatestEpochSeenByCore { get; set; }	Gets or sets latest epoch value. The LatestEpochSeenByCore method is the ordinal number of the most recent snapshot taken by the Core. This is the 'epoch number' assigned by the filter driver to this particular snapshot at the moment it was taken with VSS.
public Guid SnapshotSetId { get; set; }	Gets or sets the GUID assigned by VSS to this snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Gets or sets the collection of snapshot info for each volume included in the snapshot.

TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution)

The following table presents the available objects for the TransferScriptParameterBase parameter.

Table 210: Objects for the TransferScriptParameterBase parameter

Method	Description
public AgentTransferConfiguration TransferConfiguration { get; set; }	Gets or sets the transfer configuration.
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Gets or sets the storage configuration.

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

The following table presents the available objects for the VirtualMachineLocation parameter.

Table 211: Objects for the VirtualMachineLocation parameter

Method	Description
public string Description { get; set;}	Gets or sets a human-readable description of this location.
public string Name { get; set;}	Gets or sets the name of the VM.

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Inherits its values from the parameter, System.Collections.ObjectModel.Collection<string>.

VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

The following table presents the available objects for the VolumeName parameter.

Table 212: Objects for the VolumeName parameter

Method	Description
public string GuidName { get; set;}	Gets or sets the ID of the volume.
public string DisplayName { get; set;}	Gets or sets the name of the volume.
public string UrlEncode()	Gets a URL-encoded version of the name which can be passed cleanly on a URL. **Note:** A known issue exists in .NET 4.0 WCF (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312), which prevents path escape characters from working correctly in a URI template. Because a volume name contains both '\' and '?', you must replace the special characters '\' and '?' with other special characters.
public string GetMountName ()	Returns a name for this volume that is valid for mounting volume image to some folder.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Inherits its values from the parameter, System.Collections.ObjectModel.Collection<VolumeName>.

The following table presents the available objects for the VolumeNameCollection parameter.

Table 213: Objects for the VolumeNameCollection parameter

Method	Description
public override bool Equals(object obj)	Determines whether this instance and a specified object, which must also be a VolumeNameCollection object, have the same value. (Overrides Object.Equals(Object).)
public override int GetHashCode()	Returns the hash code for this VolumeNameCollection. (Overrides Object.GetHashCode ().)

VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

The following table presents the available objects for the VolumeSnapshotInfo parameter.

Table 214: Objects for the VolumeSnapshotInfo parameter

Method	Description
public Uri BlockHashesUri { get; set;}	Gets or sets the URI at which the MD5 hashes of volume blocks can be read.
public Uri BlockDataUri { get; set;}	Gets or sets the URI at which the volume data blocks can be read.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Inherits its values from the parameter, System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Sample PowerShell scripts

The following sample scripts are provided to assist administrative users in executing PowerShell scripts.

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

PreTransferScript.ps1

The PreTransferScript is run on the protected machine before transferring a snapshot.

Sample PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
```

```
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
               echo 'TransferPrescriptParameterObject parameter is null'
}
else {
               echo
'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration
               echo 'StorageConfiguration:'
$TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

The PostTransferScript is run on the protected machine after transferring a snapshot.

Sample PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
                      echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
                      echo 'ShadowCopyType:'
$TransferPostscriptParameterObject.ShadowCopyType
               echo 'ForceBaseImage:'
$TransferPostscriptParameterObject.ForceBaseImage
               echo 'IsLogTruncation:'
$TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

The PreExportScript is run on the Core before any export job.

Sample PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
              echo 'ExportJobRequestObject parameter is null'
}
else {
              echo 'Location:' $ExportJobRequestObject.Location
              echo 'Priority:' $ExportJobRequestObject.Priority
}
```

PostExportScript.ps1

The PostExportScript is run on the Core after any export job.

Note: There are no input parameters for the PostExportScript when used to run once on the exported protected machine after initial startup. The regular protected machine should contain this script in the PowerShell script folder as PostExportScript.ps1.

Sample PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
              echo 'ExportJobRequestObject parameter is null'
}
else {
```

```
                echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
                echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

The PreNightlyJobScript is run before every nighty job on Core side. It contains the parameter $JobClassName, which helps to handle those child jobs separately.

Sample PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
       NightlyAttachabilityJob {
                $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
                echo 'Nightly Attachability job results:';
                        if($NightlyAttachabilityJobRequestObject -eq $null) {
                                echo 'NightlyAttachabilityJobRequestObject parameter is null';
                        }
                        else {
                                echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
                                echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNight
                        }
                        break;
                }
# working with Rollup Job
       RollupJob {
                $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
                echo 'Rollup job results:';
                        if($RollupJobRequestObject -eq $null) {
                                        echo 'RollupJobRequestObject parameter is null';
                        }
                        else {
                                echo 'SimultaneousJobsCount:' $RollupJobRequestObject.Simultaneous
```

```
                                        echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
                                        echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
                        }
                        $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System
                        if($AgentsCollection -eq $null) {
                                echo 'AgentsCollection parameter is null';
                        }
                        else {
                                echo 'Agents GUIDs:'
                                foreach ($a in $AgentsCollection) {
                                        echo $a
                        }
                }
                break;
        }
# working with Checksum Check Job
                ChecksumCheckJob {
                        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                        echo 'Exchange checksumcheck job results:';
                        if($ChecksumCheckJobRequestObject -eq $null) {
                                echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                                echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPoi
                                echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
                                echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
                        }
                        break;
                }
# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
                echo 'Transfer job results:';
                if($TransferJobRequestObject -eq $null) {
                                echo 'TransferJobRequestObject parameter is null';
                }
                else {
                                echo 'TransferConfiguration:' $TransferJobRequestObject.TransferCo
                                echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConf
                        }
                        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                        break;
                }
}
```

PostNightlyJobScript.ps1

The PostNightlyJobScript is run after every nighty job on the Core. It contains the parameter $JobClassName, which helps to handle those child jobs separately.

Sample PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore,
[object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey
('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
       NightlyAttachabilityJob {
               $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
               echo 'Nightly Attachability job results:';
               if($NightlyAttachabilityJobRequestObject -eq $null) {
                       echo 'NightlyAttachabilityJobRequestObject parameter is null';
               }
               else {
                       echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
                       echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
               }
               break;
       }
# working with Rollup Job
       RollupJob {
               $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
               echo 'Rollup job results:';
               if($RollupJobRequestObject -eq $null) {
                       echo 'RollupJobRequestObject parameter is null';
               }
               else {
                       echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
                       echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
               }
               $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System.Guid]"
               if($AgentsCollection -eq $null) {
                       echo 'AgentsCollection parameter is null';
```

```
                }
                else {
                echo 'Agents GUIDs:'
                        foreach ($a in $AgentsCollection) {
                                echo $a
                                }
                        }
                        break;
                }
# working with Checksum Check Job
        ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                        echo 'ChecksumCheckJobRequestObject parameter is null';
                }
                else {
                        echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
                        echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
                        echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
                }
                break;
        }
# working with Log Truncation Job
        TransferJob {
                $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
                echo 'Transfer job results:';
                if($TransferJobRequestObject -eq $null) {
                        echo 'TransferJobRequestObject parameter is null';
                }
                else {
                         echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfigura
                        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguratio
                }
                echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
                if($TakeSnapshotResponseObject -eq $null) {
                        echo 'TakeSnapshotResponseObject parameter is null';
                }
                else {
                        echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSe
                        echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
                }
                break;
        }
}
```

Using Bourne shell and Bash scripting with Rapid Recovery

Bourne shell (sh) is a shell language or command-line interpreter for Unix-based operating systems. Bourne shell is used in Rapid Recovery with Linux to customize environments and specify certain operations to occur in a predetermined sequence. The .sh is the file extension and naming convention for Bourne shell files.

Bourne Again Shell (Bash) is a similar shell language that implements the same grammar, parameter, and variable expansion, redirection and quoting. Bash also uses the same .sh file extension. The information here applies equally to Bash.

Using pre and post transfer, pre and post snapshot, and post export script hooks, you can perform system operations before and after a transfer or snapshot, or after virtual export. For example, you may want to disable a certain cronjob while a transfer is occurring and enable it once the transfer has finished. As another example, you may need to run commands to flush application-specific data to disk. The contents are written to a temporary file and run using exec. The script then runs using the interpreter defined in the first line of the script, for example, `(#!/usr/bin/env bash)`. If the specified interpreter is not available, the script uses the default shell defined in the $SHELL environment variable.

You can substitute and use any interpreter. For example, on the `#!` line of the script, you can replace “bash” with “zsh” (Z shell), “tcsh” (tee shell), and so on, based on your preference.

You can add available objects from the TransferPrescript parameter or add your own commands to the PreTransferScript.sh and PostTransfer.sh scripts to customize them.

Only PreTransferScript and PostTransferScript receive parameters. The snapshot and export scripts do not.

This section describes the scripts that administrators can use at designated occurrences in Rapid Recovery for Windows and Linux. It includes the following topics:

- Input parameters for shell scripting
- Sample shell scripts

Prerequisites for shell scripting

Rapid Recovery provides the ability to run Bourne shell, Bash, and other shell scripts on a protected Linux machine before and after a transfer. The following scripts are supported for Linux machines protected with the Rapid Recovery Agent software.

Note: If a script is not executable, the transfer job fails.

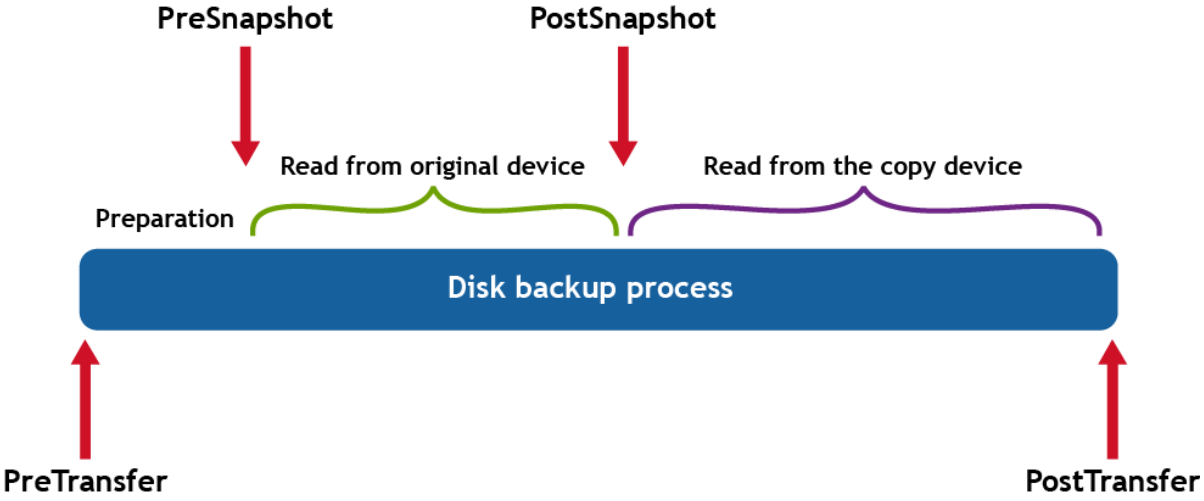
- PreTransferScript.sh
- PostTransferScript.sh
- PreSnapshotScript.sh
- PostSnapshotScript.sh
- PostExportScript.sh

To use these scripts, ensure that they reside in the `/opt/apprecovery/scripts/` directory.

Execution timing for pre and post scripts

For context, the following diagram shows the difference in timing for running pre and post transfer and snapshot scripts.

When pre and post scripts execute



Supported transfer and post-transfer script parameters

The following parameters are supported on Linux for transfer scripts. For more information, see Sample shell scripts.

- TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=$TransferPrescriptParameter_StorageConfiguration
- TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
- TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_LatestEpochSeenByCore

The following parameters are supported on Linux for post transfer scripts.

- TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration

- TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
- TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_ LatestEpochSeenByCore

Testing shell scripting

You can test the scripts you want to run by using the editor for the script (.sh) files.
Note: If the pre or post script fails, the job also fails. Information about the job is available in the /var/log/apprecovery/apprecovery.log file. Successful scripts return the exit code 0.

Input parameters for shell scripting

The parameters for shell scripting in Rapid Recovery are described in the following tables.

TransferPrescriptParameters_VolumeNames

The following table presents the available objects for the TransferPrescript parameter.
Table 215: TransferPrescript objects

Method	Description
public VolumeNameCollection VolumeNames (get; set;)	Gets or sets the collection of volume names for transfer. VolumeNames is a data structure that contains the following data: • GuidName. The Guid associated with the volume, used as the name if a DisplayName is not set. • DisplayName. The displayed name of the volume.
public ShadowCopyType ShadowCopyType { get; set; }	Gets or sets the type of copying for transfer. ShadowCopyType is an enumeration with values. The available values are: • Unknown • Copy • Full

Method	Description
public string Key { get; set; }	The Key method generates a pseudorandom (but not cryptographically secure) key, which can be used as a one-time password to authenticate transfer requests.
public bool ForceBaseImage { get; set; }	Gets or sets the value indicating whether the transfer was a forced base image capture.
public bool IsLogTruncation { get; set; }	Gets or sets the value indicating whether logging is being truncated.
public uint LatestEpochSeenByCore { get; set; }	Gets or sets latest epoch value. The LatestEpochSeenByCore method is the ordinal number of the most recent snapshot taken by the Core. This is the 'epoch number' assigned by the filter driver to this particular snapshot at the moment it was taken with VSS.

TransferPostscriptParameter

The following table presents the available objects for the TransferPostscript parameter.

Table 216: TransferPostscript objects

Method	Description
public VolumeNameCollection VolumeNames (get; set;)	Gets or sets the collection of volume names for transfer. VolumeNames is a data structure that contains the following data: • GuidName. The Guid associated with the volume, used as the name if a DisplayName is not set. • DisplayName. The displayed name of the volume.
public ShadowCopyType	Gets or sets the type of

Method	Description
ShadowCopyType { get; set; }	copying for transfer.ShadowCopyType is an enumeration with values. The available values are: • Unknown • Copy • Full
public string Key { get; set; }	The Key method generates a pseudorandom (but not cryptographically secure) key, which can be used as a one-time password to authenticate transfer requests.
public bool ForceBaseImage { get; set; }	Gets or sets the value indicating whether the transfer was a forced base image capture.
public bool IsLogTruncation { get; set; }	Gets or sets the value indicating whether logging is being truncated.
public uint LatestEpochSeenByCore { get; set; }	Gets or sets latest epoch value. The LatestEpochSeenByCore method is the ordinal number of the most recent snapshot taken by the Core. This is the 'epoch number' assigned by the filter driver to this particular snapshot at the moment it was taken with VSS.

Sample shell scripts

This section describes the sample shell scripts available for administrative users to run on protected machines.

Caution: The sample scripts provided in this document function as they exist when run by qualified administrators. Take precautions when modifying functioning scripts to retain working versions. Any modifications to the script samples included here, or any scripts you create, are considered customization, which is not typically covered by Quest Support.

Note: Protected machines use the 'exec' shell command to launch the script. You can indicate which interpreter should run the script by defining that information in the first line of the script. If you do not specify the interpreter, the default shell interprets the script. If you choose something other than the default shell, you must ensure that the specified interpreter is available on all protected machines. All sample shell scripts in this document are tested and run successfully as Bourne shell or Bash scripts.

The sample scripts for protected machines include:

PreTransferScript.sh

The PreTransferScript is run on the protected Linux machine immediately before the backup snapshot transfer begins.

Note: For clarification on when pre and post scripts are run, see .Using Bourne shell and Bash scripting with Rapid Recovery.

The following script stores the values from input parameters in PreTransferScriptResult.txt, which is stored in the root home directory.

Sample PreTransferScript

```
#!/bin/bash
 echo  "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_
VolumeNames
 TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_
ShadowCopyType
 TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
 TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_
ForceBaseImage
 TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_
IsLogTruncation
 TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_
LatestEpochSeenByCore"  >  ~/PreTransferScriptResult.txt
 exit  0
```

PostTransferScript.sh

The PostTransferScript is run on the protected Linux machine after the backup snapshot process has fully completed.

Note: For clarification on when pre and post scripts are run, see .Using Bourne shell and Bash scripting with Rapid Recovery.

The following script stores the values from input parameters in PostTransferScriptResult.txt, which is stored in the root home directory.

Sample PostTransferScript

```
#!/bin/bash
 echo  "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_
VolumeNames
 TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_
ShadowCopyType
 TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
 TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_
ForceBaseImage
 TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_
IsLogTruncation
 TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_
LatestEpochSeenByCore"  >  ~/PostTransferScriptResult.txt
 exit  0
```

PreSnapshotScript.sh

The PreSnapshotScript is run on the protected Linux machine after preparation but before data is read from the original device when capturing a snapshot. This script does not receive parameters from the protected machine.
Note: For clarification on when pre and post scripts are run, see .Using Bourne shell and Bash scripting with Rapid Recovery.
The following script returns the time that the script completed on the machine in hours, minutes, and seconds, based on the system time of the Core. This information is logged in PreSnapshotScriptResult.txt, which is stored in the root home directory.

Sample PreSnapshotScript

```
#!/bin/bash
 echo "`date +%H:%M:%S` PreSnapshot script has been executed." >
~/PreSnapshotScriptResult.txt
 exit 0
```

PostSnapshotScript.sh

The PostSnapshotScript is run on the protected Linux machine after data is read from the original device when capturing a snapshot, but before data is read from the copied device. This script does not receive parameters from the protected machine.
Note: For clarification on when pre and post scripts are run, see .Using Bourne shell and Bash scripting with Rapid Recovery.
The following script returns the time that the script completed on the machine in hours, minutes, and seconds, based on the system time of the Core. This information is logged in PostSnapshotScriptResult.txt, which is stored in the root home directory.

Sample PostSnapshotScript

```
#!/bin/bash
 echo "`date +%H:%M:%S` PostSnapshot script has been executed." >
~/PostSnapshotScriptResult.txt
 exit 0
```

PostExportScript.sh

The PostExportScript is run on the exported Linux machine after the virtual export is complete. This script does not receive parameters from the protected machine.
Note: The original machine from which the VM was cloned should be powered off before starting the VM.
The following script returns the start time of the exported virtual machine in hours, minutes, and seconds, based on the system time of the Core. This information is logged in PostExportScriptResult.txt, which is stored in the root home directory.

Sample PostExportScript

```
#!/bin/bash
echo
"`date +%H:%M:%S` Start time of the machine. This indicates that virtual export has
```

```
been completed and machine is active." > ~/PostExportScriptResult.txt
exit 0
```

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product