

Rapid Recovery 6.0 sur appliances DL

Guide d'utilisation

Remarques, précautions et avertissements

 **REMARQUE :** Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre ordinateur.

 **PRÉCAUTION :** Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

 **AVERTISSEMENT :** Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

© 2016 Dell Inc. Tous droits réservés. Ce produit est protégé par les lois sur les droits d'auteur et la propriété intellectuelle des États-Unis et des autres pays. Dell et le logo Dell sont des marques de Dell Inc. aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et tous les noms de produits mentionnés dans ce document peuvent être des marques de leurs sociétés respectives.

Table des matières

1 Présentation de l'appliance DL.....	11
Architecture de déploiement.....	11
Smart Agent.....	13
Core d'appliance DL.....	13
Processus d'instantané.....	14
Réplication de site de récupération après sinistre ou fournisseur de services.....	14
Restauration.....	14
Caractéristiques du produit	14
Comprendre les référentiels.....	15
Déduplication sous Rapid Recovery.....	16
Comprendre les clés de clés de chiffrement.....	17
Réplication avec Rapid Recovery.....	18
Rétention et archivage.....	21
Virtualisation et cloud.....	22
Alertes et gestion des événements.....	23
Portail de licences.....	23
Console Web.....	23
API de gestion des services.....	23
2 Travailler avec l'Appliance DL Core.....	24
Compréhension de la console Core Rapid Recovery.....	24
Accès à la console Core Rapid Recovery.....	24
Comprendre le guide de démarrage rapide.....	24
Navigation vers Rapid Recovery Core Console.....	26
Affichage du menu Machines protégées.....	30
Affichage des machines répliquées dans le menu de navigation.....	35
Affichage du menu Points de restauration uniquement.....	35
Affichage du menu Groupes personnalisés.....	36
Utilisation de la boîte de dialogue Erreur.....	36
Paramètres du Core.....	36
Paramètres du Core de Rapid Recovery.....	36
Sauvegarde et restauration des paramètres du Core.....	66
Outils au niveau du Core.....	68
Schéma de configuration du core	70
Logithèques.....	70
Gestion d'une logithèque DVM.....	71
Gestion de la sécurité	83
Application ou retrait du chiffrement d'une machine protégée.....	83
Gérer les clés de chiffrement.....	86
Gestion des comptes Cloud.....	94
À propos des comptes Cloud.....	94

Ajouter un compte cloud.....	94
Modifier un compte Cloud.....	95
Configurer les paramètres d'un compte cloud.....	96
Suppression d'un compte Cloud.....	96
Archivage.....	96
Description des archives.....	97
Création d'une archive.....	97
Modification d'une archive planifiée.....	100
Suspension ou reprise de l'archivage planifié.....	101
Tâche d'archivage forcée.....	102
Vérification d'une archive.....	102
Attachement d'une archive.....	103
Importer une archive.....	104
Événements.....	106
Événements de la Rapid Recovery.....	106
Affichage des événements à l'aide des tâches, des alertes et du journal.....	107
Comprendre les notifications par courrier électronique.....	110
Modèles de notifications, paramètres SMTP et groupes de notifications pour les événements système....	113
Configurer les groupes de notification.....	113
À propos de la configuration de la réduction des répétitions.....	116
Configurer la rétention des événements.....	117
Rapid Appliance Self Recovery.....	117
Création de la clé USB RASR.....	118
Exécution du RASR.....	118
Utilitaire Local Mount Utility (LMU).....	119
À propos de l'Utilitaire LMU (Local Mount Utility).....	119
Utilisation des Cores Rapid Recovery de l'utilitaire de montage local.....	120
Utilisation de machines protégées dans l'utilitaire Local Mount Utility.....	123
Utiliser la zone de notification de Local Mount Utility.....	126
3 Gestion de l'appliance.....	127
Surveillance de l'état de l'appareil.....	127
Sauvegarde Windows.....	127
État de la sauvegarde.....	128
Stratégie de sauvegarde Windows.....	129
Provisionnement du stockage.....	130
Supprimer une allocation d'espace pour un disque virtuel.....	131
Utilitaire de récupération et de mise à jour.....	131
Mettre à niveau votre appliance.....	132
Réparation de votre appliance.....	132
4 Protection des stations de travail et des serveurs	134
Protection des machines.....	134
À propos de la protection des machines avec Rapid Recovery	134
Accéder aux diagnostics des machines protégées.....	198
Gérer les machines.....	200

Supprimer une machine.....	200
Annuler des opérations sur une machine.....	201
Afficher les informations sur la licence d'une machine.....	201
VM export (Exportation NFS).....	201
À propos de l'exportation vers des machines virtuelles avec Rapid Recovery.....	202
Gestion des exportations.....	214
Gestion des données vieillissantes.....	228
À propos de la conservation et de l'archivage des données de Rapid Recovery.....	228
Gestion des stratégies de conservation.....	229
Réplication.....	234
Réplication avec Rapid Recovery.....	234
Points de restauration en chaîne et orphelins.....	238
Lorsque la réplication commence.....	239
Détermination de vos besoins et votre stratégie d'implantation.....	239
Considérations sur les performances pour le transfert de données répliquées.....	241
Réplication vers un core cible autogéré.....	243
Affichage des répliqués entrants et sortants.....	246
Configuration d'une réplication.....	248
Réplication vers un Core cible tiers.....	248
Ajouter une machine à une réplication existante.....	253
Consommation du disque source sur un Core cible.....	254
Gestion des paramètres de réplication.....	256
Suppression d'une réplication.....	263
Restaurer des données répliquées.....	265
5 Restauration de données.....	266
Gestion de la récupération	266
Instantanés et points de restauration.....	266
Gérer les instantanés et les points de restauration.....	266
Affichage de la page des points de restauration d'une machine protégée.....	266
Monter un point de restauration.....	269
Démonter des points de restauration.....	270
Utiliser des points de restauration Linux.....	270
Forcer un instantané.....	272
Supprimer des points de restauration.....	273
Supprimer une chaîne de points de restauration orphelins.....	274
Migration de points de restauration vers une logithèque différente.....	274
Restaurer des données.....	275
À propos de la restauration de données avec Rapid Recovery.....	275
Compréhension des Live Recovery.....	275
Restaurer des données à partir de points de restauration.....	276
À propos de la restauration de volumes à partir d'un point de restauration.....	277
Restauration de clusters et de nœuds de cluster.....	280
Restauration depuis une archive attachée.....	281
Comprendre la restauration Bare Metal Restore pour les machines Windows.....	282
Restauration BMR (Bare Metal Restore) pour les machines Windows.....	282

Comprendre la création du CD d'amorçage pour les machines Windows.....	287
Utilisation de l'Universal Recovery Console pour une restauration BMR.....	290
Effectuer une restauration Bare Metal Restore de machines Linux.....	298
Vérification d'une restauration bare metal restore.....	307
6 Générer et afficher des rapports.....	312
À propos des rapports Rapid Recovery.....	312
Génération d'un rapport depuis la console Core.....	313
Gestion des rapports planifiés depuis la console Core.....	316
Utilisation du menu Rapports.....	321
Utilisation de la barre d'outils Rapports.....	321
Comprendre le rapport de tâche.....	323
Présentation du rapport récapitulatif des tâches.....	323
Comprendre le rapport des échecs.....	324
Comprendre le rapport récapitulatif.....	325
Comprendre le rapport de logithèque.....	326
Central Management Console.....	326
Compréhension de la Rapid Recovery Central Management Console.....	327
Configuration de la Rapid Recovery Central Management Console.....	328
Comprendre les rapports de noyau de la Console de gestion centrale.....	332
7 Comprendre l'utilitaire Command Line Management Rapid Recovery.....	333
Commandes.....	334
Archivage.....	335
CancelActiveJobs.....	336
CheckRepository.....	337
CreateArchiveRepository.....	338
CreateBootCD.....	340
CreateRepository.....	341
DeleteRepository.....	342
Dismount.....	343
DismountArchiveRepository.....	344
EditEsxServer.....	345
Forcer.....	346
ForceAttach.....	347
ForceChecksum.....	348
ForceLogTruncation.....	349
ForceMount.....	350
ForceReplication.....	351
ForceRollup.....	351
ForceVirtualStandby.....	352
Aide.....	353
List.....	354
Montage.....	356
MountArchiveRepository.....	357
NewCloudAccount.....	358

OpenDvmRepository.....	359
Suspendre.....	360
Protect.....	362
ProtectCluster.....	363
ProtectEsxServer.....	364
RemoveAgent.....	365
RemoveArchiveRepository.....	366
RemovePoints.....	367
RemoveScheduledArchive.....	368
RemoveVirtualStandby.....	369
Replicate.....	369
Réplication.....	371
RestoreAgent.....	373
RestoreArchive.....	374
RestoreUrc.....	375
Reprendre.....	377
SeedDrive.....	378
StartExport.....	379
UpdateRepository.....	382
Version.....	383
VirtualStandby.....	384
Localisation.....	386
Annexe A : Références de la Core Console.....	387
Affichage de l'interface utilisateur de la Core Console.....	387
Barre des boutons.....	388
Barre d'icônes.....	390
Menu de navigation gauche.....	391
Affichage du volet Machines protégées.....	394
Affichage des événements pour une machine protégée.....	397
Affichage du menu Plus pour une machine protégée.....	398
Annexe B : Description du module PowerShell de Rapid Recovery.....	400
Prérequis pour l'utilisation de PowerShell.....	401
powershell.exe.config.....	401
Lancement de PowerShell et importation du module.....	401
Utilisation de commandes et de cmdlets.....	401
Aide et exemples pour les cmdlets.....	402
Cmdlets PowerShell de Rapid Recovery.....	402
Edit-EsxiVirtualStandby.....	405
Edit-HyperVVirtualStandby.....	406
Edit-ScheduledArchive.....	408
Edit-VBVirtualStandby.....	409
Edit-VMVirtualStandby.....	411
Get-ActiveJobs.....	412
Get-Clusters.....	414
Get-CompletedJobs.....	414

Get-ExchangeMailStores.....	416
Get-Failed.....	416
Get-FailedJobs.....	417
Get-Mounts.....	419
Get-Passed.....	420
Get-ProtectedServers.....	420
Get-ProtectionGroups.....	421
Get-QueuedJobs.....	422
Get-RecoveryPoints.....	423
Get-ReplicatedServers.....	424
Get-Repositories.....	425
Get-ScheduledArchives.....	426
Get-SqlDatabases.....	427
Get-UnprotectedVolumes.....	428
Get-VirtualizedServers.....	429
Get-Volumes.....	429
New-Base.....	430
New-CloudAccount.....	431
New-EncryptionKey.....	433
New-EsxiVirtualStandby.....	434
New-HyperVVirtualStandby.....	435
New-Mount.....	437
Resume-Replication.....	438
New-Repository.....	439
New-ScheduledArchive.....	440
New-Snapshot.....	443
New-VBVirtualStandby.....	443
New-VMVirtualStandby.....	445
Push-Replication.....	446
Push-Rollup.....	447
Remove-Agent.....	448
Remove-Mount.....	449
Remove-Mounts.....	450
Remove-RecoveryPoints.....	451
Remove-Repository.....	452
Remove-ScheduledArchive.....	453
Remove-VirtualStandby.....	454
Resume-Replication.....	455
Resume-Snapshot.....	456
Resume-VirtualStandby.....	457
Resume-VMExport.....	458
Start-Archive.....	459
Start-AttachabilityCheck.....	460
Start-ChecksumCheck.....	461
Start-EsxiExport.....	462

Start-HypervExport.....	464
Start-LogTruncation.....	465
Start-MountabilityCheck.....	466
Start-Protect.....	467
Start-ProtectCluster.....	468
Start-RepositoryCheck.....	469
Start-RestoreArchive.....	470
Start-ScheduledArchive.....	472
Start-VBExport.....	472
Start-VirtualStandby.....	474
Start-VMExport.....	475
Stop-ActiveJobs.....	477
Suspend-Replication.....	478
Suspend-RepositoryActivity.....	479
Suspend-ScheduledArchive.....	480
Suspend-Snapshot.....	481
Suspend-VirtualStandby.....	482
Suspend-VMExport.....	483
Update-Repository.....	483
Localisation.....	484
Qualificateurs.....	485
Annexe C : Extension des tâches Rapid Recovery avec des scripts.....	486
Utilisation des scripts PowerShell dans Rapid Recovery.....	486
Prérequis pour l'exécution de scripts PowerShell.....	487
powershell.exe.config.....	487
Test des scripts PowerShell.....	487
Localisation.....	487
Qualificateurs.....	487
Paramètres d'entrée pour les scripts PowerShell.....	488
AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents).....	488
AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer).....	489
BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs).....	490
ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks).....	491
DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange).....	491
ExportJobRequest (namespace Replay.Core.Contracts.Export).....	491
NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql).....	492
RollupJobRequest (namespace Replay.Core.Contracts.Rollup).....	492
TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer).....	492
TransferJobRequest (namespace Replay.Core.Contracts.Transfer).....	492
TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	494
TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution).....	494
TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution).....	496
VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization).....	496
VolumeImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints).....	497
VolumeName (namespace Replay.Common.Contracts.Metadata.Storage).....	497

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage).....	497
VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer).....	498
VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer).....	498
Exemples de scripts PowerShell.....	498
PreTransferScript.ps1.....	498
PostTransferScript.ps1.....	499
PreExportScript.ps1.....	499
PostExportScript.ps1.....	500
PreNightlyJobScript.ps1.....	500
PostNightlyJobScript.ps1.....	502
Utilisation des scripts Bourne Shell dans Rapid Recovery.....	503
Prérequis pour l'exécution de scripts Bourne Shell.....	504
Paramètres des scripts de transfert et de post-transfert pris en charge.....	504
Test des scripts Bourne Shell.....	505
Paramètres d'entrée pour les scripts Bourne Shell.....	505
TransferPrescriptParameters_VolumeNames.....	505
TransferPostscriptParameter.....	506
Exemples de scripts Bourne Shell.....	506
PreTransferScript.sh.....	507
PostTransferScript.sh.....	507
PostExportScript.sh.....	507
Annexe D : Les API Rapid Recovery.....	509
Public visé.....	509
Utilisation des API REST Rapid Recovery.....	509
Téléchargement et affichage des API du Core et de l'Agent.....	509
Lectures complémentaires conseillées.....	511
À propos de Dell.....	512
Contacter Dell.....	512
Ressources du support technique.....	512
Glossaire.....	513

Présentation de l'appliance DL

L'appliance DL avec le logiciel Rapid Recovery est une solution de sauvegarde, de réplication et de récupération qui offre des objectifs de durée des restauration et de points de restauration proches de zéro. Rapid Recovery offre une protection des données, une reprise après sinistre, une migration des données et une gestion de données. Vous avez la possibilité d'effectuer des restaurations sans système d'exploitation (Bare Metal Restore) vers des matériels similaires ou non, et vous pouvez restaurer des sauvegardes vers des machines physiques ou virtuelles, quelle que soit l'origine. Avec Rapid Recovery vous pouvez répliquer vers une ou plusieurs cibles pour un surcroît de redondance et de sécurité.

Votre appliance définit une nouvelle norme pour la protection unifiée des données en combinant la sauvegarde, la réplication et la restauration en une seule et même solution conçue pour être la méthode de sauvegarde la plus rapide et la plus fiable pour la protection de machines virtuelles (VM) et physiques et des environnements cloud. Votre appliance peut gérer jusqu'à des pétaoctets de données grâce à ses fonctionnalités intégrées de déduplication globale intégrée, de compression, de chiffrement et de réplication vers n'importe quelle infrastructure de cloud privé ou public. Les applications et données des serveurs peuvent être restaurées en quelques minutes pour la conservation des données et la conformité.

Votre appliance prend en charge les environnements à plusieurs hyperviseurs sur les clouds privés et publics VMware vSphere et Microsoft Hyper-V.

Rapid Recovery offre les avantages suivants :

- **Flexibilité.** Vous pouvez effectuer Universal Recovery vers de multiples plateformes : restauration de physique à virtuel, de virtuel à physique, de virtuel à virtuel et de physique à physique.
- **Intégration au cloud.** Vous pouvez archiver et répliquer les données vers le cloud, en utilisant des fournisseurs de stockage cloud prenant en charge des plateformes aussi bien propriétaires qu'open source.
- **Déduplication intelligente.** Vous pouvez réduire les besoins en stockage en ne stockant les données qu'une seule fois, et en le référençant par la suite (une fois par référentiel ou par domaine de chiffrement).
- **Récupération instantanée.** Notre fonction Live Recovery vous permet d'accéder en premier aux données critiques, alors que les autres opérations de restauration s'effectuent en parallèle.
- **Récupération au niveau fichiers.** Vous pouvez récupérer les données au niveau des fichiers sur site, depuis un emplacement distant ou à partir du cloud.
- **Prise en charge de la virtualisation.** La prise en charge améliorée de la virtualisation inclut la protection sans agent et l'identification automatique pour VMware® ESXi™ 5 et plus récent, et l'exportation vers des volumes partagés en cluster Microsoft® Hyper-V®.

Pour plus d'informations sur Rapid Recovery, vous pouvez vous reporter aux ressources suivantes.

- Le site web du support produit Dell Rapid Recovery (<https://support.software.dell.com/rapid-recovery/>).
- Le site web de documentation (<https://support.software.dell.com/rapid-recovery/release-notes-guides/>) et <http://www.dell.com/support/home/>.

Sujets :

- [Architecture de déploiement](#)
- [Caractéristiques du produit](#)

Architecture de déploiement

Votre appliance est un produit de sauvegarde et de restauration évolutif qui se déploie simplement au sein de l'entreprise ou en tant que service distribué par un fournisseur de services gérés. Le type du déploiement dépend de la taille et des exigences du client. La préparation

au déploiement de votre appliance inclut la planification de la topologie de stockage du réseau, l'infrastructure de restauration du matériel du core après sinistre ainsi que la sécurité.

L'architecture de déploiement est constituée de composants locaux et distants. Les composants distants peuvent être facultatifs pour les environnements qui n'ont pas besoin d'utiliser un site de récupération après sinistre ou un fournisseur de services gérés pour effectuer la restauration hors site. Un déploiement local de base comprend un serveur de sauvegarde appelé le Core, et une ou plusieurs machines protégées. Le composant hors site est activé à l'aide de la réplication qui fournit des fonctionnalités de restauration complète sur le site DR. Le Core utilise des images de base et des instantanés incrémentiels pour compiler les points de restauration des machines protégées.

De plus, votre appliance reconnaît les applications car elle peut détecter la présence de Microsoft Exchange et de SQL, ainsi que de leurs bases de données et fichiers journaux respectifs, puis regrouper automatiquement ces volumes avec dépendance pour une protection exhaustive et une restauration efficace. Cela garantit que vos sauvegardes ne sont jamais incomplètes lorsque vous effectuez des restaurations. Les sauvegardes sont réalisées à l'aide d'instantanés de niveau bloc avec reconnaissance de l'application. Votre appliance peut également tronquer les journaux des serveurs Microsoft Exchange et SQL Server protégés.

Le diagramme suivant illustre un déploiement simple. Dans ce diagramme, le logiciel des agents AppAssure est installé sur des machines comme le serveur de fichiers, le serveur d'e-mail, le serveur de base de données ou des machines virtuelles, et elles se connectent à un seul Core qui les protège et joue également le rôle de référentiel central. Le portail de licences gère les abonnements aux licences, les groupes et les utilisateurs des machines et des cores de votre environnement. Le portail de licences permet aux utilisateurs de se connecter, d'activer des comptes, de télécharger des logiciels et de déployer des machines et des cores protégés en fonction des licences dont vous disposez pour votre environnement.

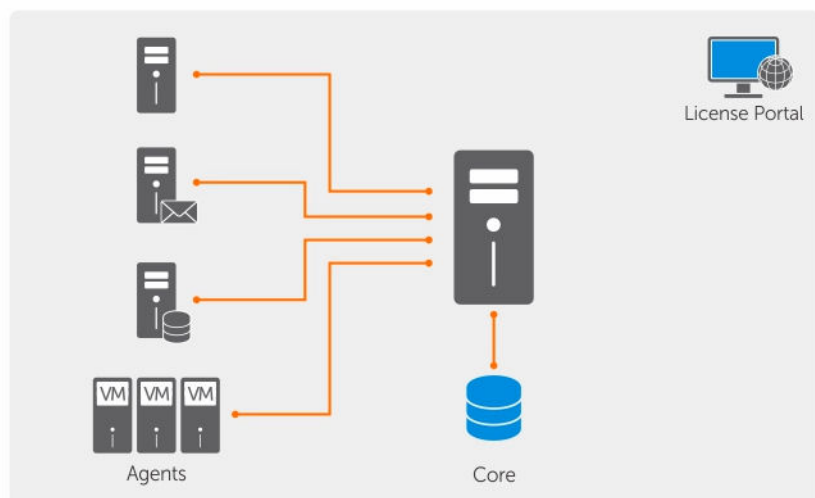


Figure 1. Architecture de déploiement de base

Vous pouvez également déployer plusieurs Cores, comme le montre le diagramme suivant. Une console centrale gère plusieurs Cores.

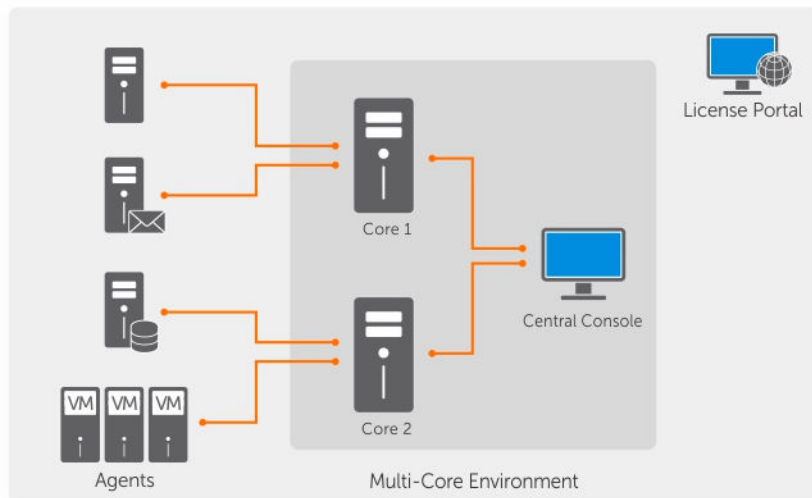


Figure 2. Architecture de déploiement avec plusieurs Cores

Smart Agent

Smart Agent effectue le suivi des modifications apportées aux blocs du volume de disques, puis prend un instantané des blocs modifiés selon l'intervalle de protection prédéfini. L'approche qui consiste à créer systématiquement des instantanés incrémentiels de niveau bloc empêche la copie répétée des mêmes données vers le core depuis la machine protégée. Rapid Recovery Smart Agent est installé sur les machines protégées par le core Rapid Recovery.

Smart Agent reconnaît les applications et détecte le type de l'application qui est installée ainsi que l'emplacement des données. Il regroupe automatiquement les volumes de données avec dépendance, comme les bases de données, puis les journalise pour assurer une protection efficace et une restauration rapide. Une fois configuré, le logiciel Rapid Recovery Agent utilise une technologie intelligente pour effectuer le suivi des blocs modifiés sur les volumes de disques protégés. Lorsque l'instantané est prêt, il est rapidement transféré au core à l'aide de connexions socket multithread intelligentes. Pour préserver la bande passante du CPU et la mémoire sur les machines protégées, Smart Agent ne chiffre ni ne déduplique les données à la source et les machines protégées sont couplées à un core à des fins de protection.

Core d'appliance DL

Le core est le composant central de l'architecture de déploiement. Il stocke et gère toutes les sauvegardes de la machine, et fournit des services de base de sauvegarde, récupération et conservation, réplication, archivage et gestion. Le Core est un ordinateur autonome adressable sur le réseau, exécutant une 64 bits de Microsoft Windows. Votre appliance effectue en ligne sur la base de la cible les opérations suivantes : compression, chiffrement et déduplication des données reçues de la machine protégée. Le core stocke alors les sauvegardes des instantanés dans des référentiels comme le SAN (Storage Area Network) ou le DAS (Direct Attached Storage).

Le référentiel peut également résider sur un stockage interne au sein du core. Pour gérer le core, il suffit d'accéder à l'adresse URL suivante à partir d'un navigateur web : **<https://NOMCORE:8006/apprecovery/admin>**. En interne, tous les services du core sont accessibles par l'intermédiaire des API REST. Vous pouvez accéder aux services du core depuis le core ou directement via Internet à partir de toute application pouvant envoyer une demande HTTP/HTTPS et recevoir une réponse HTTP/HTTPS. Toutes les opérations API s'effectuent via SSL et sont authentifiées mutuellement à l'aide de certificats X.509 v3.

Chaque core est associé à d'autres cores pour la réplication.

Processus d'instantané

Un instantané correspond à une image de base transférée vers le core depuis une machine protégée. Les instantanés capturent et stockent l'état d'un volume de disques à un moment donné alors que l'application qui génère les données est toujours en cours d'exécution. Dans Rapid Recovery, vous pouvez forcer un instantané, suspendre temporairement les instantanés et afficher la liste des points de restauration actuels présents dans le référentiel (et les supprimer, si nécessaire). Les points de restauration servent à restaurer des machines protégées ou à effectuer un montage sur un système de fichiers local. Les instantanés sont capturés par Rapid Recovery au niveau du bloc et tiennent compte des applications. Cela signifie que la création d'un instantané ne peut se faire que lorsque toutes les transactions ouvertes et tous les journaux de transaction de cumul ouverts sont terminés et que les caches sont vidés sur le disque.

Rapid Recovery utilise un pilote de filtre de volume de bas niveau, qui s'attache aux volumes montés et suit toutes les modifications intervenant au niveau bloc pour le prochain instantané prévu. Microsoft Volume Shadow Services (VSS) est utilisé pour faciliter la prise d'instantanés d'applications crash consistant.

Réplication de site de récupération après sinistre ou fournisseur de services

Le processus de réplication exige une relation source-cible associées entre deux cores. Le core source copie les points de restauration des machines protégées, puis les transmet de façon asynchrone et continue à un core cible dans un site de récupération après sinistre distant. L'emplacement hors site peut être un centre de données (core auto géré) appartenant à une société ou un emplacement ou environnement cloud d'un MSP (Managed Service Provider - Fournisseur de services tiers) géré par un tiers. Lors d'une réplication à un MSP, utilisez des flux de travail intégrés qui vous permettent de demander des connexion et de recevoir des notifications de commentaires automatiques. Pour le transfert initial de données, effectuez l'amorçage de données à l'aide d'un support externe; cela est utile pour les ensembles de données importants ou les sites dont les liens sont lents.

En cas de panne grave, votre appliance prend en charge le basculement et la restauration automatique dans les environnements répliqués. En cas de panne compréhensive, le core cible du site secondaire peut restaurer des instances à partir d'agents répliqués et commencer immédiatement la protection sur les machines basculées. Suite à la restauration du site principal, le core répliqué peut restaurer automatiquement des données à partir des instances restaurées sur les machines protégées au site principal.

Restauration

La restauration peut être réalisée sur le site local ou sur le site à distance répliqué. Une fois que le déploiement est stable avec une protection locale et une réplication optionnelle, le Core permet de réaliser une restauration à l'aide de Verified Recovery, Universal Recovery ou Live Recovery.

Caractéristiques du produit

Vous pouvez gérer la protection et la restauration des données essentielles à l'aide des éléments suivants :

- [Référentiel](#)
- [Déduplication sous Rapid Recovery](#)
- [Chiffrement](#)
- [Réplication](#)
- [Conservation et archivage](#)
- [Virtualisation et cloud](#)
- [Alertes et gestion des événements](#)
- [Portail de licences](#)

- [Console web](#)
- [API de gestion des services](#)

Comprendre les référentiels

Un référentiel est un emplacement central dans lequel sont stockées et gérées les données des instantanés de sauvegarde capturés à partir de vos stations de travail et vos serveurs protégés. Les données sont enregistrées dans un référentiel sous la forme de points de restauration.

Un référentiel peut résider sur plusieurs sortes de stockage : SAN (Storage Area Network), DAS (Direct Attached Storage) ou NAS (Network Attached Storage).

REMARQUE : Stockez les référentiels du core Rapid Recovery sur des périphériques de stockage principaux. La vitesse du volume de stockage est le facteur capital. Les périphériques de stockage d'archives comme Data Domain ne sont pas pris en charge en raison de leurs performances limitées. De même, ne stockez pas les référentiels sur des serveurs de fichiers NAS dans le cloud, car ces périphériques sont limités en termes de performances lorsqu'ils sont utilisés en tant que stockage principal.

Le DAS offre le plus haut débit de bande passante de données et l'accès le plus rapide, et il est facile à mettre en œuvre. Pour des résultats optimaux, utilisez DAS avec un stockage RAID 6. Pour plus d'informations, reportez-vous à l'[article 118153 de la base de connaissances Dell](#), "Options de référentiel zone: Direct Attached Storage, Storage Area Network ou Network Attached Storage."

L'emplacement de stockage d'un référentiel doit toujours être dans un sous-répertoire que vous spécifiez (par exemple, **E:\Repository**) et jamais à la racine d'un volume (par exemple, **E:**).

Le format de référentiel Rapid Recovery utilise DVM (Deduplication Volume Manager). Les référentiels DVM prennent en charge plusieurs volumes, jusqu'à 255 référentiels sur un même core, et l'utilisation d'extensions. Vous pouvez créer des référentiels DVM uniquement sur des machines Windows. Vous pouvez utiliser ce type de référentiel dans le cadre de nouvelles installations de Rapid Recovery. Vous pouvez spécifier la taille d'un référentiel DVM au moment de sa création et vous pouvez lui ajouter ultérieurement des extensions.

Caractéristiques et attributs des référentiels DVM :

- Prend en charge les archives et les points de restauration Rapid Recovery 6.x
- Prend en charge des emplacements de stockage sous Windows uniquement. Le volume du référentiel peut être local (sur un stockage relié au serveur core) ou sur dans emplacement de stockage sur un emplacement partagé CIFS (Common Internet File System).
- Types de stockage pris en charge : SAN (Storage Area Network), DAS (Direct Attached Storage) ou NAS (Network Attached Storage).
- Nécessite 8 Go de RAM, de préférence ECC
- Nécessite un processeur quadricœur sur la machine Core (cette exigence de longue date est maintenant appliquée)
- Prend en charge plusieurs référentiels DVM par hôte
- Aucun service supplémentaire n'est requis ; le référentiel DVM les services natifs du core pour communiquer avec ce dernier et pour le suivi des événements
- Chaque référentiel DVM prend en charge jusqu'à 4096 extensions (également appelées emplacements de stockage)
- Taille fixe. Le référentiel DVM vous demande de spécifier sa taille sur un volume. La taille que vous spécifiez ne peut pas excéder celle du volume. Chaque volume que vous définissez en tant qu'emplacement de stockage doit disposer d'un minimum de 1 Go d'espace libre.
- L'emplacement de stockage du référentiel peut être un disque simple ou dynamique, la vitesse étant le facteur le plus important
- Crée et gère dans la console Core des clés de chiffrement standard (chiffrement basé sur le core)
- Déduplique les données sur l'ensemble du référentiel (ou sur des domaines de chiffrement au sein de chaque référentiel, si des clés de chiffrement sont utilisées)
- Utilise un cache de déduplication DVM dédié et redimensionnable, avec emplacement de stockage configurable dans les paramètres du core
- Optimisé pour l'écriture des données, le stockage des données d'instantané dans un référentiel local pour le core, toutes les données étant traitées via le core

- Ne peut être renommé une fois créé
- Il est possible de créer de nouveaux référentiels à l'aide d'API REST, de l'utilitaire Command Line Management Utility (cmdutil.exe) Rapid Recovery ou du cmdlet Windows PowerShell®

Lorsque vous créez un référentiel DVM, le core Rapid Recovery pré-alloue à l'emplacement spécifié l'espace de stockage requis pour les données et les métadonnées. La taille minimale du référentiel DVM est de 1 Go, qui est en général pratiquement insuffisante, sauf pour des tests.

La déduplication DVM nécessitant un cache principal et un cache secondaire, assurez-vous que la quantité d'espace de stockage que vous réservez est le double de la taille de votre cache de déduplication. Par exemple, si vous avez sur le core 1,5 Go réservé dans les paramètres du cache de déduplication DVM, réservez 3 Go sur le volume de cache. Le chemin d'installation par défaut pour le cache est sur le lecteur C. Pour plus d'informations, reportez-vous à [Compréhension du cache de déduplication et des emplacements de stockage](#).

Vous pouvez créer plusieurs référentiels indépendants associés à un même core, jusqu'à 255 référentiels DVM. Les référentiels peuvent s'étendre sur des stockages de technologies différentes.

Vous pouvez augmenter la taille d'un référentiel DVM en lui ajoutant de nouvelles extensions ou de nouvelles spécifications de fichiers. Un référentiel étendu peut contenir un maximum de 4096 extensions qui peuvent s'étendre sur des stockages de technologies différentes.

Pour plus d'informations sur l'utilisation de référentiels DVM, reportez-vous à [Gestion d'une logithèque DVM](#).

Déduplication sous Rapid Recovery

La déduplication est une technique de compression des données qui réduit les exigences de stockage et la charge du réseau. Le processus implique le stockage physique des blocs de données uniques une seule fois sur le disque. Dans Rapid Recovery, lorsqu'un bloc de données unique se produit une seconde fois dans une logithèque, au lieu de stocker de nouveau les données, une référence virtuelle aux données est stockée.

La déduplication se produit dans des instantanés de sauvegarde capturés par le Core Rapid Recovery. Les informations de sauvegarde sont dédupliquées au sein d'une même logithèque. Elles ne peuvent pas être dédupliquées à travers plusieurs logithèques.

Rapid Recovery version 6.0.2 utilise la déduplication basée sur la cible pour toutes les logithèques DVM. Dans ce modèle, les informations sont transférées vers la logithèque DVM (la cible), et sont ensuite dédupliquées à partir de la logithèque.

Pour la partie principale, la déduplication a lieu en ligne (pendant le transfert d'informations de sauvegarde).

Pour des gains maximaux, Rapid Recovery offre également maintenant une déduplication qui se produit en tant que la déduplication post-traitement. Le post-traitement est parfois appelé déduplication de transfert. En utilisant ce modèle, les données contenues dans la logithèque sont comparées aux références dans le cache de données du DVM. Si un bloc de données de la logithèque a déjà été enregistré, alors chaque occurrence supplémentaire de ces données est remplacée par un pointeur ou référence aux données.

Ce post-traitement peut vous faire économiser de l'espace sur votre volume de stockage de logithèque, en particulier si le cache de déduplication a été rempli et que le cache a donc été agrandi pour tirer parti des déduplications supplémentaires. Ce type de déduplication a lieu lors de l'exécution d'une tâche d'optimisation de logithèque. Cette fonction est unique aux logithèques DVM, et est également appelée réclamation de bloc dupliqué.

Pour en savoir plus sur la tâche d'optimisation de logithèque, voir [À propos de la tâche d'optimisation de logithèque](#). Pour plus d'informations sur la façon de réaliser cette opération, voir [L'optimisation d'une logithèque DVM](#).

Ainsi, Rapid Recovery tire profit de tous les types de déduplication décrites ici : la déduplication basée sur la cible, la déduplication en ligne, et la déduplication post-traitement.

Pour plus d'informations sur l'emplacement des références vers lesquelles les blocs uniques sont stockés pour les logithèques DVM, voir [Compréhension du cache de déduplication et des emplacements de stockage](#).

Comprendre les clés de clés de chiffrement

Le core Rapid Recovery peut chiffrer les données d'instantanés pour tous les volumes d'un référentiel à l'aide de clés de chiffrement que vous définissez et gérez à partir de la console Core.

Plutôt que de chiffrer la totalité du référentiel, Rapid Recovery vous permet de spécifier une clé de chiffrement pour une ou plusieurs machines protégées un même core Rapid Recovery. Chaque clé de chiffrement active crée un domaine de chiffrement. Il n'y a pas de limite au nombre de clés de chiffrement qu'il est possible de créer sur le core.

Dans un environnement mutualisé (lorsqu'un même core héberge plusieurs domaines de chiffrement), les données sont partitionnées et déduplicuées au sein de chaque domaine de chiffrement. Par conséquent, Dell vous recommande d'utiliser une seule clé de chiffrement pour plusieurs machines protégées si vous souhaitez optimiser les avantages de la déduplication entre un ensemble de machines protégées.

Vous pouvez également partager des clés de chiffrement entre des cores à l'aide de l'une des trois méthodes suivantes. Une méthode consiste à exporter une clé de chiffrement sous forme de fichier sur un core Rapid Recovery et de l'importer dans un autre core. Deuxième méthode : archiver les données sécurisées avec une clé de chiffrement et importer ensuite ces données archivées dans un autre core Rapid Recovery. La troisième méthode, enfin, consiste à répliquer à l'aide d'une clé de chiffrement des points de restauration d'un ordinateur protégé. Après que vous avez répliqué les machines protégées, les clés de chiffrement utilisées sur le core source apparaissent en tant que clés de chiffrement répliquées sur le core cible.

Dans tous les cas, une fois importée, une clé de chiffrement apparaît dans le core à l'état verrouillé. Pour accéder à des données à partir d'une clé de chiffrement verrouillée, vous devez déverrouiller cette clé. Pour plus d'informations sur l'importation, l'exportation, le verrouillage et le déverrouillage de clés de chiffrement, reportez-vous à la rubrique [Gérer les clés de chiffrement](#).

Concepts et points à prendre en considération concernant la sécurité des clés :

- Le chiffrement est réalisé au format AES 256 bits en mode CBC (Cipher Block Chaining), conforme SHA-3.
- La déduplication fonctionne au sein d'un domaine de chiffrement pour assurer la confidentialité
- Le chiffrement n'a aucun effet sur les performances.
- Vous pouvez appliquer une même clé de chiffrement à n'importe quel nombre de machines protégées, mais il n'est possible d'appliquer à une machine protégée qu'une seule clé de chiffrement à la fois.
- Vous pouvez ajouter, retirer, importer, exporter, modifier et supprimer des clés de chiffrement qui sont configurées sur le core Rapid Recovery.

⚠ PRÉCAUTION : Rapid Recovery prend un nouvel instantané chaque fois que vous appliquez une clé de chiffrement à une machine protégée. Un nouvel instantané est également déclenché après que vous avez dissocié une clé de chiffrement d'une machine protégée.

Les clés de chiffrement générées depuis le core Rapid Recovery sont des fichiers texte qui contiennent les quatre paramètres décrits dans le tableau suivant :

Tableau 1. Composants d'une clé de chiffrement

Composant	Description
Nom	Cette valeur est équivalente au nom donné lors de l'ajout d'une clé à la console Core Rapid Recovery.
Clé	Ce paramètre est constitué de 107 caractères anglais alphabétiques, numériques et d'opérateurs mathématiques opérateur, générés de manière aléatoire.
ID (N°)	L'ID de la clé est constitué de 26 caractères anglais en majuscules et minuscules, générés de manière aléatoire.
Commentaire	Le commentaire contient la description qui a été entrée lors de la création de la clé.

Réplication avec Rapid Recovery

Cette section fournit des informations conceptuelles et pratiques pour vous aider à comprendre et à configurer la réplication dans Rapid Recovery.

La **réplication** est un processus qui consiste à copier les points de restauration d'un Core Rapid Recovery vers un autre Core Rapid Recovery afin de les restaurer en cas de sinistre. Ce processus exige une relation d'appariement source-cible entre au moins deux Cores.

Le Core source copie les points de restauration des machines protégées sélectionnées, puis transmet les données d'instantané de manière asynchrone et continue vers le Core cible.

Sauf si vous modifiez son comportement par défaut en définissant une planification de réplication, le Core lance une tâche de réplication immédiatement après chaque instantané de sauvegarde, vérification de somme de contrôle, vérification de la capacité d'attachement ou tâche nocturne. Pour en savoir plus, voir [Planifier la réplication](#).

Pour garantir une protection optimale des données, les administrateurs utilisent généralement un Core cible hébergé sur un site de restauration après sinistre distant. Vous pouvez configurer la réplication sortante vers un centre de données d'entreprise, vers un site de restauration après sinistre distant (à savoir, un Core cible « auto-géré »), vers un fournisseur tiers de services gérés (MSP) ou un fournisseur de stockage Cloud qui héberge des services de sauvegarde et de restauration après sinistre hors site. Lors de la réplication vers un Core cible tiers, vous pouvez utiliser des flux de travail intégrés permettant de demander des connexions et de recevoir des notifications automatiques en retour.

La réplication est gérée en fonction des machines protégées. Toute machine (ou toutes les machines) protégée ou répliquée sur un Core source peut être configurée pour être répliquée vers un Core cible.

Scénarios de réplication possibles :

- **Réplication sur un emplacement local.** Le Core cible est situé dans un centre de données local ou un emplacement sur site, et la réplication est assurée à tout moment. Dans cette configuration, la perte du Core ne peut pas empêcher la restauration.
- **Réplication sur un emplacement hors site.** Le Core cible est situé dans une installation hors site prévue pour la restauration en cas de perte (sinistre).
- **Réplication mutuelle.** Deux centres de données se trouvant à deux emplacements différents contiennent chacun un Core et protègent les machines en se servant réciproquement de sauvegarde hors site en vue d'une restauration après sinistre. Dans ce scénario, chaque Core réplique les machines protégées sur le Core situé dans l'autre centre de données.
- **Réplication hébergée ou en Cloud.** Les partenaires MSP de Rapid Recovery gèrent plusieurs Cores cibles dans un centre de données ou dans un Cloud public. Sur chacun de ces Cores, le partenaire MSP permet à un ou plusieurs clients de répliquer des points de restauration d'un Core source situé sur le site du client vers le Core cible situé sur le site du MSP moyennant des frais.

① | REMARQUE : dans ce scénario, les clients ont uniquement accès à leurs propres données.

Configurations de réplication possibles :

- **Réplication d'un point unique vers un point unique.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core source unique vers un Core cible unique.

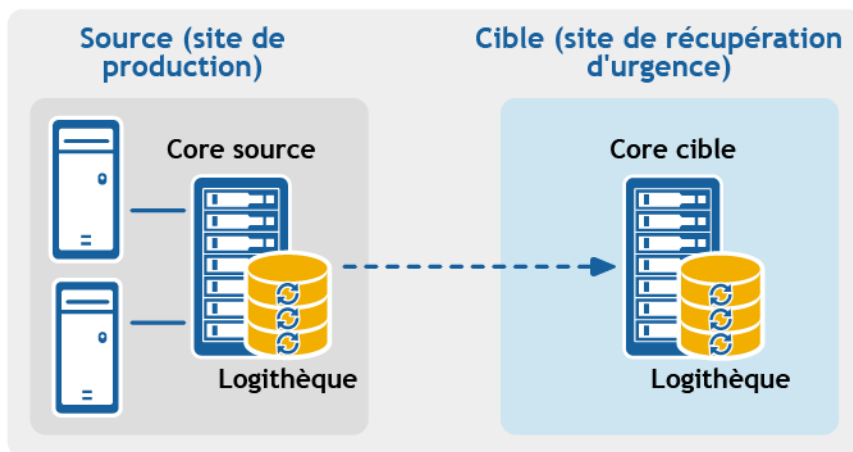


Figure 3. Configuration de réplication d'un point unique vers un point unique

- **Réplication de plusieurs points vers un point unique.** Réplique les machines protégées de plusieurs Cores source vers un Core cible unique.

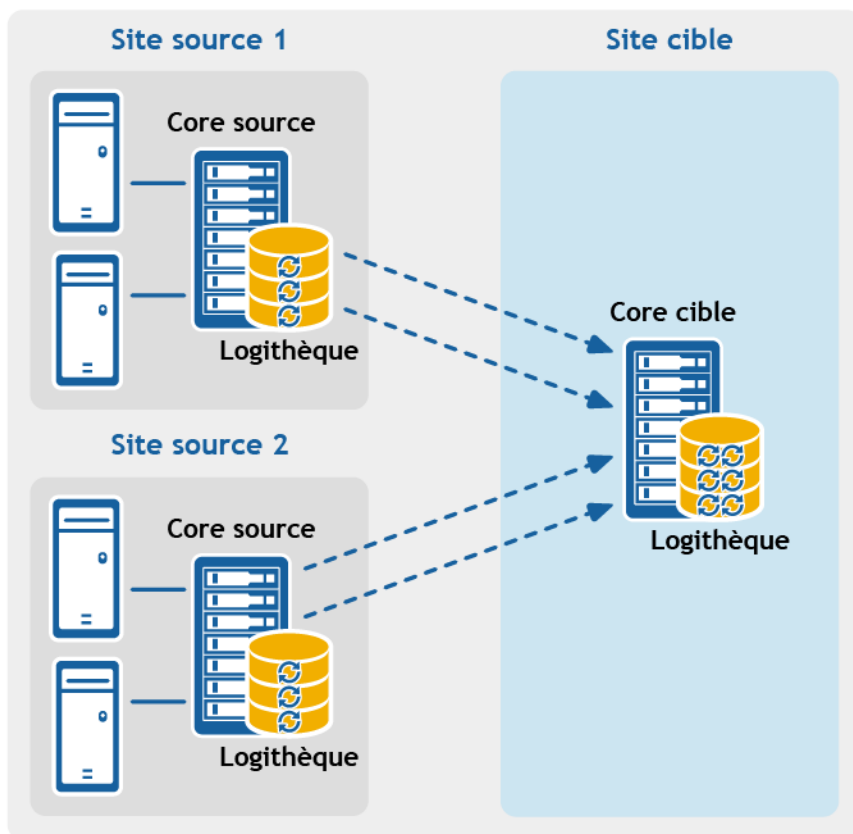


Figure 4. Configuration de réplication de plusieurs points vers un point unique

- **Réplication d'un point unique vers plusieurs points.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core source unique vers plusieurs Cores cibles.

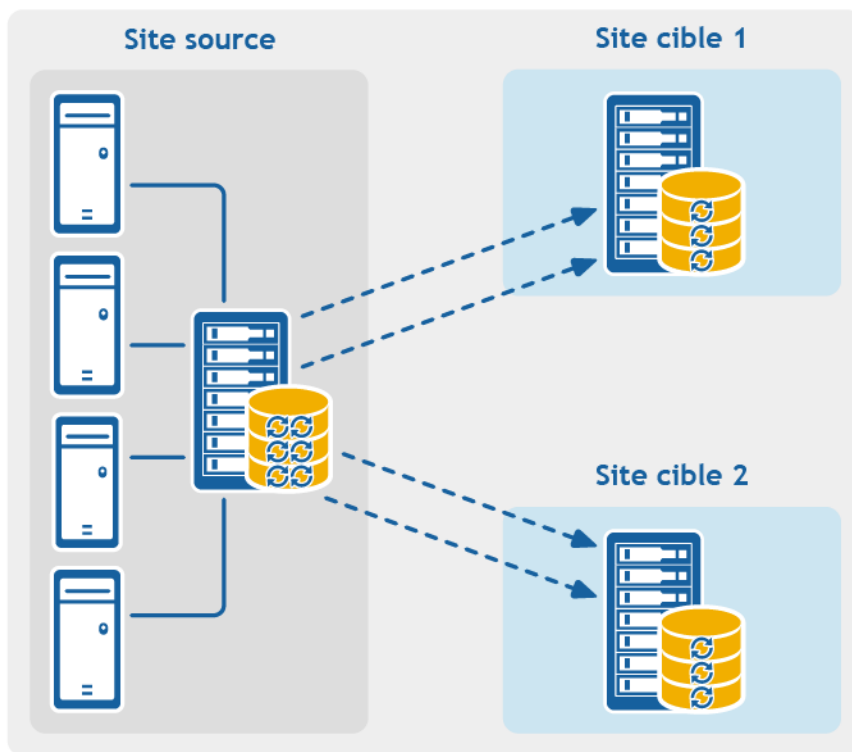


Figure 5. Configuration de réplication d'un point unique vers plusieurs points

- **Réplication multicible.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core cible vers un autre Core cible, offrant ainsi des options de basculement ou de restauration supplémentaires sur le Core répliqué.

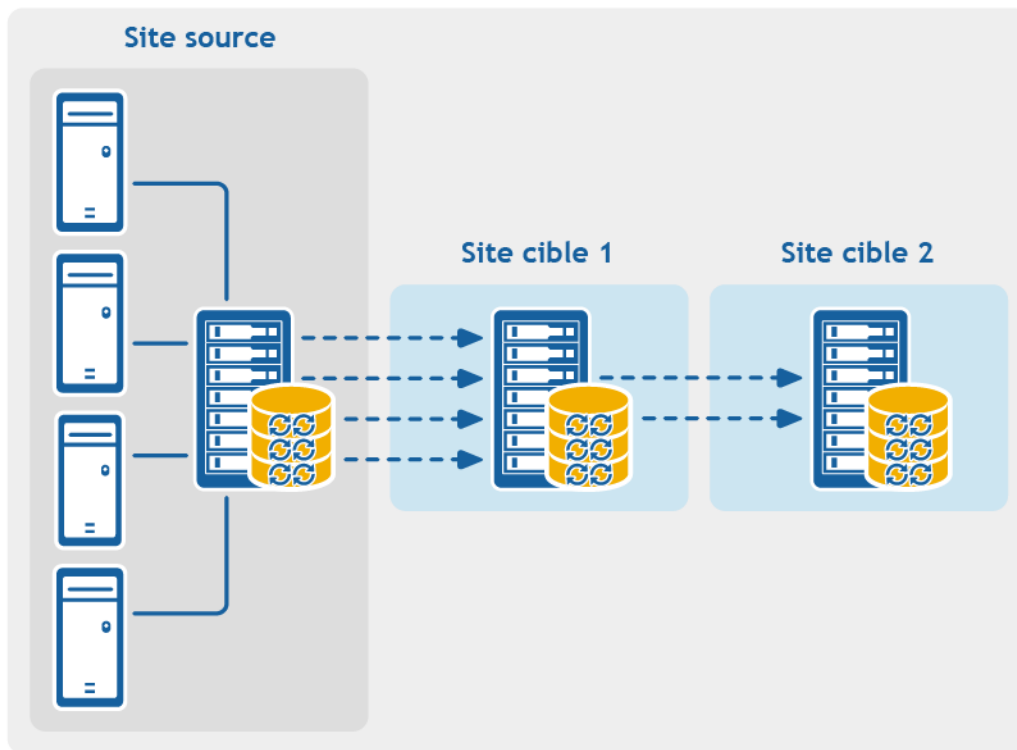


Figure 6. Configuration de réplication multicible

Si vous utilisez des appliances de sauvegarde Dell Data Protection (ex. : séries DL1x00 ou DL4x00), veillez à ce que le Core cible de la réplication dispose d'une licence logicielle valide. Chaque appliance matérielle achetée inclut une licence pour la cible de réplication. La clé de licence se trouve dans l'e-mail de bienvenue que vous avez reçu lors de l'achat de l'appliance. Pour obtenir de l'aide, consultez notre page d'aide relative aux licences à l'adresse <https://support.software.dell.com/licensing-assistance> ou envoyez un e-mail à license@software.dell.com.

Rétention et archivage

Les stratégies de sauvegarde et de rétention de votre appliance sont souples et, ainsi, faciles à configurer. La capacité d'adapter les stratégies de rétention aux besoins d'une organisation aide à satisfaire aux exigences de conformité sans compromettre le RTO.

Les stratégies de rétention appliquent les durées pendant lesquelles les sauvegardes sont stockées sur des supports à court terme (rapide et cher). Parfois, certaines exigences d'entreprise et techniques demandent une rétention étendue de ces sauvegardes, mais l'utilisation d'un stockage rapide est trop coûteuse. Ainsi, cette exigence crée le besoin d'un stockage à long terme (lent et bon marché). Les entreprises utilisent souvent un stockage à long terme pour l'archivage de données de conformité et de non conformité. La fonction d'archive prend en charge les rétentions étendues de données de conformité et de non conformité et est utilisée pour amorcer des données de réplication sur un core cible.

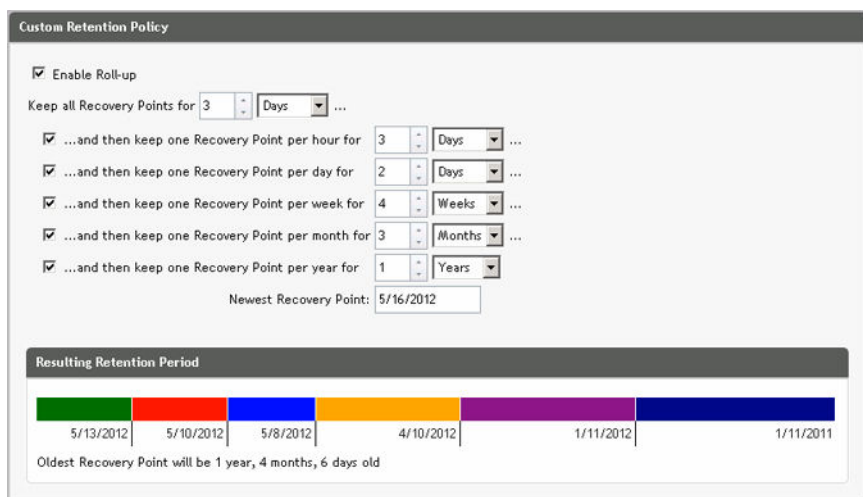


Figure 7. Stratégie de rétention personnalisée

Dans votre appliance, les stratégies de rétention peuvent être personnalisées pour spécifier la durée pendant laquelle un point de restauration de sauvegarde est conservé. Au fur et à mesure que les points de restauration s'approchent de la fin de leur période de rétention, les points de rétention parviennent à expiration et sont supprimés du pool de rétention. Normalement, ce processus devient inefficace et finit par échouer à mesure que la quantité de données et la période de rétention commencent à augmenter rapidement. Votre appliance résout le problème de grosses données en gérant la rétention de grandes quantités de données avec des stratégies de rétention complexes et en réalisant des opérations cumulatives pour les données approchant la fin de vie à l'aide d'opérations de métadonnées efficaces.

Vous pouvez réaliser les sauvegardes avec un intervalle de quelques minutes et au fur et à mesure que ces sauvegardes approchent leur fin de vie sur des jours, mois et années. Les stratégies de rétention gèrent l'approche de fin de vie et la suppression d'anciennes sauvegardes. Les niveaux dans la cascade sont définis en minutes, heures et jours ; semaines, mois et années. La stratégie de rétention est appliquée par le processus cumulatif de chaque soir.

Pour l'archivage à long terme, votre appliance fournit la capacité de créer une archive du core source ou cible de tout support amovible. L'archive est optimisée intérieurement et toutes les données de l'archive sont compressées, cryptées et dédupliquées. Si la taille totale de l'archive est supérieure à l'espace disponible sur le support amovible, l'archive s'étend sur plusieurs périphériques en fonction de l'espace disponible sur le support. L'archive peut aussi être verrouillée avec une phrase de passe. La restauration à partir d'une archive n'exige pas un nouveau core ; n'importe quel core peut acquérir l'archive et restaurer les données si l'administrateur a la phrase de passe et les clés de cryptage.

Virtualisation et cloud

Le Core est prêt pour le cloud, vous permettant de tirer profit de la capacité de calcul du cloud pour la restauration.

Votre appliance peut exporter toute machine protégée ou répliquée sur une machine virtuelle, par exemple les versions sous licence de VMware ou Hyper-V. Vous pouvez exécuter une exportation virtuelle ponctuelle ou créer une VM virtuelle de secours en établissant une exportation continue. Lors des exportations continues, la machine virtuelle est mise à jour de façon incrémentielle après chaque instantané. Les mises à jour incrémentielles sont très rapides et fournissent des clones de secours prêts à être activés d'un simple clic de bouton. Les types d'exportation de machines virtuelles pris en charge sont des stations de travail/serveurs VMware sur un dossier, une exportation directe sur un hôte vSphere/VMware ESX (i) ; une exportation vers Oracle VirtualBox ; et une exportation de données vers Microsoft Hyper-V Server sur Windows Server 2008 (64 bits), 2008 R2, 2012 (64 bits) et 2012 R2 (avec prise en charge de machines virtuelles Hyper-V génération 2)

Désormais, vous pouvez archiver les données du référentiel vers le cloud à l'aide de Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage ou d'autres services cloud OpenStack.

Alertes et gestion des événements

En plus de HTTP REST API, votre appliance offre aussi un vaste ensemble de fonctions de journalisation et de notifications d'événements par e-mail, Syslog ou le Journal d'événements Windows. Les notifications par e-mail peuvent servir à signaler l'intégrité ou l'état de différents événements aux utilisateurs ou groupes, en réponse à une alerte. Les méthodes Syslog et de Journal d'événements Windows servent à centraliser la journalisation dans un référentiel dans des environnements à plusieurs systèmes d'exploitation. Lorsqu'il s'agit d'environnements Windows uniquement, seul le Journal d'événements Windows est utilisé.

Portail de licences

Le Portail de licences offre des outils de gestion de droits de licence faciles à utiliser. Vous pouvez télécharger, activer, afficher, gérer les clés de licence et créer un profil d'entreprise pour suivre vos inventaires de licences. De plus, le portail permet aux fournisseurs de services et aux revendeurs de suivre et gérer les licences de leurs clients.

Console Web

Votre appliance comprend une nouvelle console centrale à base Web qui gère les cores distribués à partir d'un emplacement central. Ces MSP (Management Service Providers - Fournisseurs de service de gestion) et clients Entreprise avec plusieurs cores distribués peuvent déployer la console centrale pour obtenir une vue unifiée de gestion centrale. La console centrale (CMC) offre la capacité d'organiser les cores gérés en unités organisationnelles hiérarchiques. Ces unités organisationnelles peuvent représenter des unités d'affaires, des emplacements ou des clients pour les MSP auxquels on octroie un accès en fonction de leurs rôles. La console centrale peut également exécuter des rapports pour tous les cores gérés.

API de gestion des services

Votre appliance est livrée avec une API de gestion des services et fournit un accès programmé à toutes les fonctionnalités disponibles au moyen de la console de gestion centrale. L'API de gestion des services est une API REST. Toutes les opérations API sont effectuées sur SSL et sont authentifiées mutuellement à l'aide de certificats X.509 v3. Vous pouvez accéder au service de gestion depuis l'environnement ou directement par Internet à partir de toute application qui peut envoyer et recevoir une demande et une réponse HTTPS. Cette mesure permet une intégration aisée à toute application Web telle que des outils RMM (Relationship Management Methodology, Méthodologie de gestion de relations) ou des systèmes de facturation. Votre appliance est également livrée avec un client SDK pour la rédaction de scripts PowerShell.

Travailler avec l'Appliance DL Core

Compréhension de la console Core Rapid Recovery

Cette section présente les différents éléments de l'interface utilisateur de la console Core Rapid Recovery.

Accès à la console Core Rapid Recovery

Suivez les étapes ci-après pour accéder à la console Core Rapid Recovery.

- Effectuez l'une des opérations suivantes pour accéder à la console Core Rapid Recovery :
 - a Connectez-vous localement à votre serveur Core Rapid Recovery, puis double-cliquez sur l'icône de la console Core.
 - b Vous pouvez également saisir l'une des URL suivantes dans votre navigateur Web :
 - `https://<nomdevotreserveurcore>:8006/apprecovery/admin/` ou
 - `https://<adresseIPdevotreserveurcore>:8006/apprecovery/admin/`

REMARQUE : étant donné que l'interface utilisateur de la console Core Rapid Recovery se base sur JavaScript, ce langage doit être activé sur le navigateur Web que vous utilisez pour y accéder.

Si vous avez modifié le port par défaut du service Rapid Recovery, mettez à jour le port de l'URL précédente en conséquence.

Comprendre le guide de démarrage rapide

Le guide de démarrage rapide fournit un ensemble de tâches conseillées pour la configuration et l'utilisation du Core Rapid Recovery.

Le guide de démarrage rapide s'affiche automatiquement la première fois que vous installez ou mettez à niveau le Core Rapid Recovery et que vous accédez à la Core Console. Cliquez sur **Guide de démarrage** sur la page **Accueil** du guide pour afficher les diverses tâches de configuration suggérées. Parcourez le guide à l'aide des options **Skip Ignorer l'étape** et **Retour**. Après avoir affiché la dernière étape suggérée, cliquez sur **Terminer** pour fermer le guide.

Vous pouvez relancer le Guide de démarrage rapide à tout moment à partir du menu Aide de la Core Console. Vous pouvez également choisir de masquer la page **Accueil** du guide de démarrage rapide.

À moins que vous ne le masquiez, le guide de démarrage rapide s'affichera à nouveau chaque fois que vous vous connecterez à la Rapid Recovery Core Console et accéderez à la page **Accueil**. Pour plus d'informations, voir [Masquage du guide de démarrage rapide](#).

Vous n'êtes pas obligé de suivre les étapes suggérées par le guide. Vous pouvez simplement consulter les tâches suggérées, en parcourant le guide à l'aide des options **Ignorer l'étape** et **Retour**. De manière facultative, pour masquer le guide à n'importe quel moment, cliquez sur **Sortir du guide**.

Si vous choisissez d'effectuer les tâches de configuration suggérées par le guide de démarrage rapide, vous n'avez qu'à suivre les invites indiquées à chacune des étapes du guide, et l'assistant concerné ou la zone de l'interface utilisateur appropriée s'affichent. Les procédures à suivre pour effectuer chacune des tâches suggérées par le guide sont décrites dans ce document, comme indiqué dans le tableau ci-dessous.

REMARQUE : les tâches de configuration suggérées par le guide de démarrage rapide ne sont pas toutes utiles pour tous les utilisateurs. Vous devez connaître les tâches qui répondent à vos besoins.

Le guide de démarrage rapide porte sur les tâches de configuration suivantes :

Tableau 2. Tâches de configuration du guide de démarrage rapide

Fonction	Brève description	Résultat du choix de la tâche, renvoi vers la procédure
Protection	Protection d'une seule machine, protection d'un cluster de serveurs ou protection de plusieurs machines à l'aide d'une protection groupée	Cliquez sur Protéger ou choisissez Protéger une machine dans le menu déroulant pour ouvrir l'assistant Protéger une machine. Pour en savoir plus sur l'exécution de l'Assistant Protéger une machine, voir Protéger une machine. Sélectionnez Protéger le cluster dans le menu déroulant pour ouvrir la boîte de dialogue Connexion au cluster. Pour en savoir plus sur la protection d'un cluster, voir Protection d'un cluster. Sélectionnez Protection groupée pour ouvrir l'assistant Protéger plusieurs machines. Pour en savoir plus sur l'exécution de l'Assistant Protéger plusieurs machines, voir À propos de la protection de plusieurs machines.
Réplication	Configuration d'une réplication depuis un Core principal (source) vers un Core secondaire (cible)	Cliquez sur Réplication pour ouvrir la page Réplication. Vous invite à ajouter un Core cible à l'aide de l'Assistant Réplication. Pour en savoir plus sur l'utilisation de l'Assistant Réplication afin de configurer la réplication sur un Core autogéré, voir Réplication vers un core cible autogéré . Pour obtenir des informations générales sur la réplication, voir Configuration d'une réplication .
Exportation virtuelle	Exécution d'une exportation ponctuelle ou établissement d'une exportation continue d'une machine protégée vers une machine virtuelle	Cliquez sur Exportation pour exporter des données depuis votre machine protégée vers une machine virtuelle. Vous pouvez effectuer une exportation ponctuelle ou configurer un disque de secours virtuel pour une exportation en continu vers une machine virtuelle. Pour en savoir plus sur les exportations virtuelles, voir À propos de l'exportation vers des machines virtuelles avec Rapid Recovery .
Configuration	Permet de définir une configuration supplémentaire pour le Core Rapid Recovery	Cliquez sur Plus pour afficher les fonctions supplémentaires que vous pouvez configurer et gérer. Les fonctions incluent les archives, montages, CD d'amorçage, logithèques, clés de chiffrement, comptes Cloud, recherche de fichiers, stratégies de rétention, notifications, rapports, journaux et bien plus encore.
Configuration : chiffrement	Ajout ou importation de clés de chiffrement que vous pouvez utiliser pour une, deux ou plusieurs machines protégées	Cliquez sur Clés de chiffrement pour gérer la sécurité des données protégées en ajoutant ou en important des clés de chiffrement. Vous pouvez appliquer des clés de chiffrement à une, deux ou plusieurs machines protégées. Le chiffrement est décrit dans la rubrique Comprendre les clés de clés de chiffrement .
Configuration : notifications	Configuration de notifications pour les événements, les avertissements et les alertes	Cliquez sur Évènement pour spécifier des groupes de notification pour les événements, les avertissements et les alertes. Pour les envoyer par e-mail, vous devez également établir des paramètres de serveur SMTP. Pour en savoir plus sur la gestion des événements, voir la rubrique Événements , notamment les rubriques Configurer les groupes de notification et Configurer un serveur de messagerie électronique .
Configuration : rétention	Affichage ou modification de la stratégie de rétention par défaut du Core	Cliquez sur Stratégie de rétention pour ouvrir la page Stratégie de rétention pour le Core. De là, vous pouvez définir combien de temps vous voulez conserver un point de restauration avant d'effectuer une consolidation. Pour obtenir des informations conceptuelles sur les stratégies de rétention, voir la rubrique Gestion des données vieillissantes . Pour en savoir plus sur les procédures, voir Gestion des stratégies de conservation .
Restaurer	Restaurer des données à partir d'un point de restauration du Core.	Cliquez sur Restaurer pour ouvrir l'assistant Restaurer une machine. Pour plus d'informations sur la restauration de données, voir la rubrique À propos de la restauration de volumes à partir d'un point de restauration .

Masquage du guide de démarrage rapide

Le guide de démarrage rapide s'affiche automatiquement la première fois que vous installez ou mettez à niveau le Core Rapid Recovery. Il s'affiche également lorsque vous sélectionnez Guide de démarrage rapide dans le menu déroulant Aide, et chaque fois que vous accédez à l'onglet Accueil sur la Core Console.

Utilisez la procédure ci-dessous pour masquer le guide de démarrage rapide.

- Dans la Rapid Recovery Core Console, si vous visualisez la page **Accueil** du guide de démarrage rapide, procédez comme suit :
 - Si vous voulez masquer la page **Accueil** du guide de démarrage rapide, sélectionnez **Ne plus afficher**.

REMARQUE : Cette option masque la page Accueil à la prochaine ouverture du guide de démarrage, et toutes les fois suivantes, jusqu'à la prochaine mise à niveau du Core de Rapid Recovery.

Si vous choisissez de masquer cette page, et que vous voulez accéder aux options avancées à l'avenir, sélectionnez **Retour** dans l'assistant pour voir s'afficher la page masquée.

- Si vous voulez masquer le guide de démarrage rapide pour cette session uniquement, cliquez sur **Fermer**.
Le guide de démarrage rapide se ferme. La prochaine fois que vous accédez à l'onglet Accueil sur la Core Console, le guide de démarrage rapide s'affiche à nouveau.

Vous pouvez également ouvrir le guide de démarrage rapide depuis le menu d'aide.
- Depuis n'importe quelle page du guide de démarrage rapide, vous pouvez cliquer sur **Sortir du guide**.
Le guide de démarrage rapide se ferme. Si vous sélectionnez cette option, vous pouvez toujours ouvrir le guide de démarrage rapide à partir du menu Aide.

Navigation vers Rapid Recovery Core Console

Lorsque vous vous connectez à Core Console et chaque fois que vous cliquez sur l'icône **Accueil** , la page **Accueil** s'affiche. La page **Accueil** affiche le Core de Rapid Recovery, avec deux options. Dans la zone d'affichage principale, le contenu par défaut est le nouveau tableau de bord du Core, qui affiche un ensemble de rapports en temps réel sur votre système. Les rapports du tableau de bord par défaut comprennent l'état des récentes tâches de transfert, par transfert de machine, une présentation de la logithèque et l'état de connectivité des machines protégées, des machines répliquées et des machines de points de restauration uniquement. Vous pouvez également basculer vers la vue des tableaux récapitulatifs. Dans cette vue, le titre de la page reprend le nom d'affichage du Core de Rapid Recovery, et vous pouvez voir des tableaux récapitulatifs répertoriant les machines protégées, les logithèques et les alertes récentes. Pour plus d'informations, voir [Compréhension de la page Accueil \(vue des tableaux récapitulatifs\)](#) et [Compréhension du tableau de bord du Core](#), respectivement.

Sur la page **Accueil** (et sur chaque page de la Core Console), la zone de navigation de gauche affiche les éléments qui sont protégés sur votre Core. Vous pouvez naviguer vers d'autres pages de l'interface utilisateur en effectuant l'une des opérations suivantes :

- Cliquer sur les différentes icônes de la barre d'icônes dans la zone de navigation de gauche. Les options accessibles à partir de la barre d'icônes sont entre autres : Réplication, Disque de secours virtuel, Événements, Paramètres, etc.
- Développer le menu  (Plus) sur la barre d'icônes, puis sélectionner une destination.
- Cliquer sur un bouton ou une option de menu dans la barre des boutons. Les boutons incluent les options Protéger, Restaurer, Archiver et Répliquer.

Lorsque vous sélectionnez un élément dans la zone de navigation de gauche, la Core Console affiche des informations récapitulatives sur cet élément. Par exemple, si vous cliquez sur le nom d'une machine protégée, la Core Console affiche des informations concernant cette machine uniquement, et non plus le Core. Dans cet exemple, le nom d'affichage de la machine protégée s'affiche en tant que titre de la page. Un sous-menu s'affiche sur la droite. Il vous permet d'afficher des informations spécifiques sur la machine protégée. Les options de menu disponibles sont les suivantes : Synthèse, Points de récupération, Événements, Paramètres, Rapports, etc.

Pour revenir à l'affichage des informations sur le Core, comprenant des rapports sur le tableau de bord ou une vue récapitulative de plusieurs machines protégées ou répliquées, cliquez sur l'icône **Accueil**  en haut à gauche de l'interface utilisateur. Sur la page **Accueil**, vous pouvez basculer entre la vue de tableau de bord et l'affichage de la page Synthèse. Pour cela, cliquez sur le lien rouge dans la partie supérieure droite de la page.

Vous pouvez vous servir du titre situé dans la partie supérieure de la Core Console pour comprendre le contexte des informations que vous consultez dans le Core. Par exemple :

- Le nom d'affichage ou l'adresse IP du Core s'affiche toujours en tant que titre de la page sur laquelle vous consultez des informations récapitulatives au sujet du Core.
- Si le titre est Tableau de bord, vous consultez le tableau de bord du Core.
- Si vous voyez le nom d'affichage ou l'adresse IP d'une machine protégée, ou un volet Synthèse dans la partie supérieure d'une page, alors vous consultez des informations concernant une seule machine protégée par le Core ou répliquée dans le Core.
- Si vous voyez le titre Machines protégées, vous consultez des informations concernant toutes les machines protégées dans le Core Rapid Recovery.
- Si vous voyez le titre Machines répliquées à partir de..., vous consultez des informations concernant toutes les machines répliquées dans le Core Rapid Recovery.
- Si vous voyez le titre Points de restauration uniquement, vous consultez des informations concernant toutes les machines de points de restauration uniquement de ce Core.

Pour plus d'informations sur les fonctionnalités et les fonctions disponibles sur chaque page, voir la section correspondante ci-dessous.

Pour en savoir plus sur l'affichage des machines protégées, voir [Affichage du menu Machines protégées](#). Pour en savoir plus sur la gestion des machines protégées, voir [Gérer les machines protégées](#).

Pour en savoir plus sur l'affichage des machines répliquées, voir [Affichage des répliquations entrantes et sortantes](#).

Pour plus d'informations sur l'affichage des machines de points de restauration uniquement, voir [Affichage du menu Points de restauration uniquement](#)

Description de la zone de navigation gauche

La zone de navigation gauche de la Core Console est affichée à gauche de l'interface utilisateur. Le contenu de cette zone de navigation varie en fonction du type d'objets protégés dans votre Core Rapid Recovery.

La zone de navigation gauche contient toujours les éléments suivants :

- **Barre d'icônes.** Sert à parcourir les pages principales de la Core Console.
- **Filtre Texte.** Le filtre Texte est un champ de texte qui vous permet de filtrer les éléments figurant dans les différents menus affichés plus bas. Cliquez sur la flèche située à droite du filtre Texte pour développer ou réduire les menus déroulants affichés plus bas.

Outre ces éléments, la zone de navigation gauche affiche généralement des menus permettant de parcourir, de filtrer et d'afficher les objets protégés sur votre Core (machines protégées, machines répliquées, etc.)

Chaque menu est contextuel, c'est-à-dire qu'il ne s'affiche dans la Core Console qu'au moment adéquat. Par exemple, si vous protégez plusieurs machines, le menu Machines protégées s'affiche, et ainsi de suite.

Pour plus d'informations, voir les tableaux de la zone de navigation gauche dans [Affichage de l'interface utilisateur de la Core Console](#).

Affichage de la page Accueil de la console Core Rapid Recovery

Chaque fois que vous vous connectez à la console Core Rapid Recovery ou que vous cliquez sur l'icône **Accueil**  dans la barre d'icônes, la page **Accueil** s'affiche.

La page **Accueil** de la console Core propose une nouvelle vue de **tableau de bord**, en plus de la vue des **tableaux récapitulatifs** classique. Le tableau de bord est la vue par défaut.

Vous pouvez passer d'une vue à l'autre sur la page **Accueil** en cliquant sur le lien rouge dans la partie supérieure droite de la page **Accueil**.

Sur la page **Accueil**, ainsi que sur toutes les autres pages de la console Core, vous pouvez accéder aux fonctions qui vous intéressent à l'aide de la zone de navigation de gauche.

Pour en savoir plus, reportez-vous aux rubriques suivantes :

- [Description de la zone de navigation gauche](#)
- [Compréhension du tableau de bord du Core](#)
- [Compréhension de la page Accueil \(vue des tableaux récapitulatifs\)](#)

Compréhension de la page Accueil (vue des tableaux récapitulatifs)

La page **Accueil** s'applique uniquement au Core. Dans la vue du tableau de bord, des rapports graphiques sont affichés en temps réel. Lorsque vous basculez vers la vue des tableaux récapitulatifs, la page **Accueil** affiche toutes les machines protégées ou répliquées par le Core, les logithèques associées à votre Core et les alertes relatives aux machines de ce Core.

La vue de chacun des volets de la page **Accueil** peut être développée ou réduite. Par exemple, si vous cliquez sur l'icône  (Réduire la vue) dans la partie supérieure droite du volet Machines protégées, la vue des machines protégées est réduite, de sorte que seul le nom du volet soit visible. Pour développer la vue afin de réafficher toutes les machines protégées, cliquez sur l'icône  (Élargir la vue).

Le tableau suivant présente les différents éléments de la page **Accueil** dans la vue des tableaux récapitulatifs.

Tableau 3. Options de la page Accueil

Élément de l'IU	Description
Machines protégées	Le volet Machines protégées répertorie les machines que ce Core protège. Ce volet s'affiche, que des machines aient été ajoutées ou non au Core à des fins de protection. Cette section contient les informations suivantes pour chacune des machines protégées : • Type de machine. Une icône indique si la machine est une machine physique, une machine virtuelle ou un cluster protégé. • État. Les cercles colorés de la colonne État indiquent si la machine protégée est accessible, en pause ou déconnectée et inaccessible. • Nom d'affichage. Nom d'affichage ou adresse IP de la machine protégée. • Nom de la logithèque. Le nom de la logithèque qui stocke les points de restauration pour cette machine. • Dernier instantané. Date et heure auxquelles Rapid Recovery a créé le dernier instantané des points de restauration pour cette machine. • Points de restauration. Nombre de points de restauration stockés dans la logithèque et espace de stockage de chaque machine protégée. • Version. Version du logiciel Agent Rapid Recovery installée sur cette machine. Si vous cliquez sur le nom d'une machine spécifique s'affichant dans ce volet, la page Synthèse s'ouvre. Cette page fournit des informations récapitulatives concernant la machine sélectionnée. Pour en savoir plus sur les opérations que vous pouvez effectuer sur la page Synthèse, voir Affichage des informations récapitulatives d'une machine protégée.
Machines répliquées	Le volet Machines répliquées répertorie toutes les machines répliquées par ce Core à partir d'un autre Core. Ce volet s'affiche uniquement si votre Core réplique des machines à partir d'un autre Core. Cette section contient les informations suivantes pour chacune des machines répliquées : • Type de machine. Une icône indique si la machine est une machine physique, une machine virtuelle ou un cluster protégé. • État. Les cercles colorés de la colonne État indiquent si la machine répliquée est accessible, en pause ou déconnectée et inaccessible.

Élément de l'UI	Description
	• Nom d'affichage. Nom d'affichage ou adresse IP de la machine répliquée. • Nom de réplication. Nom d'affichage du Core source d'origine pour toutes les machines répliquées sur ce Core cible. Vous pouvez définir ce nom pendant la configuration de la réplication. • Nom de la logithèque. Le nom de la logithèque qui stocke les points de restauration pour cette machine. • Dernier instantané répliqué. Date et heure auxquelles Rapid Recovery a créé le dernier répliqua de la machine protégée d'origine. • Points de restauration. Nombre de points de restauration stockés dans la logithèque et espace de stockage de chaque machine répliquée. • Version. Version du logiciel Agent Rapid Recovery installée sur cette machine. Si vous cliquez sur le nom d'une machine spécifique s'affichant dans ce volet, la page Récapitulatif s'affiche. Cet onglet fournit des informations récapitulatives concernant cette machine répliquée.
Machines de points de restauration uniquement	Le volet Machines de points de restauration uniquement répertorie toutes les machines exclues de la protection ou de la réplication, si les points de restauration ont été conservés. Ces machines peuvent être utilisées pour une restauration au niveau des fichiers, mais pas pour une restauration bare metal restore (BMR), pour une restauration de volumes entiers ou pour un ajout de données d'instantané. Ce volet s'affiche uniquement si certaines de vos machines correspondent à cette définition. Cette section comprend les informations suivantes pour chacune des machines comportant uniquement des points de restauration : • Type de machine. Une icône indique si la machine est une machine physique, une machine virtuelle ou un cluster protégé. • État. Les cercles colorés de la colonne État indiquent si la machine de points de restauration uniquement est accessible, en pause ou déconnectée et inaccessible. • Nom d'affichage. Nom d'affichage ou adresse IP de la machine pour laquelle vous avez conservé des points de restauration. • Nom de la logithèque. Nom de la logithèque stockant les points de restauration restants de cette machine. • Points de restauration. Nombre de points de restauration stockés dans la logithèque et espace de stockage de chaque machine de points de restauration uniquement. Si vous cliquez sur le nom d'une machine spécifique s'affichant dans ce volet, la page Récapitulatif s'affiche pour cette machine de points de restauration uniquement.
Référentiels DVM	Ce volet s'affiche pour le DL1000, que des logithèques DVM aient été créées ou non. Ce volet s'affiche uniquement si votre Core contient une ou plusieurs logithèques DVM. Il contient les informations suivantes pour chaque logithèque DVM : • Type. Une icône représente une logithèque. • État. Des cercles de couleur dans la colonne État indiquent si la logithèque est montée et peut accepter des transferts de points de restauration, ou si elle est inaccessible ou dans un état d'erreur. • Nom de la logithèque. Le nom d'affichage de la logithèque. • Utilisation de l'espace. Quantité totale d'espace utilisée dans la logithèque, et taille ou étendue du volume de stockage. • Données protégées. La quantité d'espace utilisé dans la logithèque. • Machines. Nombre de machines pour lesquelles la logithèque stocke des points de restauration. • Points de restauration. Le nombre de points de restauration stockés dans la logithèque. • Taux de compression. Le taux auquel la logithèque compresse les données protégées pour économiser de l'espace. Pour plus d'informations, voir Comprendre les référentiels.
Alertes	Cette section répertorie les alertes importantes relatives au Core et à toutes les machines qu'il protège. Cette section contient les informations suivantes : • Icônes. La colonne des icônes indique la nature de l'alerte. Il peut s'agir de messages d'information ou d'erreurs • Date. Affiche la date et l'heure auxquelles Rapid Recovery a émis l'alerte.

Élément de l'IU	Description
	• Message. Décrit l'alerte. Vous pouvez également afficher ces détails sur la page Événements du Core. Pour plus d'informations, voir Affichage des événements à l'aide des tâches, des alertes et du journal.

Compréhension du tableau de bord du Core

Le tableau de bord du Core affiche un ensemble de rapports graphiques en temps réel représentant des données pertinentes pour votre Core et les machines que vous protégez. Le tableau de bord comprend les rapports suivants :

- **Tâche de transfert.** Ce rapport affiche tous les transferts de données d'instantanés (y compris les images de base et les instantanés incrémentiels) qui se sont terminés durant ces dernières 24 heures. Les instantanés incluent des images de base et des instantanés incrémentiels. Ce rapport de tableau de bord apparaît sous forme de diagramme circulaire.
- **Tâche de transfert par machine.** Cette tâche indique, par machine protégée, le nombre de tâches de transfert réussies ou ayant échoué dans les dernières 24 heures. Ce rapport de tableau de bord apparaît sous forme de graphique linéaire.
- **Logithèque.** Ce rapport affiche les logithèques associées à votre Core. Il affiche le nombre de logithèques, le nombre de machines protégées dans chacune, le nombre de points de restauration et le pourcentage de compression ou de déduplication. Ce rapport est actualisé toutes les minutes.
- **Connectivité de la machine.** Ce rapport affiche l'état de connectivité des machines protégées et répliquées sur votre Core. Il affiche également la connectivité pour les données sur [machines comportant uniquement des points de restauration](#).

Vous pouvez réduire ou développer la vue de tous les rapports dans le tableau de bord en cliquant sur la flèche vers le haut ou vers le bas dans l'en-tête du rapport. Certains rapports du tableau de bord (Machine Connectivity et Repository) disposent d'un signe plus (+) en regard de la flèche, qui vous permet d'ajouter une autre machine protégée ou une autre logithèque, respectivement.

Vous pouvez également utiliser la fonctionnalité glisser-déposer pour modifier l'emplacement de l'un des rapports sur le tableau de bord, afin d'ordonner les rapports en fonction de votre utilisation.

Affichage du menu Machines protégées

Dans l'interface utilisateur de Rapid Recovery, un menu Machines protégées s'affiche dans la zone de navigation de gauche. Comme tous les libellés des menus de la zone de navigation, le libellé de ce menu est entièrement en lettres majuscules. Par défaut, ce menu est complètement développé, et il affiche la liste de toutes les machines protégées par ce Core. Si certains de vos clusters de serveurs sont protégés, ceux-ci sont inclus dans cette liste.

Vous pouvez réduire ou développer la vue des machines ou clusters de serveurs protégés dans votre Core en cliquant simplement sur la flèche située sur la gauche de ce menu.

Le menu Machines protégées comprend un menu déroulant sur la droite qui répertorie les fonctions pouvant être exécutées sur toutes les machines protégées. Cliquez sur la flèche à droite de **Machines protégées** pour afficher le menu et effectuer l'une des tâches suivantes :

- Forcer la capture d'instantanés incrémentiels pour toutes les machines
- Forcer une image de base pour toutes les machines
- Suspendre la protection pour toutes les machines (si la protection est active)
- Reprendre la protection pour toutes les machines (si la protection est suspendue)
- Actualisation des métadonnées de toutes les machines protégées
- Retrait de la protection de toutes les machines sur le Core

Chacune des machines répertoriées dans le menu Machines protégées dispose également d'un menu déroulant qui contrôle uniquement les fonctions de cette machine individuelle. À partir du menu déroulant de n'importe quelle machine, vous pouvez :

- Forcer un instantané incrémentiel pour la machine sélectionnée
- Suspendre la protection de la machine sélectionnée (si la protection est active)

- Réactiver la protection de la machine sélectionnée (si la protection est suspendue)
- Actualiser les métadonnées
- Retirer la protection de la machine sélectionnée sur le Core
- Accéder à la page Synthèse de la machine sélectionnée
- Accéder à la page Points de restauration de la machine sélectionnée
- Accéder à la page Événements de la machine sélectionnée
- Accéder à la page Paramètres de la machine sélectionnée
- Générer des rapports spécifiques à cette machine
- Accéder à d'autres fonctions spécifiques à la machine sélectionnée, notamment les informations sur le système, les montages, la stratégie de rétention, les notifications ou un journal spécifique à la machine
- Créer une étiquette personnalisée qui affiche la liste des machines protégées

Si vous gérez des clusters de serveurs à partir du Core Rapid Recovery, ces clusters s'affichent également dans le menu de navigation de gauche. À partir du menu déroulant de n'importe quel cluster, vous pouvez également :

- Accéder à la page **Nœuds protégés** du cluster sélectionné

Si vous cliquez sur la flèche à gauche du menu Machines protégées, la liste des machines et des clusters de serveurs protégés se réduit, et aucune machine n'est répertoriée. Cliquez de nouveau cette flèche pour afficher de nouveau la liste des machines.

Le fait de cliquer sur le nom d'une machine dans le menu Machines protégées ouvre l'onglet Synthèse de cette machine. Pour en savoir plus sur les opérations que vous pouvez effectuer sur la page Synthèse, voir [Affichage des informations récapitulatives d'une machine protégée](#).

Enfin, le fait de cliquer directement sur le menu **Machines protégées** a pour effet d'ouvrir la page **Machines protégées** dans la zone de contenu principale, avec un seul volet affichant les machines protégées sur ce Core. Pour en savoir plus sur les opérations que vous pouvez effectuer dans le volet **Machines protégées** de la page éponyme, voir [Affichage du volet Machines protégées](#).

REMARQUE : sur la page Machines protégées, vous pouvez rétablir la vue basée sur le Core, en cliquant sur l'icône Accueil de la barre d'icônes.

Affichage des informations récapitulatives d'une machine protégée

Lorsque vous cliquez sur le nom d'une machine protégée dans la Core Console, la page **Récapitulatif** s'affiche. Elle contient au moins un volet [Synthèse](#) et un volet [Volumes](#). Si une machine est ajoutée à une réplication, un volet [Réplication](#) s'affiche également.

Si vous utilisez un ou plusieurs serveurs Exchange protégés, un volet [Informations Exchange Server](#) est également disponible. Ce volet contient des données sur votre serveur Exchange protégé.

Si vous utilisez des serveurs SQL protégés, un volet [Informations SQL Server](#) est également disponible. Ce volet contient des données sur vos serveurs SQL protégés.

La partie supérieure de cette page inclut un menu comportant les actions que vous pouvez effectuer sur la machine protégée. En dessous se trouvent au moins un volet Synthèse et un volet Volumes. Si une machine est ajoutée à la réplication, un volet Réplication s'affiche également.

Lorsque vous consultez les informations d'une machine protégée, sur la page Synthèse et dans toutes les autres vues, vous trouverez dans la partie supérieure de la page un menu indiquant les fonctions que vous pouvez utiliser. Ce menu s'affiche juste en dessous du nom de la machine protégée.

Liens connexes

- [Affichage du volet Synthèse](#)
- [Affichage des volumes sur une machine protégée](#)
- [Affichage des informations de réplication](#)
- [Affichage du volet d'Informations Exchange Server](#)
- [Affichage du volet Informations SQL Server](#)

Affichage du volet Synthèse

Le volet **Synthèse** contient des informations récapitulatives sur la machine protégée, notamment le nom d'hôte, la date et l'heure du dernier instantané, la date et l'heure de l'instantané planifié suivant, ainsi que des informations sur les clés de chiffrement et sur la version du logiciel Agent Rapid Recovery. Vous y trouverez également un lien vers une page Informations sur le système détaillée concernant la machine.

Affichage des volumes sur une machine protégée

Pour une machine protégée, dans le volet Volumes de la page Synthèse, vous pouvez exécuter les actions suivantes pour les volumes répertoriés :

- Définir ou modifier une planification de protection pour un volume sélectionné. Les planifications de protection sont généralement définies lorsque vous protégez une machine pour la première fois. Pour en savoir plus sur la modification d'une planification de protection, voir [Modification des planifications de protection](#).
- Forcer une image de base ou un instantané. En règle générale, les instantanés sont exécutés en fonction de la planification de la protection. Cependant, à tout moment, vous pouvez forcer une image de base ou un instantané incrémentiel pour les volumes sélectionnés. Pour en savoir plus, voir [Forcer un instantané](#).

Affichage des informations de réplication

Le volet **Réplication** contient des informations récapitulatives sur la machine répliquée, notamment le nom de réplication, l'état de réplication, l'avancement et l'espace disponible.

Affichage du volet d'Informations Exchange Server

Le volet d'**Informations Exchange Server** s'affiche uniquement pour les machines protégées qui sont des serveurs Exchange.

Ce volet contient des informations récapitulatives sur le serveur Exchange protégé, y compris la version de Microsoft Exchange installée, le chemin du répertoire où est installé Exchange et le chemin d'accès est défini pour les données de boîtes aux lettres d'Exchange.

Les magasins d'e-mails montre le nom de la base de données Exchange (EDB), le chemin d'accès du fichier EDB, le chemin du répertoire où sont stockés les fichiers journaux, le préfixe de journal, le chemin d'accès du système, le groupe de disponibilité de base de données (DAG), et le type de magasin d'e-mails.

Affichage du volet Informations SQL Server

Le volet **Informations SQL Server** s'affiche uniquement pour les serveurs SQL protégés.

Ce volet contient des informations récapitulatives sur les serveurs SQL protégés. Vous pouvez afficher les détails de chaque tableau dans la base de données en développant les informations de la base de données. Vous pouvez également afficher le nom de la base de données ou du tableau ainsi que le chemin d'accès de la base de données.

Affichage des points de restauration d'une machine

La page points de restauration affiche la liste des points de restauration collectés pour cette machine protégée, ainsi que des données pertinentes sur la machine et la logithèque. Sur cette page, vous pouvez monter, exporter et restaurer des points de restauration spécifiques, ainsi que supprimer les points de restauration.

La page est divisée en deux volets : Récapitulatif des points de restauration et points de restauration. Le volet Synthèse ne comporte aucun lien pouvant donner lieu à une action. Il affiche les données suivantes pour la machine.

Tableau 4. Données du volet Récapitulatif des points de restauration

Élément de l'IU	Description
Total des points de restauration	Le nombre des points de restauration collectés pour cette machine protégée particulière.
Données totales protégées	La quantité de données de la machine protégée qui sont stockées dans la logithèque.
Logithèque	Le nom de la logithèque dans laquelle Rapid Recovery stocke les points de restauration de cette machine protégée.
État de la logithèque	La barre d'avancement affiche un pourcentage de l'espace total utilisé dans la logithèque. La quantité de données utilisées et la taille totale de la logithèque s'affichent au-dessous de la barre d'avancement.

Pour plus d'informations, voir [Affichage du volet Machines protégées](#).

Affichage des événements pour une machine protégée

Sur la page **Événements**, vous pouvez afficher les tâches qui se sont déjà produites ou sont en cours pour la machine protégée que vous avez sélectionnée. Les boutons situés en haut de la page vous permettent de naviguer jusqu'aux listes des tâches dans chacune des trois catégories d'activités :

- **Tâches.** Une tâche que Rapid Recovery doit exécuter pour fonctionner correctement.
- **Alertes.** Notification relative à une tâche ou un événement, comprenant les erreurs et les avertissements.
- **Journal.** Combinaison de toutes les tâches et alertes relatives à la machine protégée.

Le tableau suivant comprend des descriptions de chacun des éléments de la page **Événements**.

Tableau 5. Éléments de la page Événements

Élément de l'IU	Description
Mot-clé de recherche	Vous permet de rechercher un élément spécifique dans chaque catégorie. Disponible pour les tâches uniquement.
From	Pour affiner vos résultats, vous pouvez entrer la date à laquelle vous voulez commencer la recherche. Disponible pour les tâches uniquement.
To	Pour affiner vos résultats, vous pouvez entrer la date à laquelle vous voulez arrêter la recherche. Disponible pour les tâches uniquement.
Icônes d'état	Chaque icône représente un état différent de la tâche. Pour les alertes et les tâches, en cliquant sur une des icônes, vous pouvez filtrer la liste en fonction de cet état, ce qui va générer un rapport. En cliquant sur l'icône une

Élément de l'IU	Description
	deuxième fois, vous supprimez le filtre pour cet état. Vous pouvez filtrer en utilisant plus d'un état. Les états comprennent : • Actif. Une tâche en cours. • En file d'attente. Une tâche en attente de la fin d'une autre tâche pour pouvoir commencer. • En attente. Une tâche qui attend votre approbation ou une finalisation, comme un disque source. (Pour plus d'informations sur les disques sources, voir Réplication.) • Terminé. Une tâche qui a été achevée avec succès. • Échec. Une tâche qui a échoué et n'a pas pu être terminée.
Icône de service	Ce bouton ajoute des tâches de service à la liste des tâches. Lorsque vous cliquez sur cette icône, une icône de service plus petite s'affiche sur chacune des icônes d'état, ce qui vous permet de filtrer par tâches de service dans cet état (s'il y en a). Exemples de tâches de service : suppression des fichiers d'indexation ou retrait de la protection d'une machine.
Liste déroulante des types d'exportation	La liste déroulante comprend les formats auxquels vous pouvez exporter le rapport des événements. Disponible pour les tâches uniquement. Elle comprend les formats suivants : • PDF • HTML • CSV • XLS • XLSX
 (Icône d'exportation)	Convertit le rapport des événements au format choisi. Disponible pour les tâches uniquement.
Choix des pages	Les rapports des événements peuvent inclure de multiples tâches réparties sur plusieurs pages. Les numéros et les flèches au bas de la page Événements vous permettent de naviguer entre les différentes pages du rapport.

La page **Événements** affiche tous les événements sous forme de tableau. Le tableau suivant répertorie les informations affichées pour chaque élément.

Tableau 6. Informations détaillées sur le tableau récapitulatif des événements

Élément de l'IU	Description
État	Indique l'état de la tâche, de l'alerte ou de l'élément de journal. Disponible pour les alertes ou les éléments de journal, cliquez sur l'en-tête pour filtrer les résultats par état.
Nom	Le nom est uniquement disponible pour les tâches. Ce champ de texte répertorie les types de tâche qui se sont terminées pour cette machine protégée. Exemples : transfert de volume, entretien de logithèque, consolidation, vérification de montabilité, vérification de somme de contrôle, etc.
Heure de début	Disponible pour les tâches, alertes et éléments de journal. Affiche la date et l'heure auxquelles la tâche ou l'opération a débuté.
Heure de fin	Disponible pour les tâches uniquement. Indique la date et l'heure auxquelles l'événement est survenu.
 Détails de la tâche	Disponible pour les tâches uniquement. Ouvre la boîte de dialogue Surveiller la tâche active , afin de pouvoir afficher les détails d'une tâche ou d'une opération spécifique. Ces informations comprennent un ID pour la tâche, la vitesse de transfert du Core (si applicable), le temps écoulé pour l'exécution de la tâche, le travail total en gigaoctets et toute tâche enfant associée à la tâche.
Message	Disponible pour les alertes et éléments de journal. Ce champ de texte fournit un message descriptif de l'alerte ou de l'élément du journal.

Affichage de rapports pour une machine protégée



Le menu déroulant **Rapports** vous permet de générer des rapports à la demande pour la machine protégée sélectionnée.

Le rapport Tâche présente l'état des tâches terminées ou ayant échoué pour la machine sélectionnée. Vous pouvez également afficher les tâches ayant échoué dans un rapport sur les défaillances. Pour en savoir plus sur ce type de rapport, voir [Comprendre le rapport de tâche](#).

Le rapport Échec contient des informations sur les tâches de Core qui ont échoué ou ont été annulées sur la machine spécifiée. Pour en savoir plus sur ce type de rapport, voir [Comprendre le rapport des échecs](#).

Pour en savoir plus sur la création de ces rapports, voir [Génération d'un rapport Core à la demande](#).

Affichage des machines répliquées dans le menu de navigation

Si votre Core réplique des machines à partir d'un autre Core Rapid Recovery, le nom d'affichage du Core source s'affiche sous la forme d'un menu déroulant, dans la zone de navigation gauche de la Core Console. Comme tous les libellés de menus de la zone de navigation, le nom du menu Machines répliquées est affiché en majuscules, sous le menu Machines protégées. Par défaut, le menu Machines répliquées est complètement développé et affiche toutes les machines répliquées sur votre Core cible à partir de ce Core source.

Vous pouvez réduire ou développer la liste des machines répliquées de ce Core source en cliquant simplement sur la flèche située à gauche de ce menu.

Chaque menu Machines répliquées s'accompagne d'un menu déroulant sur la droite qui répertorie les fonctions pouvant être exécutées simultanément sur toutes les machines répliquées à partir de ce Core. Cliquez sur la flèche située à droite du menu Machines répliquées pour afficher une liste déroulante des fonctions utilisables. Vous pouvez notamment accomplir les actions suivantes :

- Permet de suspendre la réplication. Si la réplication est actuellement active, l'action s'arrête jusqu'à ce que vous la relanciez.
- Permet de reprendre la réplication. Si la réplication a été interrompue, une nouvelle réplication commence de zéro.
- Forcer la réplication. Réplique à la demande, plutôt qu'à une heure planifiée.
- Supprimer la réplication. Supprime la relation de réplication entre le Core source et le Core cible. Si vous le souhaitez, vous pouvez supprimer les points de restauration stockés sur ce Core. Pour en savoir plus, voir [Suppression d'une réplication](#).

Cliquez directement sur le nom du Core source dans le menu de navigation pour afficher la page **Machines répliquées à partir de [Nom du Core source]** dans la zone de contenu principale. Pour en savoir plus sur les opérations réalisables sur cette page, voir [Affichage des réplifications entrantes et sortantes](#).

Liens connexes

[Suspendre et reprendre la réplication](#)

[Forcer la réplication](#)

[Suppression d'une réplication](#)

Affichage du menu Points de restauration uniquement

Le menu Points de restauration uniquement s'affiche dans le volet de navigation gauche lorsque l'une des conditions suivantes est remplie :

- si votre Core Rapid Recovery conserve des points de restauration d'une machine préalablement protégée ;
- si vous avez supprimé la réplication, mais conservé les points de restauration.

Comme tous les libellés de menus du volet de navigation, le libellé de ce menu est affiché en majuscules.

Vous pouvez réduire ou développer la vue des machines comportant uniquement des points de restauration en cliquant simplement sur la flèche située sur la gauche de ce menu.

Ce menu comprend un menu déroulant sur la droite qui répertorie les fonctions pouvant être exécutées simultanément sur toutes les machines comportant uniquement des points de restauration. Dans ce cas, la seule fonction que vous pouvez effectuer est celle consistant à supprimer les points de restauration du Core.

⚠ PRÉCAUTION : cette action supprime de votre Core toutes les machines ne comportant que des points de restauration Rapid Recovery, et ce de façon définitive. Vous ne pourrez plus restaurer d'informations à partir des points de restauration de ce Core.

Affichage du menu Groupes personnalisés

Le menu des groupes personnalisés s'affiche dans la zone de navigation gauche uniquement si vous avez défini un ou plusieurs groupes personnalisés. Comme pour tous les libellés de menu dans la zone de navigation, la zone de libellé de ce menu est entièrement en majuscules.

Vous pouvez réduire ou développer la vue des éléments de ce menu en cliquant simplement sur la flèche située sur la gauche de ce menu.

Le menu Groupes personnalisés comprend un menu déroulant sur la droite qui répertorie les fonctions pouvant être exécutées simultanément sur tous les éléments semblables de ce groupe.

Pour plus d'informations, voir [Comprendre les groupes personnalisés](#).

Utilisation de la boîte de dialogue Erreur

Lorsqu'une erreur se produit dans l'interface utilisateur de la console Core Rapid Recovery, par exemple en cas de saisie d'un paramètre non valide, une boîte de dialogue Erreur s'affiche. Cette boîte de dialogue indique généralement la cause de l'erreur, fournit des liens vers des informations complémentaires sur l'erreur, et comporte un bouton Fermer. Vous devez fermer la boîte de dialogue Erreur avant de pouvoir continuer, mais il peut s'avérer utile d'afficher plus d'informations sur l'erreur.

Dans la boîte de dialogue Erreur, choisissez parmi les options suivantes :

Les erreurs de l'interface utilisateur entraînant l'apparition de la boîte de dialogue Erreur ne sont pas suivies dans l'onglet Événements Rapid Recovery, car il s'agit de simples erreurs de validation ou de saisie de données. Cependant, lorsque vous cliquez sur l'option Rechercher dans la base de connaissances en cas d'erreur, le lien URL fourni pour cette erreur est enregistré dans le fichier journal CoreAppRecovery.log. Vous pouvez rechercher la chaîne de texte « KB article url generated » dans le journal pour voir l'URL de chacune des erreurs qui a été affichée dans un navigateur. Pour plus d'informations sur le téléchargement ou l'affichage des journaux d'erreur du Core, voir les rubriques [Téléchargement et affichage du fichier journal du Core](#) ou [Accès aux journaux du Core](#), respectivement.

Paramètres du Core

Cette section explique comment gérer et modifier les paramètres de votre Rapid Recovery Core via l'icône  (Paramètres).

Paramètres du Core de Rapid Recovery

Les paramètres du Core de Rapid Recovery sont configurés par défaut pour des performances optimales pour la plupart des utilisateurs. Ces paramètres affectent les performances du Core de Rapid Recovery ou dans certains cas l'affichage des informations dans la Rapid

Recovery Core Console. Sur la barre d'icônes, cliquez sur  (Paramètres) pour accéder aux paramètres du Core. Une liste de tous les

paramètres du Core s'affiche sur la gauche. Vous pouvez cliquer sur le titre de l'un des paramètres de cette liste pour accéder à la configuration complète du paramètre en question, sur la droite. Vous pouvez également faire défiler vers le bas les paramètres du Core, sur la droite, pour voir toutes les options de configuration. Pour plus d'informations, voir [Paramètres du Core de Rapid Recovery](#).

Vous pouvez également accéder aux outils Core tels que l'affichage d'un récapitulatif des informations système ou le téléchargement des fichiers journaux du Core. Pour plus d'informations, voir [Outils au niveau du Core](#).

La liste complète des paramètres du Core de Rapid Recovery que vous pouvez configurer est décrite dans le tableau suivant.

Tableau 7. Paramètres configurables du Core de Rapid Recovery

Paramètre de configuration	Description
Sauvegarde et restauration de la configuration du Core	Rapid Recovery vous permet de sauvegarder les paramètres de configuration du Core sur un fichier XML. Si vous avez un fichier de sauvegarde, vous pouvez l'utiliser pour restaurer ou faire migrer les paramètres du Core. Pour plus d'informations sur la sauvegarde et la restauration des paramètres du Core, voir Sauvegarde et restauration des paramètres du Core .
Généralités	Les paramètres généraux comprennent des options de configuration qui s'appliquent de façon générale au Core de Rapid Recovery, notamment les options d'affichage et les ports utilisés pour le serveur Web et le service Rapid Recovery. Pour plus d'informations sur les paramètres généraux du Core de Rapid Recovery, notamment la manière de configurer ces paramètres, voir Configuration des paramètres généraux du Core .
Mises à jour	Les paramètres de mise à jour contrôlent les aspects de la fonctionnalité de mise à jour automatique, qui vérifie s'il existe des versions mises à jour du logiciel Rapid Recovery. Pour plus d'informations sur les paramètres de mise à jour du Core Rapid Recovery, notamment la manière de configurer ces paramètres, voir Configurer les paramètres de mise à jour .
Tâches nocturnes	Les paramètres des tâches nocturnes sont des tâches automatisées que le Core effectue quotidiennement. Vous pouvez configurer le moment auquel les tâches commencent et quelles tâches sont exécutées. Dell recommande de planifier l'exécution des tâches en dehors des heures de travail normales, afin de réduire leur impact sur le système lorsque la demande en ressources est élevée. Pour plus d'informations, voir Comprendre les travaux nocturnes , Configuration des tâches nocturnes du Core et Personnalisation des tâches nocturnes pour une machine protégée .
File d'attente de transfert	Les paramètres de la file d'attente de transfert contrôlent le nombre de fois que des opérations de transfert vont être tentées si les tâches échouent en raison de l'indisponibilité des ressources. Vous pouvez établir le nombre maximal de transferts simultanés et le nombre maximal de nouvelles tentatives de transfert des données. Pour plus d'informations sur les paramètres de la file d'attente de transfert, voir Modifier les paramètres de la file d'attente de transfert .
Délai d'expiration client	Les paramètres du délai d'expiration client déterminent le laps de temps pendant lequel doivent être tentées des demandes de connexion ou des opérations de lecture/écriture spécifiques avant expiration. Pour plus d'informations sur les paramètres du délai d'expiration client, voir Ajuster les paramètres de délai d'expiration client .
Cache de déduplication DVM	La déduplication est là pour faire en sorte que des blocs d'informations individuels ne soient stockés qu'une seule fois dans votre logithèque, en créant des références pour les blocs de données répétés. Les références sont stockées dans un cache de déduplication. Si des clés de chiffrement sont utilisées, la déduplication survient alors dans chaque domaine de chiffrement. Les paramètres du cache de déduplication DVM vous permettent de configurer la taille et de spécifier des emplacements pour le cache primaire et le cache secondaire, ainsi que l'emplacement du cache des métadonnées.

Paramètre de configuration	Description
	Pour plus d'informations sur le cache de déduplication, voir Compréhension du cache de déduplication et des emplacements de stockage . Pour en savoir plus sur la façon d'ajuster les paramètres, voir Configuration des paramètres du cache de déduplication DVM .
Moteur Replay	Les paramètres Replay Engine contrôlent les informations à propos du canal de communication pour Replay Engine, telles que les paramètres relatifs aux adresses IP ou délais d'expiration, pour mieux adapter les performances à vos besoins en réseau. Pour plus d'informations sur les paramètres du moteur pour Rapid Recovery, voir Configurer les paramètres du moteur Replay.
Déploiement	Les paramètres de déploiement vous permettent de définir des options pour déployer le logiciel agent Rapid Recovery depuis votre Core sur les machines que vous souhaitez protéger. Pour plus d'informations sur la configuration des paramètres de déploiement, voir Configurer les paramètres de déploiement.
Connexion de la base de données	Rapid Recovery stocke les informations transactionnelles dans une base de données de service MongoDB installée localement par défaut sur la machine Core. Vous pouvez configurer ces paramètres pour changer la durée de conservation de ces informations dans la base de données, ou pour changer la taille du pool de connexion afin de permettre plus ou moins de connexions simultanées. Pour plus d'informations sur l'établissement ou la modification des paramètres de connexion de la base de données de service, voir Configurer les paramètres de connexion de la base de données.
Base de données locale	Rapid Recovery affiche des informations sur la page Événements sur les tâches, les événements et les alertes du Core. Rapid Recovery stocke ces informations transactionnelles dans une base de données de service MongoDB installée localement sur la même machine que le Core de Rapid Recovery. Vous pouvez configurer les identifiants (nom d'utilisateur et mot de passe) pour la base de données de service Mongo locale à l'aide des paramètres Base de données locale. Pour en savoir plus sur l'ajustement des paramètres de base de données locale, voir Modification des paramètres de connexion de la base de données locale.
Serveur SMTP	Configurez des paramètres de serveur SMTP (Simple Mail Transfer Protocol) pour le Core pour envoyer par e-mail les informations relatives aux événements du Core. Pour plus d'informations sur la configuration d'un serveur de messagerie SMTP, voir Configurer un serveur de messagerie électronique. REMARQUE : Pour envoyer des informations relatives aux événements par e-mail, vous devez également configurer les paramètres des groupes de notification. Pour plus d'informations sur la façon de spécifier des événements pour pouvoir recevoir des alertes par e-mail, voir Configurer les groupes de notification.
Configuration des clouds	Les paramètres de configuration du Cloud permettent de spécifier les paramètres de configuration des comptes de stockage Cloud pris en charge. Ces paramètres ne permettent pas de créer des comptes cloud. Au lieu de cela, ils associent les comptes de stockage Cloud existants à votre Core de Rapid Recovery de sorte à faciliter les actions telles que l'archivage des informations Rapid Recovery. Pour en savoir plus sur la gestion des informations relatives aux comptes de stockage Cloud sur le Core Rapid Recovery, voir Gestion des comptes Cloud.
Rapports	Les paramètres des rapports comprennent un paramètre de configuration unique qui vous permet de sélectionner la police utilisée lorsqu'un rapport est généré depuis le Core de Rapid Recovery. Pour plus d'informations sur la modification des paramètres de rapport, voir Gestion des paramètres des rapports.
Capacité d'attachement	Les paramètres de la capacité d'attachement vous permettent de spécifier si vous souhaitez effectuer des vérifications de capacité d'attachement de SQL sur la machine protégée, ou si vous souhaitez utiliser l'instance de serveur SQL sur le Core. Si vous spécifiez SQL sur le Core, vous devez fournir les références nécessaires.

Paramètre de configuration	Description
	Pour plus d'informations sur la gestion des paramètres de capacité d'attachement de SQL pour le Core, voir Gestion des paramètres de capacité d'attachement SQL du Core .
Tâches	Les tâches du Core sont créées automatiquement chaque fois que vous lancez des opérations telles que la réplication. Vous pouvez spécifier des paramètres pour chaque tâche à l'aide des paramètres de tâches du Core. Vous pouvez configurer le nombre de tâches à exécuter en même temps. Si des erreurs réseau ou d'autres erreurs de communication empêchent une tâche de réussir du premier coup, vous pouvez définir le nombre de fois qu'une tâche doit être tentée, à l'aide du paramètre Nombre de tentatives. Pour plus d'informations sur les tâches du Core, quelles tâches sont disponibles et comment les configurer, voir Paramètres des tâches du Core.
Licences	À partir de la Core Console, Rapid Recovery vous permet de changer la licence associée à votre Core, de limiter le nombre d'instantanés quotidiens, de voir les informations sur le pool de licences et de contacter le serveur de licences. Pour plus d'informations sur la gestion des licences du Core, voir Gérer les licences. Pour plus d'informations sur la gestion des licences, consultez le Guide Portail des licences Dell Data Protection Rapid Recovery. REMARQUE : Le Guide Portail des licences Dell Data Protection Rapid Recovery a un cycle de publication différent de celui du logiciel Rapid Recovery. Pour consulter les documents les plus récents sur les produits, voir le site Internet de la documentation technique de Dell.
Configuration SNMP	SNMP (Simple Network Management Protocol) est un protocole de gestion des appareils sur un réseau IP. Vous pouvez configurer le Core de Rapid Recovery en tant qu'agent SNMP. Le Core rapporte alors des informations telles que les alertes et l'état des logithèques et des machines protégées. Pour plus d'informations sur l'utilisation du protocole SNMP avec Rapid Recovery, voir Compréhension des paramètres SNMP.
vSphere	Les paramètres du Core de vSphere s'appliquent uniquement aux utilisateurs de la protection de machines virtuelles sans agent. Si vous utilisez un hôte vSphere, ces paramètres incluent les paramètres de connexion qui s'appliquent aux machines virtuelles. Pour plus d'informations sur les paramètres vSphere pour une protection sans agent VMware ou ESXi, voir Configuration des paramètres vSphere.
Envoi des journaux	Lorsque cette option est définie sur Oui, le Rapid Recovery Core télécharge les fichiers journaux vers Dell pour effectuer une analyse dans le cadre de l'effort continu déployé pour l'amélioration de la qualité globale du produit. Ce paramètre est facultatif.

Configuration des paramètres généraux du Core

Les paramètres généraux du Core de Rapid Recovery incluent le nom d'affichage du Core, le port de serveur Web, le port de service et les paramètres régionaux (la langue d'affichage de la console Core).

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **Général**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à faire apparaître l'en-tête Général. Les paramètres généraux du Core s'affichent.
- 3 Cliquez sur le paramètre général à modifier.

Le paramètre sélectionné devient modifiable, comme un champ de texte ou un menu déroulant.

- 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 8. Informations sur les paramètres généraux

Zone de texte	Description
Nom d'affichage	Entrez un nouveau nom d'affichage pour le core. Il s'agit du nom qui s'affichera dans la console Core de Rapid Recovery. Vous pouvez entrer jusqu'à 64 caractères.
Port du serveur internet	Entrez un numéro de port pour le serveur Internet. Le port par défaut est 8006.
Port de service	Entrez un numéro de port pour le service Core de Rapid Recovery. Le port par défaut est 8006.
Paramètres régionaux	Dans la liste déroulante Paramètres régionaux, choisissez la langue que vous voulez utiliser pour l'affichage. Vous avez le choix entre l'allemand, l'anglais, le chinois simplifié, le coréen, l'espagnol, le français, le japonais et le portugais.

REMARQUE : Si vous modifiez la langue, confirmez le message qui apparaît vous indiquant que le service Core de Rapid Recovery doit redémarrer pour afficher la nouvelle langue définie dans la console Core. Vous pouvez redémarrer ce service à partir du Gestionnaire des tâches de Windows.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Configurer les paramètres de mise à jour

Rapid Recovery inclut la fonction Mise à jour automatique. Lorsque vous installez le Core Rapid Recovery, vous pouvez choisir d'effectuer la mise à jour automatique du logiciel du Core Rapid Recovery lorsque de nouvelles mises à jour sont disponibles, et déterminer la fréquence à laquelle vous souhaitez que le système recherche des mises à jour.

En règle générale, les numéros de version de Rapid Recovery incluent quatre blocs d'informations, séparés par des points décimaux : les numéros de version principale, version secondaire, la révision et de build. Par exemple, la première version renommée de Rapid Recovery a été 6.0.1.609. La prochaine version a été 6.0.2.142.

La fonction de mise à jour automatique compare tous les chiffres d'un numéro de version. Si vous activez la mise à jour automatique, le logiciel Core est mis à jour sans intervention uniquement lorsque les numéros de version majeure et mineure sont identiques. Par exemple, la mise à jour automatique aurait lieu de Core version 6.0.1.609 à 6.0.2.142 (tous deux commençant par 6.0). Sur la même machine, le Core ne pourrait pas se mettre à jour automatiquement de 6.0.2.142 à 6.1.1.XXX, car les chiffres après la première valeur décimale sont différents. Au lieu de cela, vous serez prévenu (par une bannière dans la partie supérieure de la Core Console) qu'une mise à jour du logiciel Core est disponible. Cette notification vous donne la possibilité d'examiner les remarques concernant cette mise à jour, pour que vous déterminiez par vous-même si la mise à jour vers la version la plus récente du Core est adaptée à vos besoins.

REMARQUE : pour en savoir plus sur l'installation du logiciel du Core Rapid Recovery, voir le guide d'installation et de mise à niveau de Dell Data Protection | Rapid Recovery.

Vous pouvez afficher et modifier les paramètres que le système utilise pour rechercher des mises à jour à n'importe quel moment.

PRÉCAUTION : lorsque vous utilisez la réplication, si vous configurez votre système pour qu'il installe les mises à jour automatiquement, cela peut entraîner la mise à niveau du Core source avant celle du Core cible, ce qui peut conduire à un échec de la réplication ou à l'incapacité d'établir une nouvelle réplication entre les Cores. Pour les utilisateurs de réplication, Dell conseille aux administrateurs d'appliquer les mises à jour automatiques uniquement sur le Core cible, puis de mettre à niveau le Core source manuellement, et en dernier lieu de mettre à niveau les machines protégées.

Exécutez la procédure suivante pour définir les paramètres de mise à jour.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Mises à jour**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à afficher l'en-tête Mises à jour. Les paramètres Mises à jour du Core s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 9. Informations sur les paramètres de mise à jour

Zone de texte	Description
Vérification des nouvelles mises à jour	Sélectionnez la fréquence de recherche et d'installation de mises à jour par Rapid Recovery. Vous pouvez choisir parmi les options suivantes : • Jamais • Tous les jours • Toutes les semaines • Tous les mois Si vous choisissez les mises à jour automatiques, une fois le seuil de temps sélectionné écoulé, si une mise à jour est disponible, celle-ci est installée après l'exécution des tâches nocturnes.
Installation des mises à jour	Indiquez comment vous voulez gérer les mises à jour éventuellement disponibles en choisissant l'une des options suivantes : • Ne jamais rechercher les mises à jour • Me signaler les mises à jour, mais ne pas les installer automatiquement • Installer automatiquement les mises à jour
État	L'état indique si de nouvelles mises à jour sont disponibles.
Dernière vérification	Le champ Dernière vérification indique la date et l'heure auxquelles le système a recherché une mise à jour pour la dernière fois. Cliquez sur Vérifier maintenant pour déterminer immédiatement si une mise à jour de logiciel est disponible. Cette vérification s'effectue indépendamment de la fréquence définie.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Comprendre les travaux nocturnes

Les travaux nocturnes sont des tâches quotidiennes automatisées qui se déclenchent à un moment prédéterminé en dehors des heures normales d'ouverture. Ces travaux sont gourmands en mémoire et consistent en diverses vérifications de et consolidation de l'intégrité des données qui sont plus efficaces lorsque le core Rapid Recovery est moins actif.

Tous les travaux nocturnes et leur champ d'application sont décrits dans le tableau suivant. Les travaux nocturnes peuvent être gérés au niveau du core (et donc sont applicables à toutes les machines protégées sur ce dernier). Les travaux nocturnes qui sont applicables également à une machine protégée spécifique sont signalés comme étant de portée « machine protégée »).

Tableau 10. Travaux nocturnes

Nom du travail	Champ d'application	Description
 Modification	S/O	Cette option affiche la boîte de dialogue Travaux nocturnes, dans laquelle vous pouvez activer, désactiver ou modifier les paramètres de chacun des travaux nocturnes.
Heure des travaux nocturnes	Tous	Ce paramètre représente l'heure de démarrage planifiée pour les travaux nocturnes. Dell recommande de configurer l'exécution de ceux-ci par votre cœur à un moment de faible activité. L'heure par défaut est 00h00.
Cumul	Core ou machine protégée	Applique la stratégie de conservation pour les données sauvegardées en combinant ou cumulant des points de restauration selon la planification imposée par la stratégie. Vous pouvez personnaliser la stratégie sur le core, laquelle, dès lors, s'appliquera par défaut à toutes les machines protégées sur ce dernier. Par défaut, le travail de cumul s'exécute pour l'ensemble du core. Vous pouvez également cliquer sur  afin de définir pour quelles machines protégées effectuer un cumul à l'aide de la stratégie du core. Pour plus d'informations sur l'utilisation sur une machine protégée d'une stratégie de conservation qui diffère de la stratégie par défaut définie sur le core, voir Personnalisation des paramètres de la stratégie de conservation pour une machine protégée.
Vérifier la capacité d'attachement de bases de données SQL	Machine protégée	Vérifie l'intégrité des points de récupération contenant des bases de données SQL. Procédure : • Monter le point de restauration le plus récent pour les groupes de protection contenant des bases de données. • Se connecter à la base de données depuis SQL Server. • Ouvrir la base de données. • Fermer la base de données. • Démonter le point de restauration. Pour activer cette vérification nocturne, spécifiez l'instance SQL Server à utiliser pour effectuer les vérifications de capacité d'attachement des bases de données SQL Server sur des machines protégées.  REMARQUE : Cette option n'apparaît que si vous protégez un SQL Server sur votre core.
Télécharger les journaux depuis des machines protégées	Core	Télécharge vers le core les journaux depuis les machines protégées afin que ces journaux puissent être envoyés à un serveur de journalisation.
Consolider les instantanés VMware de machines virtuelles protégées	Core ou machine protégée	Ce travail nocturne est utile si vous utilisez les API VMware natives pour protéger des machines sans Rapid Recovery Agent. Vous devez périodiquement consolider les instantanés VMware. L'activation de ce travail nocturne vous permet d'effectuer ces consolidations quotidiennement. Ce travail nocturne contient un seul paramètre, qui est le nombre maximum de consolidations simultanées, lequel nombre doit être compris entre 1 et 100.
Vérifier l'intégrité des points de restauration	Core ou machine protégée	Vérifie l'intégrité des points de récupération de chaque machine protégée. Par défaut, l'option <code>Check integrity of recovery points</code> n'est pas activée. Procédure : • Monter le point de restauration le plus récent pour chacun des groupes de protection. • Énumérer les fichiers et dossiers de chaque volume. • Examine la validité des points de restauration. • Démonter le point de restauration.

Nom du travail	Champ d'application	Description
Vérifier la somme de contrôle de bases de données Exchange	Machine protégée	Vérifie l'intégrité des points de récupération contenant des fichiers de base de données Exchange (EDB). REMARQUE : Cette option n'apparaît que si vous protégez un Exchange Server sur votre core.
Tronquer les journaux SQL (modèle de restauration simple uniquement)	Machine protégée	Maintient la taille des journaux SQL Server en tronquant le journal des transactions de la base de données pour le faire correspondre au dernier point de restauration. REMARQUE : Cette option n'apparaît que si vous protégez un SQL Server sur votre core.
Tronquer les journaux Exchange	Machine protégée	Maintient la taille des journaux Exchange en tronquant le journal des transactions de la base de données pour le faire correspondre au dernier point de restauration. REMARQUE : Cette option n'apparaît que si vous protégez un Exchange Server sur votre core.
Journaliser les statistiques des référentiels	Core	Envoie à un serveur de journalisation les statistiques des référentiels.
Supprimer les anciens événements et les anciens travaux	Core	Maintient l'échelle de la base de données des événements en supprimant les anciens événements. Le nombre de jours est configurable ; par défaut, il est de 30 jours.

Configuration des tâches nocturnes du Core

Lorsqu'une tâche nocturne est activée sur le Core Rapid Recovery, la tâche sélectionnée est exécutée une fois par jour aux heures spécifiées pour toutes les machines protégées par le Core. À l'inverse, si vous désactivez une des tâches nocturnes au niveau Core, la tâche spécifiée ne s'exécute plus pour toutes les machines protégées par le Core.

REMARQUE : si la portée d'une tâche nocturne, comme indiqué dans la rubrique [Comprendre les travaux nocturnes](#), comprend des machines protégées, vous pouvez configurer cette tâche nocturne de sorte qu'elle s'applique uniquement à une ou plusieurs machines protégées spécifiques, de manière individuelle. Pour en savoir plus sur l'application des paramètres de tâches nocturnes spécifiques à une machine protégée, voir [Personnalisation des tâches nocturnes pour une machine protégée](#).

Puisque les tâches nocturnes consomment beaucoup de mémoire, Dell vous conseille de configurer votre Core pour qu'il les exécute à des heures d'activité réduite. L'heure par défaut d'exécution des tâches nocturnes est 00:00 (minuit). Si une autre heure convient mieux, modifiez ce paramètre dans le champ Heure des tâches nocturnes en suivant cette procédure.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page **Paramètres**, cliquez sur **Tâches nocturnes**.
 - Faites défiler dans la partie inférieure droite de la page **Paramètres** jusqu'à afficher l'en-tête Tâches nocturnes. Les paramètres Tâches nocturnes du Core s'affichent.
- 3 Pour modifier une tâche nocturne, ou pour modifier l'heure à laquelle les tâches nocturnes commencent à s'exécuter, cliquez sur **Modifier**. 
La boîte de dialogue **Tâches nocturnes** s'affiche.
- 4 Si vous voulez modifier l'heure d'exécution des tâches nocturnes, saisissez une nouvelle heure dans le champ **Heure des tâches nocturnes**.

- 5 Dans la première colonne, cliquez pour sélectionner chaque option relative aux tâches nocturnes à définir pour le Core. Cliquez sur n'importe quelle option sélectionnée pour la désélectionner.
- 6 Cliquez sur **OK**.
La boîte de dialogue **Tâches nocturnes** se ferme. Vos paramètres relatifs aux tâches nocturnes du Core sont enregistrés.

Modifier les paramètres de la file d'attente de transfert

Les paramètres de file d'attente de transfert sont définis au niveau du Core ; ils déterminent le nombre maximal de transfert simultanés et le nombre maximal de tentatives de transfert des données.

Effectuez cette procédure pour modifier les paramètres de file d'attente de transfert.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des opérations suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **File d'attente de transfert**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à faire apparaître l'en-tête File d'attente de transfert. Les paramètres de la File d'attente de transfert du Core s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 11. Informations sur les paramètres de File d'attente de transfert

Zone de texte	Description
Nombre maximal de transferts simultanés	Entrez une valeur pour mettre à jour le nombre de transferts simultanés. Vous pouvez choisir un nombre entre 1 et 60. Plus le nombre est petit, plus la charge sur le réseau et les autres ressources du système est faible. Plus le nombre d'agents traités augmente, plus la charge sur le système augmente.
Nombre maximal de tentatives	Entrez une valeur pour définir le nombre maximal de tentatives avant l'annulation de l'opération de transfert. Vous pouvez choisir un nombre entre 1 et 60.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Ajuster les paramètres de délai d'expiration client

Les paramètres de délai d'expiration client contrôlent le laps de temps pendant lequel diverses opérations vont être tentées avant l'expiration de cette opération.

REMARQUE : Dell recommande de conserver les paramètres d'expiration par défaut, sauf si vous rencontrez des problèmes spécifiques à votre environnement particulier et qu'un représentant du support technique de Dell vous conseille de modifier ces paramètres.

Effectuez cette procédure pour définir les paramètres de délai d'attente client.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Délai d'attente client**.

- Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à afficher l'en-tête Délai d'attente client. Les paramètres Délai d'attente client du Core s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
 - 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.
 - 5

Tableau 12. Informations sur les paramètres d'expiration du délai d'attente client

Paramètre	Description
Délai d'expiration de la connexion	Contrôle le délai d'attente avant l'expiration de la connexion entre le Core et les machines protégées lors de l'envoi de données selon le protocole de transfert de données hypertexte (http). Saisissez le temps imparti avant l'expiration du délai d'attente de la connexion. Ce paramètre utilise le format HH:MM:SS.
REMARQUE : le paramètre par défaut est 0:05:00, soit cinq minutes.	
Délai d'expiration des lectures/écritures	Contrôle le délai d'attente avant l'expiration de la connexion entre le Core et les machines protégées lors de la lecture ou de l'écriture de données en flux selon le protocole http. Exemple : réception de blocs de données modifiés à partir d'une machine protégée sur le Core pour un snapshot incrémentiel. Saisissez le temps imparti avant l'expiration du délai pendant un événement de lecture/d'écriture. Ce paramètre utilise le format HH:MM:SS.
REMARQUE : le paramètre par défaut est 0:05:00, soit cinq minutes.	
Délai d'expiration de l'interface utilisateur de connexion	Contrôle le délai d'attente avant l'expiration de la connexion entre l'interface utilisateur graphique et le service Core Rapid Recovery sur le protocole http. Saisissez le temps imparti avant l'expiration du délai d'attente de l'UI de la connexion. Ce paramètre utilise le format HH:MM:SS.
REMARQUE : le paramètre par défaut est 0:05:00, soit cinq minutes.	
Délai d'expiration de l'interface utilisateur des lectures/écritures	Contrôle le délai d'attente avant l'expiration de la connexion entre les flux de données de lecture et d'écriture et le service Core Rapid Recovery sur le protocole http. Saisissez la période souhaitée avant l'expiration du délai pendant des événements de lecture/d'écriture. Ce paramètre utilise le format HH:MM:SS.
REMARQUE : le paramètre par défaut est 0:05:00, soit cinq minutes.	

- 6 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Compréhension du cache de déduplication et des emplacements de stockage

La déduplication globale réduit la quantité d'espace de stockage disque nécessaire aux données sauvegardées par votre Core. Chaque logithèque est dédupliquée en stockant chaque bloc unique une fois physiquement sur le disque et en utilisant des références virtuelles ou des pointeurs vers ces blocs dans les sauvegardes suivantes. Pour identifier des blocs dupliqués, Rapid Recovery comprend un cache de déduplication pour les logithèques DVM (Deduplication Volume Manager). Le cache contient des références vers des blocs uniques.

Par défaut, le cache de déduplication des logithèques DVM est de 1,5 Go. Cette taille est suffisante pour un grand nombre de logithèques. Tant que la taille du cache n'est pas atteinte, les données sont dédupliquées dans la logithèque. Lorsque les données redondantes saturer le cache de déduplication, votre logithèque ne peut plus tirer entièrement parti de la déduplication pour les nouvelles données ajoutées. La

quantité de données enregistrées dans la logithèque avant la saturation du cache de déduplication varie en fonction du type de données à sauvegarder et des utilisateurs.

Vous pouvez augmenter la taille du cache de déduplication DVM en modifiant le paramètre correspondant sur le Core Rapid Recovery. Pour en savoir plus sur l'augmentation de la taille du cache, voir la rubrique [Configuration des paramètres du cache de déduplication DVM](#).

Lorsque vous augmentez la taille du cache de déduplication DVM, vous devez tenir compte de deux éléments : l'espace disque et l'utilisation de la mémoire vive.

Espace disque. Deux copies du cache de déduplication DVM sont stockées sur le disque : un cache principal et un cache secondaire, qui est une copie parallèle. Ainsi, si vous utilisez la taille de cache par défaut de 1,5 Go pour une logithèque DVM, 3 Go de stockage de disque sont utilisés dans votre système. Lorsque vous augmentez la taille du cache, la quantité d'espace disque utilisée reste proportionnellement égale au double de la taille du cache. Pour pouvoir assurer un bon fonctionnement et une tolérance aux pannes, le Core modifie dynamiquement la priorité de ces caches. Les deux caches sont nécessaires, la seule différence étant que le cache principal est enregistré en premier.

Utilisation de la mémoire vive. Lorsque le Core Rapid Recovery démarre, il charge le cache de déduplication dans la mémoire vive. De cette manière, la taille du cache affecte l'utilisation de la mémoire sur votre système. La quantité totale de mémoire vive utilisée par le cache dépend de nombreux facteurs. Ces facteurs incluent les opérations en cours d'exécution, le nombre d'utilisateurs, le nombre de machines protégées et la taille du cache de déduplication. Chaque opération exécutée par le Core (transfert, réplication, consolidation, etc.) utilise plus de mémoire vive. Lorsqu'une opération prend fin, la consommation de la mémoire diminue en conséquence. Cependant, les administrateurs doivent envisager d'utiliser la quantité de mémoire vive maximale pour assurer un bon fonctionnement.

Les paramètres par défaut du Core Rapid Recovery placent le cache principal, le cache secondaire et le cache des métadonnées des logithèques DVM dans le répertoire AppRecovery. Ce dossier est installé sur la machine Core.

REMARQUE : selon vos paramètres, ce répertoire peut être masqué sur le Core Rapid Recovery. Pour l'afficher, il peut être nécessaire de changer le panneau de configuration Options de dossier pour afficher les fichiers, dossiers et lecteurs masqués.

Si le Core Rapid Recovery est installé sur le lecteur C, ces emplacements sont généralement les suivants :

Tableau 13. Emplacements de stockage par défaut des paramètres du cache de déduplication DVM

Paramètre	Emplacement de stockage par défaut
Emplacement du cache principal	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Emplacement du cache secondaire	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Emplacement du cache des métadonnées	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Vous pouvez modifier l'emplacement de stockage de ces caches. Par exemple, pour améliorer la tolérance aux pannes, vous pouvez changer l'emplacement du cache secondaire en le plaçant sur un lecteur physique différent de celui du cache principal, à condition que le Core Rapid Recovery ait accès à cet emplacement.

Pour en savoir plus sur la modification des emplacements de stockage de ces paramètres, voir la rubrique [Configuration des paramètres du cache de déduplication DVM](#).

Dell vous recommande de gérer le stockage de déduplication séparément. La déduplication se produit dans une seule logithèque (et non sur plusieurs). Si vous utilisez un chiffrement basé sur le Core, la déduplication est davantage limitée pour les données protégées par une seule clé, étant donné que pour des raisons de sécurité, chaque clé fait office de domaine de chiffrement unique.

Pour en savoir plus sur la déduplication, voir [Déduplication sous Rapid Recovery](#).

Configuration des paramètres du cache de déduplication DVM

Suivez les étapes de cette procédure pour configurer les paramètres du cache de déduplication des logithèques DVM.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **Cache de déduplication DVM**. Ce paramètre s'affiche uniquement si votre Core contient une ou plusieurs logithèques DVM.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à faire apparaître l'en-tête Cache de déduplication DVM. Le paramètre Cache de déduplication DVM du Core s'affiche.
- 3 Vous pouvez à tout moment restaurer les paramètres du cache de déduplication DVM par défaut. Pour cela, effectuez les opérations suivantes :
 - a En haut de la zone des paramètres du cache de déduplication, cliquez sur **Restaurer les valeurs par défaut**. La boîte de dialogue Restaurer les valeurs par défaut s'affiche
 - b Cliquez sur **Oui** pour confirmer la restauration.
- 4 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 5 Pour modifier les paramètres du cache de déduplication, entrez les informations de configuration comme indiqué dans le tableau suivant.

Tableau 14. Informations sur les paramètres du cache de déduplication DVM

Paramètre	Description
 Restaurer les valeurs par défaut	Cette commande réinitialise les emplacements du cache DVM sur les emplacements par défaut du système, qui sont décrits pour chaque paramètre.
Emplacement du cache principal	Si vous voulez changer l'emplacement du cache principal des logithèques DVM, dans la zone de texte Emplacement du cache principal, saisissez le chemin d'un emplacement de stockage accessible pour le Core. L'emplacement par défaut est : C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache Comme les caches principal et secondaire ont la même taille, le stockage collectif de ces deux caches nécessite le double de l'espace alloué à la taille de cache de déduplication. Par exemple, si vous spécifiez la taille par défaut de 1,5 Go pour le cache de déduplication, vous devez vous assurer que chacun des deux emplacements de stockage dispose d'au moins 1,5 Go. En particulier, si les deux emplacements appartiennent au même disque (C, par exemple), il doit exister au moins 3 Go d'espace disque disponible.
Emplacement du cache secondaire	Si vous voulez changer l'emplacement du cache secondaire des logithèques DVM, dans la zone de texte Emplacement du cache secondaire, saisissez le chemin d'un emplacement de stockage accessible pour le Core. L'emplacement par défaut est : C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Emplacement des métadonnées de cache	Si vous voulez changer l'emplacement des métadonnées de cache des logithèques DVM, dans la zone de texte Emplacement des métadonnées de cache, saisissez le chemin d'un emplacement de stockage accessible pour le Core. L'emplacement par défaut est :

Paramètre	Description
	C:\ProgramData\AppRecovery\RepositoryMetadata\CacheMetadata
Taille du cache de déduplication, en Go	Si vous souhaitez modifier la taille du cache de déduplication des logithèques DVM, dans la zone de texte Taille du cache de déduplication, entrez une nouvelle valeur (en Go). L'emplacement par défaut est : C:\ProgramData\AppRecovery\RepositoryMetadata\SecondaryCache La taille de cache minimale est 1,5 Go. En outre, la taille du cache ne peut pas être supérieure à la moitié de la mémoire vive installée.
6	Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Configurer les paramètres du moteur Replay

Vous pouvez configurer les informations concernant le moteur Replay, qui est le canal de communication de Rapid Recovery. Ces réglages déterminent les paramètres du Core permettant d'avoir une communication efficace.

En règle générale, Dell recommande d'utiliser les paramètres par défaut. Dans certains cas, vous pouvez être invité par le support technique de Dell à modifier ces paramètres pour tenter d'ajuster les performances afin de répondre à vos besoins réseau spécifiques.

Suivez les étapes de cette procédure pour définir les paramètres du moteur Replay.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **Replay Engine**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à afficher l'en-tête Replay Engine. Les paramètres du Core Replay Engine s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 15. Informations sur les paramètres Replay Engine

Zone de texte	Description
Adresse IP	Le Core utilise cette adresse IP lors de l'exécution du montage et de la restauration d'un point de restauration, pour permettre des commentaires entre les machines protégées et le Core. L'adresse IP de Replay Engine est automatiquement renseignée avec l'adresse IP de la machine Core. Si vous saisissez manuellement l'adresse IP du serveur, cette valeur sera utilisée lorsque la machine protégée ne parviendra pas à résoudre l'adresse IP fournie automatiquement. Vous n'aurez à définir cette valeur manuellement que si les machines protégées rencontrent des problèmes de communication avec le Core.
Port privilégié	Entrez un numéro de port ou acceptez la valeur par défaut. Le port par défaut est 8007. Le port est utilisé pour indiquer le canal de communication pour le moteur Replay.

Zone de texte	Description
Port en cours d'utilisation	Représente le port en cours d'utilisation pour la configuration du moteur Replay.
Autoriser l'attribution automatique de port	Cliquez pour autoriser l'attribution automatique de port TCP.
Groupe Admin	Entrez un nouveau nom pour le groupe Admin. Le nom par défaut est BUILTIN\Administrators.
Longueur d'E/S asynchrones minimale	Entrez une valeur ou choisissez la valeur par défaut. Décrit la longueur d'E/S asynchrones minimale. Le paramètre par défaut est 65536.
Expiration du délai d'attente de lecture	Entrez une valeur de délai de lecture ou choisissez la valeur par défaut. Le paramètre par défaut est 00:05:00.
Expiration du délai d'attente d'écriture	Entrez une valeur ou choisissez la valeur par défaut. Le paramètre par défaut est 00:05:00.
Taille du tampon de réception	Entrez une taille de tampon entrant ou la valeur par défaut. Le paramètre par défaut est 8192.
Taille du tampon d'envoi	Entrez une taille de tampon sortant ou acceptez la valeur par défaut. Le paramètre par défaut est 8192.
Aucun délai	Il est recommandé de ne pas sélectionner cette case afin de ne pas affecter le réseau. Si vous déterminez que vous avez besoin de modifier ce paramètre, contactez au préalable le support technique de Dell.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Configurer les paramètres de déploiement

Rapid Recovery permet de télécharger des programmes d'installation depuis le Core Rapid Recovery vers les machines à protéger.

Vous pouvez configurer les paramètres relatifs au déploiement du logiciel Agent Rapid Recovery depuis votre Core vers les machines à protéger.

Exécutez la procédure suivante pour définir les paramètres de déploiement.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres à gauche de la page Paramètres, cliquez sur **Déployer**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Déployer. Les paramètres Déployer du Core s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 16. Informations sur les paramètres de déploiement

Zone de texte	Description
Nom du programme d'installation du logiciel Agent	Le nom du fichier par défaut est Agent-Web.exe. Si vous souhaitez modifier ce nom de fichier pour une raison quelconque, vous pouvez utiliser ce paramètre afin de définir un nouveau nom pour le fichier exécutable du programme d'installation Web du Core. Le fichier diffuse un téléchargement de la dernière version du programme d'installation du Core Rapid Recovery, qui s'exécute directement sur le Web et permet de suspendre et de reprendre le processus selon vos besoins.
Adresse du Core	Entrez l'adresse de votre serveur Core. Celle-ci comprend normalement le protocole, le nom et le port de votre serveur Core, et le répertoire où résident les fichiers Core. Par exemple, si votre serveur est Exemple, ce paramètre sera https://exemple:8006/apprecovery/admin/Core
Délai d'expiration échec réception	Le laps de temps pendant lequel le déploiement du logiciel Agent doit être tenté avant l'expiration de l'opération. Le paramètre par défaut est 00:25:00, soit vingt-cinq minutes. Si vous souhaitez modifier ce paramètre, saisissez la durée d'expiration de la tentative de déploiement du logiciel Agent par le système, pendant des événements de lecture ou d'écriture. Ce paramètre utilise le format HH:MM:SS.
Nombre maximal d'installations parallèles	Ce paramètre contrôle le nombre de déploiements maximal du logiciel Agent que le Core peut tenter simultanément. Le paramètre par défaut est 100.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Configurer les paramètres de connexion de la base de données

Rapid Recovery affiche des informations sur la page Événements sur les tâches, les événements et les alertes du Core. Rapid Recovery stocke ces informations transactionnelles dans une base de données de service MongoDB installée localement par défaut sur la machine Core. Vous pouvez configurer ces paramètres pour changer la durée de conservation de ces informations dans la base de données, ou pour changer la taille du pool de connexion afin de permettre plus ou moins de connexions simultanées.

Si vous utilisez un deuxième Core Rapid Recovery, vous pouvez configurer les paramètres de connexion de la base de données sur le premier Core de façon à ce qu'ils pointent vers la deuxième machine Core. De cette manière, les données événements des deux Cores seront stockées dans la base de données MongoDB sur le deuxième Core.

Sinon, vous pouvez configurer les paramètres de connexion de la base de données sur le Core de façon à ce qu'ils pointent vers une autre machine sur laquelle a été installé séparément MongoDB qui est accessible sur le réseau pour le Core de Rapid Recovery. Les données transactionnelles sur les événements de votre Core sont alors enregistrées sur cette base de données de service, et non localement. Pour plus d'informations sur l'établissement ou la modification des paramètres de connexion de la base de données de service, voir [Configurer les paramètres de connexion de la base de données](#).

 **REMARQUE :** pour en savoir plus sur l'affichage des informations sur les événements du Core Rapid Recovery, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Les clients peuvent choisir de spécifier l'installation de la base de données de service MongoDB sur une autre machine accessible sur le réseau pour le Core Rapid Recovery. Si la base de données de service utilisée par votre Core Rapid Recovery est installée sur une machine différente de celle qui héberge le Core Rapid Recovery, vous devez fournir les informations d'identification de la base de données (nom d'utilisateur et mot de passe) dans ces paramètres.

Suivez les étapes de cette procédure pour modifier les paramètres de connexion de la base de données de service utilisée par le Core Rapid Recovery.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Connexion à la base de données**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à afficher l'en-tête Connexion à la base de données. Les paramètres Connexion à la base de données du Core s'affichent.
- 3 Dans la partie supérieure de la zone Paramètres de connexion de la base de données, vous pouvez effectuer les opérations suivantes :
 - Cliquez sur **Tester la connexion** pour vérifier vos paramètres.
Il est recommandé de tester la connexion lorsque vous modifiez les paramètres de connexion de la base de données.
 - Cliquez sur **Restaurer les valeurs par défaut** pour restaurer tous les paramètres de connexion de la base de données par défaut. Vous êtes invité à confirmer cette action, ce qui entraîne l'abandon des éventuels paramètres de connexion de la base de données personnalisés.
- 4 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 5 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 17. Informations sur les paramètres de connexion de la base de données

Zone de texte	Description
Nom de l'hôte	Entrez un nom d'hôte de la connexion de la base de données.  REMARQUE : lorsque localhost est le paramètre spécifié pour l'hôte, la base de données MongoDB est installée localement sur la machine qui héberge le Core.
Port	Entrez un numéro de port pour la connexion de la base de données.  REMARQUE : le paramètre par défaut est 27017.
Nom d'utilisateur	Entrez le nom d'un utilisateur disposant de privilèges administratifs pour la base de données de service MongoDB.  REMARQUE : si le paramètre Nom d'hôte est localhost, ce champ n'a pas besoin d'être rempli.
Mot de passe	Saisissez le mot de passe associé au nom d'utilisateur que vous avez spécifié.  REMARQUE : si le paramètre Nom d'hôte est localhost, ce champ n'a pas besoin d'être rempli.
Période de rétention (jours)	Entrez le nombre de jours pendant lesquels vous souhaitez conserver l'historique des événements et des tâches dans la base de données de service.
Taille maximale du pool de connexion	Définit le nombre maximal de connexions de la base de données mises en cache pour permettre une réutilisation dynamique.  REMARQUE : le paramètre par défaut est 100.
Taille minimale du pool de connexion	Définit le nombre minimal de connexions de la base de données mises en cache pour permettre une réutilisation dynamique.  REMARQUE : le paramètre par défaut est 0.

- 6 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Modification des paramètres de connexion de la base de données locale

Vous pouvez afficher les événements système associés au Core Rapid Recovery sur la page Événements. Le Core Rapid Recovery stocke ces informations transactionnelles dans une base de données de service MongoDB. Par défaut, cette base de données est installée localement sur la machine Core, et le nom d'hôte des paramètres de connexion de la base de données par défaut est localhost. Dans ce cas, l'interface de boucle de rappel contourne le matériel d'interface réseau, et les informations d'identification de la base de données ne sont pas requises.

Éventuellement, afin de renforcer la sécurité, vous pouvez spécifier explicitement les informations d'identification (comprenant un nom d'utilisateur et un mot de passe) de la base de données MongoDB utilisée par le Core Rapid Recovery.

REMARQUE : pour en savoir plus sur l'affichage des informations sur les événements du Core Rapid Recovery, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#). Pour en savoir plus sur les paramètres de connexion de la base de données, voir [Configurer les paramètres de connexion de la base de données](#).

Suivez les étapes de cette procédure de modification des paramètres de connexion de la base de données pour spécifier des informations d'identification de la base de données.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Paramètres de base de données locale**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Paramètres de base de données locale.Les paramètres Base de données locale du Core s'affichent.
- 3 Cliquez sur le paramètre à modifier.
Vous pouvez maintenant modifier le paramètre sélectionné.
- 4 Saisissez les informations d'identification appropriées pour la connexion à la base de données de service, comme indiqué dans le tableau suivant.

Tableau 18. Informations sur les paramètres de base de données locale

Zone de texte	Description
Nom d'utilisateur	Entrez le nom d'un utilisateur disposant de privilèges administratifs pour la base de données de service MongoDB.
Mot de passe	Saisissez le mot de passe associé au nom d'utilisateur que vous avez spécifié.

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Gestion des paramètres du serveur SMTP

Si vous configurez les paramètres de serveur SMTP (Simple Mail Transfer Protocol) du Core, vous pouvez envoyer des notifications de tâche, d'événement et d'alerte par e-mail.

Des informations sur la configuration d'un serveur de messagerie SMTP sont fournies dans la rubrique [Configurer un serveur de messagerie électronique](#).

REMARQUE : pour envoyer des informations relatives aux événements par e-mail, vous devez également configurer les paramètres des groupes de notification. Pour plus d'informations sur la façon de spécifier des événements pour pouvoir recevoir des alertes par e-mail, voir [Configurer les groupes de notification](#).

Gestion des paramètres de configuration Cloud

Dans Rapid Recovery, vous pouvez associer les comptes de stockage dont vous disposez auprès de fournisseurs de stockage Cloud avec votre Core Rapid Recovery. Vous pouvez ainsi archiver les informations provenant de machines protégées lorsque les données deviennent obsolètes.

Rapid Recovery s'intègre à Amazon™ S3, Microsoft Azure et aux fournisseurs de Cloud géré utilisant la technologie OpenStack en « open source ».

Pour en savoir plus sur la gestion des informations relatives aux comptes de stockage Cloud sur le Core Rapid Recovery, voir [Gestion des comptes Cloud](#).

Gestion des paramètres des rapports

Vous pouvez générer des rapports pour le Core Rapid Recovery ou pour les machines protégées. Pour en savoir plus sur les rapports que vous pouvez générer, voir [Générer et afficher des rapports](#).

Suivez les étapes de cette procédure pour gérer les paramètres de génération de rapports du Core.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Rapports**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Rapports. Les paramètres **Rapports** du Core s'affichent. Les paramètres des rapports sont présentés dans le tableau suivant.

Option	Description
Restaurer les valeurs par défaut	Cette option restaure tous les paramètres par défaut des rapports. Les valeurs par défaut de chaque paramètre sont répertoriées ci-dessous.
Police	Cette option contrôle la police par défaut utilisée pour les rapports. La police par défaut est Trebuchet MS. Vous pouvez la remplacer par toute police disponible sur votre système.
Format du papier	Cette option contrôle le format de papier utilisé par défaut pour l'impression de rapports. Le format par défaut est A4. Vous avez le choix entre les formats de papier suivants : • Lettre • Tabloïd • Ledger • Légal • A3 • A4 • Exécutif • B4 • Enveloppe C3 • Enveloppe C4
Orientation de page	Cette option contrôle l'orientation de page des rapports exportés. L'orientation par défaut est Portrait. Vous avez le choix entre les dispositions suivantes : • Portrait

Option	Description
	• Paysage
3	Pour modifier les paramètres des rapports, cliquez sur le champ du paramètre approprié. Le champ du paramètre correspondant s'affiche sous la forme d'un menu déroulant configurable.
4	Cliquez sur le menu déroulant, puis sélectionnez l'une des valeurs disponibles. Par exemple, dans le champ Police, cliquez sur Times New Roman .
5	Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer. L'option choisie s'affiche désormais comme le nouveau réglage du paramètre de rapports sélectionné.

Gestion des paramètres de capacité d'attacheement SQL du Core

Les vérifications de capacité d'attacheement de SQL se produisent dans le cadre des tâches nocturnes de Rapid Recovery. Pour alléger les coûts d'octroi de licences, Rapid Recovery vous propose deux options pour effectuer les vérifications de capacité d'attacheement : via une instance sous licence du serveur SQL installée sur la machine Core de Rapid Recovery ou via l'instance du serveur SQL déjà installée sur votre machine protégée. Cette seconde option est maintenant le paramètre par défaut. Toutefois, si votre machine protégée est déjà en cours d'utilisation à l'heure à laquelle les tâches nocturnes sont lancées, effectuez les vérifications avec une instance du serveur SQL sur le Core.

En résumé, le processus de gestion des paramètres de capacité d'attacheement SQL du Core comprend les tâches suivantes :

- Montez le dernier point de restauration pour les groupes de protection contenant des bases de données.
 - Connectez-vous à la base de données depuis le serveur SQL.
 - Ouvrez la base de données.
 - Fermez la base de données.
 - Démontez le point de restauration.
- Pour activer cette vérification nocturne, spécifiez une instance de SQL Server à utiliser pour effectuer les vérifications de la capacité d'attacheement des bases de données SQL Server sur les machines protégées.

REMARQUE : Cette option ne s'affiche pas si vous ne protégez pas un serveur SQL sur votre Core.

Pour configurer le Core de façon à ce qu'il vérifie la capacité d'attacheement SQL dans le cadre des tâches nocturnes, suivez les étapes décrites suivantes.

REMARQUE : si vous sélectionnez l'option par défaut pour utiliser l'instance du serveur SQL installée sur la machine protégée, cette instance du serveur SQL gère la capacité d'attacheement SQL pour toutes les machines SQL protégées. Si vous ne souhaitez pas appliquer ce paramètre à toutes les machines SQL protégées, sélectionnez Utiliser le serveur SQL sur le Core. Pour effectuer les vérifications de capacité d'attacheement sur le Core, vous devez installer ou utiliser une version sous licence du serveur SQL sur la machine Core.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **Capacité d'attacheement**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à afficher l'en-tête Capacité d'attacheement.
- 3 Pour utiliser l'instance du serveur SQL installée sur la machine du serveur SQL protégée, sélectionnez **Utiliser le serveur SQL sur la machine protégée**. Il s'agit de l'option par défaut.
- 4 Pour utiliser l'instance du serveur SQL installée sur le Core de Rapid Recovery, sélectionnez **Utiliser le serveur SQL sur le Core**, puis saisissez les informations d'authentification, comme indiqué dans le tableau suivant.

Tableau 19. Informations sur les identifiants du serveur SQL

Zone de texte	Description
SQL Server	Dans le menu déroulant du serveur SQL, sélectionnez l'instance du serveur SQL appropriée, à partir du serveur Core.
Type d'informations d'identification	Sélectionnez la méthode d'authentification appropriée pour vos identifiants parmi les options suivantes : - Windows - SQL
Nom d'utilisateur	Indiquez un nom d'utilisateur pour accéder au serveur SQL sur le Core, en fonction de votre type d'identifiant sélectionné.
Mot de passe	Indiquez un mot de passe pour accéder au serveur SQL sur le Core, en fonction de votre type d'identifiant sélectionné.

5 Cliquez sur **Test de connexion**.

REMARQUE : si vous n'avez pas entré les bons identifiants, un message vous indique que vous ne pouvez pas vous connecter avec ces identifiants. Corrigez les identifiants, puis tentez de vous connecter à nouveau.

6 Lorsque vous êtes satisfait de vos modifications, cliquez sur **Appliquer**.

Compréhension des tâches de Core

Les tâches de Core sont des processus que le Core de Rapid Recovery effectue pour la prise en charge de ses opérations, notamment la sauvegarde de points de restauration, la réplication de données, l'archivage de données, l'exportation de données vers des machines virtuelles, la maintenance de logithèques, etc. Les tâches de Core sont lancées automatiquement pour certaines opérations, telles que la réplication ou l'archivage, selon une planification établie. Vous pouvez également invoquer certaines tâches à la demande à partir de divers éléments de la console Core.

- Lors de l'affichage ou de la modification des paramètres de tâches de Core, chaque tâche de Core dispose de deux paramètres : Nombre maximum de tâches simultanées et Nombre de tentatives.
 - Le paramètre Nombre maximal de tâches simultanées détermine le nombre de tâches de ce type qui peuvent être exécutées en même temps.
 - Le paramètre Nombre de tentatives détermine le nombre de tentatives de la tâche avant son abandon, si des erreurs réseau ou d'autres erreurs de communication empêchent la tâche de réussir du premier coup.
- Dans le tableau Tâches de Core, la colonne Paramètres indique si la tâche répertoriée est incluse dans les paramètres de tâches de Core par défaut ou si elle doit y être ajoutée explicitement.

Le tableau suivant présente les principales tâches de Core disponibles, ainsi que leurs fonctions.

Tableau 20. Tâches de Core

Nom de la tâche	Description	Nombre maximal de tâches simultanées	Nombre de tentatives	Paramètres
Vérifier la capacité d'attachement de bases de données SQL dans les instantanés	Permet au Core de vérifier la cohérence des bases de données SQL et d'assurer la disponibilité de tous les fichiers MDF (données) et LDF (journaux) dans l'instantané de sauvegarde. Processus : Monter le dernier point de restauration pour les groupes de protection contenant des bases de données SQL.	1	0	Par défaut

Nom de la tâche	Description	Nombre maximal de tâches simultanées	Nombre de tentatives	Paramètres
	- Monter la base de données. En cas d'exécution de la capacité d'attachement à partir du serveur SQL protégé, effectuer le montage à l'aide du chemin UNC. - Connectez-vous à la base de données depuis le serveur SQL. - Effectuer la vérification de la capacité d'attachement. - Effectuer les opérations de nettoyage. - Fermez la base de données. - Démonter la base de données. - Démontez le point de restauration.			
Vérifier la somme de contrôle de bases de données Exchange	Vérifie l'intégrité des points de restauration contenant des bases de données Exchange. Processus :	1	0	Par défaut
	- Monter le dernier point de restauration pour les groupes de protection contenant des bases de données SQL. - Connectez-vous à la base de données depuis le serveur SQL. - Ouvrez la base de données. - Fermez la base de données. - Démontez le point de restauration.			
Vérifier la montabilité des bases de données Exchange	Vérifie que les bases de données Exchange peuvent être montées.	1	0	Par défaut
Répliquer les données de machines protégées depuis la source distante	Transfère une copie des points de restauration d'une machine protégée à partir d'un Core source vers un Core cible. Cette tâche s'exécute sur le Core cible qui reçoit les points de restauration de réplication entrante.	3	0	Par défaut
Répliquer des données de machines protégées vers une cible distante	Transfère une copie des points de restauration d'une machine protégée à partir d'un Core source (sur lequel ils étaient enregistrés à l'origine) vers un Core cible. Cette tâche s'exécute sur le Core source et contrôle la réplication sortante.	1	3	Par défaut
Restaurer les points de restauration	Applique la stratégie de rétention pour vos données sauvegardées via la combinaison ou la consolidation de points de restauration sur la planification définie dans la stratégie de rétention.	1	0	Par défaut
Vérifier les points de restauration	Vérifie l'intégrité des points de restauration.	1	0	Ajouter
Supprimer tous les points de restauration	Supprime l'intégralité des points de restauration d'une machine protégée.	1	0	Ajouter
Supprimer la chaîne de points de restauration	Supprime une chaîne de points de restauration complète d'une machine protégée.	1	0	Ajouter

Nom de la tâche	Description	Nombre maximal de tâches simultanées	Nombre de tentatives	Paramètres
Supprimer la plage de points de restauration	Supprime un ensemble de points de restauration d'une machine protégée, par identificateur de point de restauration ou plage de dates.	1	0	Ajouter
Déployer le logiciel agent sur des machines	Déploie le logiciel agent Rapid Recovery sur la ou les machine(s) spécifiée(s).	1	0	Ajouter
Télécharger les bibliothèques Exchange	Télécharge les bibliothèques Microsoft Exchange depuis la machine protégée vers la machine du Core, sur le chemin C:\ProgramData\AppRecovery\ExchangeLibraries .	1	0	Ajouter
Exporter vers une archive	Crée une sauvegarde dans le chemin spécifié avec une archive des points de restauration sélectionnés. Processus : - Monter des points de restauration. - Écrire des données dans les sauvegardes. - Démontez le point de restauration.	1	0	Ajouter
Exporter vers la machine virtuelle	Exporte les données à partir d'un point de restauration spécifique d'une machine protégée vers le chemin cible, comme une machine virtuelle. Processus : - Monter le point de restauration. - Créer une machine virtuelle à partir du point de restauration des données dans le chemin de destination. - Démontez le point de restauration.	1	0	Ajouter
Importer des archives	Importe un point de restauration à partir de la sauvegarde spécifiée sur une archive de Core précédemment créée.	1	0	Ajouter
Gérer la logithèque	Effectue une vérification de la logithèque. Processus : - Vérifier le système de fichiers de la logithèque. - Monter le point de restauration. - Recalculer le cache de déduplication de la logithèque. - Charger les points de restauration à partir de la logithèque.	1	0	Ajouter
Monter les instantanés du point de restauration	Effectue le montage du point de restauration vers le chemin spécifié.	1	0	Ajouter
Protéger les machines virtuelles ESX®	Ajoute toutes les machines virtuelles spécifiées à une protection sans agent. La tâche est exécutée immédiatement après l'ajout d'une protection sans agent pour une ou plusieurs machines virtuelles au Core, à l'aide de l'Assistant Protéger plusieurs machines. La tâche définit le numéro d'identification de chaque machine virtuelle spécifiée, écrit les informations	1	0	Ajouter

Nom de la tâche	Description	Nombre maximal de tâches simultanées	Nombre de tentatives	Paramètres
	concernant le Core dans un fichier de configuration et extrait les métadonnées à partir du fichier.			
Restaurer depuis le point de restauration	Effectue une restauration à partir d'un point de restauration vers une machine cible spécifiée. Processus : • Monter le point de restauration. • Écrire toutes les données du point de restauration vers la machine spécifiée. • Démontez le point de restauration.	1	0	Ajouter
Charger les journaux	Charge des journaux vers le serveur spécifié.	1	0	Ajouter

Certaines tâches de Core sont incluses dans les Paramètres. Les paramètres des tâches vous permettent de spécifier combien de tâches simultanées du même type le Core peut exécuter, ainsi que le nombre de nouvelles tentatives à effectuer si la première tentative échoue.

Pour plus d'informations sur ces paramètres, voir [Paramètres des tâches du Core](#).

Pour plus d'informations sur l'ajout de tâches aux paramètres du Core, voir [Ajout de tâches de Core aux paramètres](#).

Pour plus d'informations sur la modification des paramètres des tâches dans la liste de paramètres, voir [Modification des paramètres des tâches du Core](#).

Paramètres des tâches du Core



Lorsque vous sélectionnez (Paramètres) dans la barre d'icônes, vous accédez aux paramètres de certaines tâches du Core. La zone **Tâches** sur la page Paramètres du Core vous permet de déterminer deux paramètres pour chaque type de tâche répertorié :

- 1 Le nombre maximal de tâches de ce type que le Core peut tenter de manière simultanée. Ce paramètre doit être défini sur une valeur comprise entre 1 et 50.
- 2 Le nombre de fois qu'une tâche doit être tentée si une erreur réseau ou de communication empêche la tâche de réussir du premier coup. Ce paramètre doit être défini sur une valeur comprise entre 0 et 10.

Plusieurs tâches sont automatiquement incluses dans les paramètres du Core. Ces tâches comprennent une valeur Par défaut dans la colonne Paramètres, comme indiqué dans la rubrique [Compréhension des tâches de Core](#).

Vous pouvez ajouter d'autres tâches aux paramètres si vous souhaitez configurer ces paramètres pour contrôler le nombre maximal de tâches ou de nouvelles tentatives pour ces fonctions. Ces tâches comprennent une valeur Ajouter dans la colonne Paramètres. Pour plus d'informations sur la façon d'ajouter ces tâches au tableau Paramètres, voir [Ajout de tâches de Core aux paramètres](#).

Les tâches du Core non disponible dans la zone Paramètres ne permettent pas de définir ces deux paramètres.

Pour les tâches répertoriées dans Paramètres, vous pouvez modifier les paramètres existants. Cela vous permet de personnaliser les deux paramètres, de supprimer un type de tâche de la liste des paramètres de tâche ou de restaurer les paramètres par défaut. Pour plus d'informations, voir la rubrique [Modification des paramètres des tâches du Core](#).

Ajout de tâches de Core aux paramètres

Les paramètres de tâches du Core vous permettent de définir, pour chaque type de tâche, le nombre maximal de tâches que le Core peut tenter d'exécuter simultanément et le nombre de nouvelles tentatives d'exécution d'une tâche en cas d'échec de la première tentative.

Chaque type de tâche de Core comprend des valeurs par défaut pour ces deux paramètres, comme indiqué dans la rubrique [Paramètres des tâches du Core](#). Cette liste indique également les types de tâches inclus par défaut aux paramètres du Core.

L'ajout d'une tâche de Core aux paramètres permet de modifier ces paramètres pour le type de tâche ajouté.

Suivez les étapes de la procédure ci-après pour ajouter une tâche aux paramètres du Core.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Tâches**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Tâches. Les paramètres Tâches du Core s'affichent.
- 3 Sur la page Paramètres du Core, sous Tâches, cliquez sur  **Ajouter**. La boîte de dialogue Paramètres des tâches s'ouvre.
- 4 Dans la boîte de dialogue **Paramètres de la tâche**, dans le champ **Tâches**, sélectionnez le nom d'une tâche à ajouter aux paramètres du Core. Ces tâches sont présentées dans la rubrique [Paramètres des tâches du Core](#).
- 5 Pour définir le nombre maximal de tâches que le Core peut tenter d'exécuter simultanément, dans la zone de texte **Nombre maximal de tâches simultanées**, saisissez une nouvelle valeur comprise entre 1 et 50.
- 6 Pour définir le nombre de tentatives que le Core doit entreprendre avant d'abandonner la tâche, dans la zone de texte **Nombre de tentatives**, saisissez une nouvelle valeur comprise entre 0 et 10.
- 7 Cliquez sur **Enregistrer**. La boîte de dialogue Paramètres de la tâche se ferme, et vos nouveaux paramètres de tâche sont appliqués.

Modification des paramètres des tâches du Core

Les paramètres de tâches du Core vous permettent de définir, pour chaque type de tâche, le nombre maximal de tâches que le Core peut tenter d'exécuter simultanément et le nombre de nouvelles tentatives d'exécution d'une tâche en cas d'échec de la première tentative.

Chaque type de tâche de Core comprend des valeurs par défaut pour ces deux paramètres, comme indiqué dans la rubrique [Compréhension des tâches de Core](#). Cette liste indique également les types de tâches inclus par défaut aux paramètres du Core. Lorsque vous modifiez les paramètres de tâche du Core, vous pouvez réaliser les opérations suivantes :

- Vous pouvez personnaliser les paramètres de chaque type de tâche du Core.
 - Vous pouvez supprimer un type de tâche dans la liste des paramètres du Core. Cette fonction n'est pas disponible si le type de tâche est inclus aux paramètres par défaut.
- ① **REMARQUE :** la suppression d'une tâche des paramètres du Core supprime simplement le type de tâche de cette liste. Pour modifier de nouveau les paramètres du Core de ce type de tâche ultérieurement, vous pouvez l'ajouter à la liste, comme indiqué dans la rubrique [Ajout de tâches de Core aux paramètres](#).
- Vous pouvez restaurer les paramètres par défaut de tout type de tâche.
- ① **REMARQUE :** bien que vous puissiez uniquement utiliser cette fonction pour les types de tâches inclus dans les paramètres par défaut du Core, vous pouvez restaurer les valeurs par défaut d'autres types de tâches en les supprimant de la liste et en les ajoutant de nouveau.

Suivez la procédure ci-dessous pour modifier les paramètres d'une tâche.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Tâches**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Tâches. Les paramètres Tâches du Core s'affichent.

- 3 Dans la grille des tâches, sélectionnez une tâche à supprimer de la liste. Dans le menu déroulant  de cette tâche, sélectionnez **Supprimer**.
La tâche est supprimée de la liste.
- 4 Dans la grille des tâches, sélectionnez dans la liste une tâche dont vous souhaitez réinitialiser les paramètres. Dans le menu déroulant  de cette tâche, sélectionnez **Réinitialiser aux valeurs par défaut**.
Les paramètres par défaut de cette tâche sont réinitialisés.
- 5 Dans la grille des tâches, sélectionnez une tâche à modifier. Dans le menu déroulant  de cette tâche, sélectionnez **Modifier**.
- 6 La boîte de dialogue Paramètres de la tâche : [JobName] s'ouvre.
- 7 Pour modifier le nombre maximal de tâches que le Core peut tenter simultanément, dans le champ Nombre maximal de tâches simultanées, entrez une nouvelle valeur comprise entre 1 et 50.
- 8 Pour modifier le paramètre relatif au nombre de tentatives supplémentaires que le Core doit entreprendre avant d'abandonner la tâche, dans la zone de texte Nombre de tentatives, saisissez une nouvelle valeur comprise entre 0 et 10.
- 9 Cliquez sur **Enregistrer**.
La boîte de dialogue Paramètres de la tâche se ferme, et vos nouveaux paramètres de tâche sont appliqués.

Gérer les licences

De nombreux utilisateurs du Core de Rapid Recovery débutent avec une licence d'évaluation, qui offre des fonctions limitées. Une licence d'évaluation est valable pendant 14 jours, et peut être étendue une fois par l'administrateur du groupe pour passer à une licence de 28 jours. Une fois la période d'évaluation expirée, le Core de Rapid Recovery arrête de prendre des instantanés jusqu'à l'obtention et l'enregistrement d'une licence hors évaluation valide.

 **REMARQUE :** pour en savoir plus sur la saisie de la clé de licence ou sur les informations de fichier (par exemple, pour effectuer une mise à jour ou passer d'une licence d'évaluation à une licence à long terme valide), voir [Mise à jour ou modification d'une licence](#).

Les licences sont validées à l'aide de fichiers de licence ou de clés de licence.

Les **fichiers de licence** sont des fichiers texte qui se terminent par l'extension de fichier **.lic**. Voici des exemples de fichiers de licence :

- Les fichiers de licence peuvent comporter neuf caractères, et sont composés de trois groupes de chiffres arabes séparés par un tiret ; par exemple, 123-456-789.lic.
- Les licences basées sur des logiciels peuvent s'afficher au format Logiciel-<Nom du groupe>.lic, avec le groupe nommé selon le nom du client ou le compte ; par exemple, Software-YourCompany.lic.
- Les licences d'appliance Dell peuvent s'afficher au format <Appliance Series>-<Nom du groupe>.lic, avec le groupe nommé selon le nom du client ou le compte ; par exemple, DL4X00 Series-YourCompany.lic.

Les **clés de licence** comportent 30 caractères et sont composées de six groupes de caractères alphanumériques anglais, séparés par un tiret. Voici un exemple de format de clé de licence : ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11.

Rapid Recovery vous permet de gérer des licences ou de contacter le serveur de licences directement à partir de la console Core. Pour

cela, sélectionnez  (Paramètres) à partir de la barre d'icônes et cliquez sur **Octroi de licences**.

Les paramètres Octroi de licences contiennent les informations suivantes :

Détails de la licence :

-  **Modifier la licence.** Vous permet de modifier une licence existante associée au Core, via le chargement d'un fichier de licence ou la saisie d'une clé de licence.
-  **Ajouter une licence.** Cette option est disponible uniquement pour les appliances de sauvegarde Dell et vous permet de charger un fichier de licence ou de saisir une clé de licence.

- **Groupe portail des licences.** Cette option ouvre le portail des licences pour la gestion de groupes.
- **Type de licence.** Les types de licence sont Évaluation, Abonnement ou Entreprise. Pour plus d'informations, voir la rubrique À propos des types de licence de logiciel du Portail des licences Dell Data Protection | Rapid Recovery dans le guide d'utilisation Portail des licences Dell Data Protection | Rapid Recovery.
- **État de la licence.** Indique l'état de la licence. Un statut actif garantit la prise d'instantanés telle qu'elle a été planifiée. Si la licence est bloquée, qu'elle a expiré, ou si le Core n'est pas en mesure de communiquer avec le Portail des licences Dell Data Protection | Rapid Recovery une fois passé le délai de grâce, les instantanés sont suspendus jusqu'à ce que l'état de la licence soit corrigé.

Contraintes de licence :

- **Nombre maximal d'instantanés par jour.** Indique le nombre maximal de sauvegardes possibles avec la licence spécifiée.

Pool de licences :

- **Taille de pool.** Le pool de licences correspond au nombre de licences hors évaluation qui sont disponibles pour être affectées à des groupes et des sous-groupes dans le Portail des licences Dell Data Protection | Rapid Recovery. La taille du pool indique le nombre des licences pouvant être affectées. Pour plus d'informations, voir la rubrique "Compréhension des pools de licences" dans le Guide d'utilisation *Portail des licences Dell Data Protection | Rapid Recovery*.
- **Protégées par ce Core.** Indique le nombre de machines du pool de licences qui sont protégées par ce Core.
- **Total protégé dans le groupe.** Indique le nombre total des machines protégées dans le même groupe de licences que ce Core.

Serveur de licences. Ces paramètres s'appliquent aux licences standard (phone home). Ces paramètres ne s'appliquent pas aux appliances et aux autres licences de type « non-phone-home ».

- **Adresse du serveur de licences.** Affiche une URL active pour le serveur de licences associé à ce Core.
- **Dernière réponse du serveur de licences.** Indique si la dernière tentative de communication avec le portail du serveur des licences a été réussie.
- **Dernier contact avec le serveur de licences.** Affiche la date et l'heure du dernier contact réussi avec le serveur d'octroi de licences.
- **Prochaine tentative de contact du serveur d'octroi de licences.** Indique le prochain couple date/heure planifié pour tenter une communication avec le serveur de licences.
- **Contacteur maintenant.** Ce bouton contacte le serveur de licences à la demande. Utilisez cette option après avoir apporté des modifications à votre configuration de licence, pour enregistrer immédiatement ces modifications, au lieu d'attendre la prochaine tentative planifiée.

Pour plus d'informations sur les licences, voir le *Guide d'utilisation du Portail des licences Dell Data Protection | Rapid Recovery*.

Pour plus d'informations sur l'ajout ou la modification d'un fichier ou d'une clé de licence, voir [Mise à jour ou modification d'une licence](#).

Pour plus d'informations sur la manière de contacter le serveur de portail des licences, voir [Contact du serveur Portail des licences Dell Data Protection | Rapid Recovery](#)

Vous pouvez également voir les informations sur les licences pour une seule machine protégée. Pour plus d'informations, voir [Afficher les informations sur la licence d'une machine](#).

Mise à jour ou modification d'une licence

Après la mise à niveau ou l'achat d'une licence Rapid Recovery à long terme, vous recevrez un fichier ou une clé de licence par e-mail.

Suivez les étapes de cette procédure pour mettre à niveau votre licence d'évaluation ou modifier votre licence existante, puis associez-la à la console Core Rapid Recovery.

REMARQUE : les utilisateurs d'appliances de sauvegarde Dell peuvent également ajouter des licences au Core, si nécessaire. Pour plus d'informations, voir [Ajout d'une licence](#).

Pour en savoir plus sur l'obtention d'une clé de licence, ou pour obtenir des détails sur l'utilisation du Portail des licences pour télécharger des logiciels, enregistrer des appliances, gérer des souscriptions de licences et de groupes de licences, et générer des rapports sur le Portail des licences, voir le guide d'utilisation du *Portail des licences Dell Data Protection | Rapid Recovery*.

Si vous venez d'installer un nouveau Core et êtes invité à choisir un fichier de licence ou une clé, passez à l'[étape 5](#).

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Paramètres).
- 3 Faites défiler vers la partie inférieure droite de la page **Paramètres** jusqu'à faire apparaître l'en-tête Octroi de licences. Les paramètres du Core relatifs à l'octroi de licences s'affichent.
- 4 Pour mettre à jour ou modifier la licence existante associée à votre Core, dans la partie supérieure de la zone des paramètres Détails de la licence du Core, cliquez sur  **Modifier la licence**.
La boîte de dialogue **Modifier la licence** s'affiche.
- 5 Pour définir une clé de licence ou télécharger un fichier de licence, effectuez l'une des opérations suivantes :
 - a Si vous souhaitez *saisir manuellement* la clé de licence, dans la boîte de dialogue Modifier la licence, saisissez la clé avec précaution, puis cliquez sur **Continuer**.
La boîte de dialogue se ferme et le fichier de licence sélectionné est authentifié. Cette licence est maintenant associée à votre Core.
 - b Si vous souhaitez *télécharger* un fichier de licence, dans la boîte de dialogue Modifier la licence, cliquez sur **Choisir un fichier**. Dans la boîte de dialogue **Charger un fichier**, accédez au système de fichiers et recherchez le nouveau fichier de licence à utiliser. Par exemple, recherchez `Software-YourCompany.lic`.
 - c Cliquez sur le fichier de licence, puis sur **Ouvrir**.
La boîte de dialogue Charger un fichier se ferme. Le fichier de licence sélectionné s'affiche dans la boîte de dialogue Modifier la licence.
 - d Dans la boîte de dialogue **Modifier la licence**, cliquez sur **Continuer**.
La boîte de dialogue se ferme et le fichier de licence sélectionné est authentifié. Cette licence est maintenant associée à votre Core.
- 6 Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Serveur de licences. Les paramètres Octroi de licences du Core s'affichent.
- 7 Dans la zone Serveur de licences, cliquez sur **Contacter maintenant**.
Dès que la licence est appliquée au serveur de licences, les machines protégées associées sont automatiquement mises à jour avec la nouvelle licence.

Ajout d'une licence

Les propriétaires d'une appliance de sauvegarde Dell peuvent ajouter une ou plusieurs licences à la console Core de Rapid Recovery.

Après la mise à niveau ou l'achat d'une licence Rapid Recovery, vous recevrez un fichier ou une clé de licence par e-mail.

Vous pouvez également mettre à jour ou modifier une licence existante via la console Core. Pour plus d'informations, voir [Mise à jour ou modification d'une licence](#).

❗ REMARQUE : seuls les utilisateurs d'une appliance de sauvegarde Dell peuvent voir le bouton Ajouter une appliance.

❗ REMARQUE : pour en savoir plus sur l'obtention d'une clé de licence, voir le guide d'utilisation du *Portail des licences Dell Data Protection / Rapid Recovery*.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Paramètres).
- 3 Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à faire apparaître l'en-tête Octroi de licences. Les paramètres du Core relatifs à l'octroi de licences s'affichent.
- 4 Pour ajouter une licence et l'associer à votre Core, en haut de la zone des paramètres du Détails de la licence, cliquez sur **Ajouter une licence**. Dans la boîte de dialogue **Ajouter une licence**, effectuez l'une des opérations suivantes :
 - a Si vous souhaitez *saisir manuellement* la clé de licence, dans la boîte de dialogue Modifier la licence, saisissez la clé avec précaution, puis cliquez sur **Continuer**.

La boîte de dialogue se ferme et le fichier de licence sélectionné est authentifié. Cette licence est maintenant associée à votre Core.

- b Si vous souhaitez *télécharger* un fichier de licence, dans la boîte de dialogue Modifier la licence, cliquez sur **Choisir un fichier**. Dans la boîte de dialogue **Charger un fichier**, accédez au système de fichiers et recherchez le nouveau fichier de licence à utiliser. Par exemple, recherchez `Software-YourCompany.lic`.

- c Cliquez sur le fichier de licence, puis sur **Ouvrir**.

La boîte de dialogue Charger un fichier se ferme. Le fichier de licence sélectionné s'affiche dans la boîte de dialogue Modifier la licence.

- d Dans la boîte de dialogue **Modifier la licence**, cliquez sur **Continuer**.

La boîte de dialogue se ferme et le fichier de licence sélectionné est authentifié. Cette licence est maintenant associée à votre Core.

- 5 Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Serveur de licences.

Les paramètres Octroi de licences du Core s'affichent.

- 6 Dans la zone Serveur de licences, cliquez sur **Contacter maintenant**.

Dès que la licence est appliquée au serveur de licences, les machines protégées associées sont automatiquement mises à jour avec la nouvelle licence.

Contact du serveur Portail des licences Dell Data Protection | Rapid Recovery

La console Core Rapid Recovery contacte régulièrement le serveur du portail pour rester à jour en appliquant les éventuelles modifications apportées au Portail des licences Dell Data Protection | Rapid Recovery.

Pour les licences hors évaluation, le Core Rapid Recovery contacte le Portail des licences toutes les heures. Si le Core ne parvient pas à joindre le Portail des licences après ce « délai de grâce » de 10 jours, le Core arrête de créer des instantanés.

En règle générale, la communication avec le serveur du Portail des licences est établie automatiquement à des intervalles définis. Cependant, la communication peut être initiée à la demande.

Suivez les étapes de cette procédure pour contacter le serveur du Portail des licences.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Sur la barre d'icônes, cliquez sur **Paramètres**, puis faites défiler vers la partie inférieure droite de la page **Paramètres** pour faire apparaître l'en-tête Serveur de licences.
- 3 Dans la zone Serveur de licences, cliquez sur **Contacter maintenant**.

Compréhension des paramètres SNMP

SNMP (Simple Network Management Protocol) est un protocole de gestion des appareils sur un réseau IP. SNMP est utilisé essentiellement pour surveiller l'apparition de problèmes devant être signalés sur les appareils d'un réseau. Ce protocole utilise des composants logiciels (agents) pour transmettre des informations à des ordinateurs administratifs (gestionnaires). Un agent SNMP gère les requêtes du gestionnaire pour obtenir ou définir certains paramètres. L'agent SNMP peut également envoyer des interruptions (notifications concernant des événements spécifiques) au gestionnaire.

Les objets de données gérés par des agents SNMP sont organisés dans un fichier Base d'informations de gestion (MIB) contenant des identificateurs d'objet (OID). Chaque OID contient une variable qui peut être lue ou définie à l'aide de SNMP.

Rapid Recovery inclut la prise en charge de SNMP version 1.0.

Vous pouvez configurer le Core de Rapid Recovery en tant qu'agent SNMP. Le Core rapporte alors des informations telles que les alertes et l'état des logithèques et des machines protégées. Un hôte SNMP peut lire ces informations à l'aide d'une application autonome appelée « navigateur SNMP ». Vous pouvez installer le navigateur SNMP sur toute machine accessible sur le réseau pour le Core de Rapid Recovery.

Pour vous assurer que les notifications d'événement du Core SNMP puissent être reçues par le navigateur SNMP, vérifiez que les options de notification pour un groupe de notification sont correctement configurées pour une notification via une interruption SNMP.

REMARQUE : vous pouvez utiliser le groupe par défaut ou créer un groupe de notification personnalisé. Le processus est identique.

Ouvrez le groupe de notification, sélectionnez l'onglet **Options de notification**, puis vérifiez que l'option **Notifier via une interruption SNMP** est activée. Le groupe de notification spécifie le nombre d'interruptions par défaut sur 1. Si nécessaire, vous pouvez modifier le nombre d'interruptions pour vous assurer qu'il correspond au paramètre attendu par le navigateur SNMP.

Pour plus d'informations et des détails spécifiques sur la configuration des options de notification, voir [Configurer les groupes de notification](#).

Vous pouvez également télécharger un fichier MIB à partir du Core de Rapid Recovery. Ce fichier peut être lu par un navigateur SNMP de façon plus conviviale que les données qu'il reçoit directement du Core.

Cette section contient les rubriques suivantes :

- [Configuration des paramètres SNMP](#)
- [Téléchargement du fichier MIB SNMP](#)

Configuration des paramètres SNMP

Utilisez les paramètres SNMP pour contrôler la communication entre le Core et le navigateur SNMP. Cela inclut le port SNMP, le port de réception des interruptions et le nom d'hôte du destinataire des interruptions.

Suivez cette procédure pour configurer les paramètres SNMP du Core.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Paramètres, puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core à gauche de la page Paramètres, cliquez sur **Configuration SNMP**.
 - Faites défiler vers la partie inférieure droite de la page Paramètres jusqu'à faire apparaître l'en-tête Configuration SNMP. Les paramètres Configuration SNMP s'affichent.
- 3 Modifiez les paramètres SNMP comme indiqué dans le tableau suivant.

Tableau 21. Informations sur les paramètres de connexion SNMP

Zone de texte	Description
Port entrant	Saisissez un numéro de port pour la connexion SNMP.
REMARQUE : le paramètre par défaut est 8161.	
Port de réception des interruptions	Saisissez le numéro de port du destinataire des interruptions. Le paramètre par défaut est 162.
Nom d'hôte récepteur des interruptions	Saisissez un nom d'hôte pour la connexion SNMP.
REMARQUE : le nom d'hôte par défaut est localhost.	

- 4 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

Téléchargement du fichier MIB SNMP

Le protocole SNMP (Simple Network Management Protocol) est utilisé pour surveiller les appareils d'un réseau pour les conditions qui nécessitent votre attention. Lorsque le Core Rapid Recovery est défini en tant qu'agent SNMP, le Core rapporte des informations, concernant par exemple les alertes, l'état de la logithèque et les machines protégées. Ces informations peuvent être lues par un hôte SNMP utilisant une application autonome appelée navigateur SNMP.

Les objets de données gérés par des agents SNMP sont organisés dans un fichier de base d'informations de gestion (MIB) contenant des identificateurs d'objet (OID). Chaque OID contient une variable qui peut être lue ou définie à l'aide de SNMP.

Vous pouvez télécharger un fichier MIB à partir du Core Rapid Recovery. Ce fichier, appelé `dell-aa-core.mib`, peut être lu par un navigateur SNMP de manière plus conviviale que les données qu'il reçoit directement du Core.

Suivez cette procédure pour télécharger le fichier MIB SNMP à partir du Core Rapid Recovery.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis cliquez sur **Téléchargements**.
La page **Téléchargements** s'affiche.
- 3 Faites défiler vers le bas jusqu'au volet Autres fichiers.
- 4 Pour télécharger le fichier MIB, cliquez sur le lien de téléchargement **Fichier MIB SNMP**.
Les paramètres Configuration SNMP s'affichent.
- 5 Dans la boîte de dialogue **Ouverture de dell-aa-core.mib**, effectuez l'une des opérations suivantes :
 - Pour ouvrir le fichier journal, sélectionnez **Ouvrir avec**, choisissez une application de navigateur SNMP permettant d'afficher le fichier texte MIB, puis cliquez sur **OK**.
Le fichier `dell-aa-core.mib` s'ouvre dans l'application sélectionnée.
 - Pour enregistrer le fichier localement, sélectionnez **Enregistrer le fichier**, puis cliquez sur **OK**.
Le fichier `dell-aa-core.mib` est enregistré dans votre dossier Téléchargements. Il est possible de l'ouvrir à l'aide d'un navigateur SNMP ou d'un éditeur de texte.

Configuration des paramètres vSphere

VMware vSphere est une suite de logiciels de virtualisation, à partir de laquelle vous pouvez gérer des machines virtuelles ESXi ou vCenter Server. Avec vSphere, vous n'avez plus besoin de charger le logiciel agent Rapid Recovery sur les machines virtuelles pour les protéger. Cette fonction est appelée « protection sans agent » et s'applique uniquement aux machines virtuelles.

Suivez cette procédure pour configurer les paramètres vSphere du Core.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **vSphere**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à afficher l'en-tête vSphere.
Les paramètres vSphere s'affichent.
- 3 Modifiez les paramètres vSphere comme indiqué dans le tableau suivant.

Tableau 22. Informations sur les paramètres du Core vSphere

Élément de l'IU	Type d'interface utilisateur	Description
Durée de vie d'une connexion	Zone de sélection numérique	Définit le délai avant l'expiration de la connexion avec le serveur ESXi. Ce paramètre utilise le format HH:MM:SS. REMARQUE : le paramètre par défaut est 00:10:00, soit dix minutes.
Nombre maximal de consolidations simultanées	Champ de texte	Définit le nombre maximal de consolidations simultanées pour les machines virtuelles protégées. REMARQUE : le paramètre par défaut est 0.
Nombre maximal de nouvelles tentatives	Champ de texte	Définit le nombre maximal de nouvelles tentatives pour la connexion à un disque virtuel ou pour des opérations de lecture et d'écriture avant l'expiration. REMARQUE : le paramètre par défaut est 10.
Permettre la restauration parallèle	Booléen (case à cocher)	Lorsque cette option est cochée, la restauration parallèle est activée pour une machine virtuelle sans agent. Lorsque cette option n'est pas sélectionnée, cette fonction est désactivée. REMARQUE : le paramètre par défaut est Non autrement dit, la case n'est pas cochée.

- 4 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur la coche pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur **X** pour quitter le mode d'édition sans enregistrer.

Sauvegarde et restauration des paramètres du Core

Vous pouvez sauvegarder les informations de paramétrage du Core dans un fichier, puis restaurer ultérieurement ces paramètres si vous rencontrez des problèmes avec la machine Core ou si vous souhaitez faire migrer ces paramètres vers une autre machine. Les informations sauvegardées sont : les métadonnées de la logithèque (comme le nom de la logithèque, le chemin des données et le chemin des métadonnées), les machines protégées dans le Core, les relations de réplication (cibles et sources), quelles machines sont configurées pour la veille virtuelle, et les informations sur les clés de chiffrement.

Ce processus restaure les paramètres de configuration uniquement, et non les données en tant que telles. Les informations de sécurité (telles que les identifiants d'authentification) ne sont pas stockées dans le fichier de configuration. La sauvegarde d'un fichier de configuration du Core ne pose aucun risque pour la sécurité.

REMARQUE : vous devez d'abord sauvegarder les informations de paramétrage du Core avant de pouvoir utiliser ce processus pour restaurer les paramètres du Core.

Utilisez cette procédure pour sauvegarder et restaurer les paramètres du Core.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur .
L'écran **Paramètres** s'affiche. Dans la partie supérieure du volet Paramètres, au-dessus des catégories de paramètres, se trouvent deux boutons : Paramètres de sauvegarde et Paramètres de restauration.
- 3 Si vous souhaitez sauvegarder les paramètres du Core, passez à l'étape 4. Si vous souhaitez restaurer les paramètres du Core, passez à l'étape 6.
- 4 Pour sauvegarder les paramètres actifs dans un fichier XML, dans la partie supérieure de la page Paramètres, cliquez sur **Sauvegarder les paramètres**.

La boîte de dialogue Configuration de la sauvegarde du Core s'affiche.

- 5 Dans la zone de texte Chemin local, saisissez un chemin de répertoire accessible localement sur la machine Core sur laquelle vous souhaitez stocker les paramètres du Core en tant que fichier XML, puis cliquez sur **Sauvegarder**.

Par exemple, saisissez C:\Users\Your_User_Name\Documents\AA5CoreSettings et cliquez sur **Sauvegarder**.

Un fichier est enregistré sous le nom AppRecoveryCoreConfigurationBackup.xml à la destination spécifiée.

- 6 Pour restaurer les paramètres du Core à partir d'un fichier XML de sauvegarde préalablement enregistré avec cette méthode, suivez les étapes suivantes.

REMARQUE : lorsque vous restaurez les paramètres de configuration du Core, le service Core Rapid Recovery redémarre.

- a Dans la partie supérieure de la page **Paramètres**, cliquez sur **Restaurer**.

La boîte de dialogue **Configuration de la restauration du Core** s'affiche.

- b Dans la zone de texte **chemin local**, saisissez le chemin local de l'emplacement où vous avez enregistré les paramètres de configuration du Core.

Par exemple, saisissez C:\Users\Your_User_Name\Documents\AA5CoreSettings.

- c Si vous ne souhaitez pas restaurer les informations des logithèques, passez à l'étape g.

- d Éventuellement, si vous souhaitez restaurer les informations des logithèques telles que configurées dans le fichier de sauvegarde, sélectionnez **Restaurer les logithèques**, puis cliquez sur **Restaurer**.

La boîte de dialogue **Restaurer des logithèques** s'affiche.

Si vous choisissez de restaurer les informations des logithèques à partir des données de configuration sauvegardées, toutes les logithèques qui étaient configurées au moment de la sauvegarde des paramètres du Core s'affichent à des fins de vérification. Par défaut, toutes les logithèques existantes sont sélectionnées.

- e Vérifiez les informations sur les logithèques que vous souhaitez restaurer. Si plusieurs logithèques s'affichent dans les listes de vérification, et que vous souhaitez uniquement restaurer les informations de certaines d'entre elles, désélectionnez les logithèques dont vous ne voulez pas.

- f Lorsque la sélection des logithèques à restaurer vous convient, cliquez sur **Enregistrer**.

La boîte de dialogue **Restaurer des logithèques** se ferme.

- g Dans la boîte de dialogue **Restaurer des logithèques**, cliquez sur **Restaurer**.

La boîte de dialogue **Restaurer des logithèques** se ferme et le processus de restauration commence. Une alerte s'affiche, indiquant que la configuration du service des logithèques a été modifiée.

- h Si certains paramètres de configuration n'ont pas pu être restaurés, vous allez voir un message d'erreur s'afficher. Prenez connaissance des détails de ce message d'erreur pour voir si vous devez faire quelque chose. Pour plus d'informations, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#). Pour continuer, cliquez sur **Fermer** pour fermer la boîte de dialogue d'erreur.

- i Une fois la restauration de la configuration effectuée, vérifiez les points suivants :

- Déverrouillez toutes les clés de chiffrement. Pour plus d'informations, voir [Déverrouillage d'une clé de chiffrement](#).
- Si le disque de secours virtuel est configuré pour mettre à jour en continu une machine virtuelle sur une destination réseau, vous devez spécifier les informations d'identification du réseau dans les paramètres du disque de secours virtuel avant de pouvoir réussir une synchronisation. Pour plus d'informations, voir [VM export \(Exportation NFS\)](#).
- Si l'archive programmée est configurée vers un compte de stockage Cloud, vous devez indiquer les informations d'identification du compte en question pour que le Core puisse s'y connecter. Pour en savoir plus sur l'association du Core avec un compte de stockage Cloud, voir [Ajouter un compte cloud](#).
- Si la réplication est configurée et que vous souhaitez effectuer une restauration sur un Core cible, vérifiez les paramètres de ce dernier (en particulier l'hôte) sur le Core source. Pour en savoir plus, si vous gérez votre propre Core, voir [Réplication vers un core cible autogéré](#). Pour la réplication d'un Core géré par un tiers, voir [Réplication vers un Core cible tiers](#).
- Si la vérification de capacité d'attachement de SQL est configurée, et que l'instance SQL Server exécutant la vérification se trouve sur la machine Core, spécifiez les informations d'identification SQL dans les paramètres Capacité d'attachement. Pour plus d'informations, voir [Gestion des paramètres de capacité d'attachement SQL du Core](#).

Vérifiez que la configuration de Replay Engine a été restaurée, et mettez à jour les paramètres si ceux-ci n'ont pas permis d'assurer une communication efficace. Pour plus d'informations, voir [Configurer les paramètres du moteur Replay](#).

Outils au niveau du Core

Outre la configuration des paramètres du Core, vous pouvez également utiliser les outils au niveau du Core décrits dans le tableau suivant.

Tableau 23. Autres outils au niveau du Core

Élément de l'UI	Description
Informations système	Rapid Recovery permet d'afficher des informations concernant le Core de Rapid Recovery, notamment des informations sur le système, les volumes locaux et montés, et les connexions Replay Engine. Pour plus de détails sur les informations affichées sur la page Informations sur le système, voir Compréhension des informations sur le système du Core. Pour plus d'informations sur l'affichage des informations sur le système, voir Affichage des informations sur le système du Core.
Téléchargement des fichiers journaux du Core	Des informations sur les différentes activités du Core Rapid Recovery sont enregistrées dans le fichier journal du Core. Pour diagnostiquer les éventuels problèmes, vous pouvez télécharger et afficher les journaux du Core de Rapid Recovery. Pour plus d'informations sur l'accès aux journaux du Core et de leur affichage, voir Accès aux journaux du Core. Chaque machine protégée enregistre également un journal d'activité. Ce journal peut être chargé sur le Core si vous sélectionnez la tâche nocturne appelée Téléchargement des journaux à partir des machines protégées. Pour plus d'informations sur les tâches nocturnes, voir Comprendre les travaux nocturnes. Pour plus d'informations sur la configuration des paramètres des tâches nocturnes du Core, voir Configuration des tâches nocturnes du Core. Pour plus d'informations sur la configuration des tâches nocturnes pour des machines protégées particulières, voir Personnalisation des tâches nocturnes pour une machine protégée.

Compréhension des informations sur le système du Core

Rapid Recovery permet d'afficher des informations sur le Core Rapid Recovery. Vous pouvez afficher des informations générales, des informations sur les volumes locaux et des informations sur les volumes montés.

Dans le volet **Généralités**, vous pouvez afficher les informations présentées dans le tableau suivant.

Tableau 24. Informations système

Élément de l'UI	Description
Nom de l'hôte	Nom de la machine de votre Core Rapid Recovery.
Version du système d'exploitation	Version du système d'exploitation installé sur le Core Rapid Recovery.
Architecture du système d'exploitation	Répertorie la structure sous-jacente et la conception de la machine hébergeant votre Core Rapid Recovery. Comprend éventuellement le chipset et répertorie le système 64 bits. Le Core Rapid Recovery prend uniquement en charge les systèmes 64 bits.
Mémoire (Physique)	Répertorie la quantité de mémoire vive (RAM) installée sur la machine Core.
Nom d'affichage	Affiche le nom d'affichage du Core, lequel peut être modifié (voir Configuration des paramètres généraux du Core).
Nom de domaine complet	Affiche le nom de domaine pleinement qualifié de la machine Core.

Élément de l'UI	Description
Emplacement du cache des métadonnées	Affiche le chemin de l'emplacement du cache des métadonnées. Pour plus d'informations, voir Compréhension du cache de déduplication et des emplacements de stockage .
Emplacement du cache principal	Affiche le chemin de l'emplacement du cache de déduplication primaire. Pour plus d'informations, voir Compréhension du cache de déduplication et des emplacements de stockage .
Emplacement du cache secondaire	Affiche le chemin de l'emplacement du cache de déduplication secondaire. Pour plus d'informations, voir Compréhension du cache de déduplication et des emplacements de stockage .

Le volet **Volumes** contient les informations suivantes sur les volumes de stockage de la machine Core : nom, identifiant du périphérique, système de fichiers, capacité brute, capacité formatée, capacité utilisée et points de montage.

Le volet **Connexions du moteur Replay** affiche des informations détaillées sur les points de restauration actuellement montés. Vous pouvez afficher le point de terminaison local, le point de terminaison distant, l'identifiant de l'agent de l'image montée, l'identifiant de l'image montée et le nom d'affichage de l'image montée. Vous pouvez voir si le montage est inscriptible, voir l'utilisateur authentifié, le nombre d'octets lus et le nombre d'octets écrits.

Vous pouvez démonter des points de restauration montés localement sur un Core depuis la page Montages. Pour en savoir plus sur le démontage des points de restauration, voir [Démonter des points de restauration](#).

Pour plus d'informations, voir [Affichage des informations sur le système du Core](#).

Affichage des informations sur le système du Core

Les informations sur le système du Core incluent des informations générales, des informations sur les volumes locaux et des informations sur les volumes montés du Core. Pour obtenir une description détaillée des informations disponibles sur cette page, voir [Compréhension des informations sur le système du Core](#).

Suivez les étapes de cette procédure pour afficher les informations sur le système du Core.

REMARQUE : vous pouvez également consulter les informations sur le système d'une machine protégée. Pour plus d'informations, voir [Affichage des informations sur le système d'une machine protégée](#).

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sur  **Informations sur le système**.
La page Informations sur le système s'affiche.

Accès aux journaux du Core

Des informations sur les différentes activités du Core Rapid Recovery sont enregistrées dans le fichier journal du Core. Par défaut, ce fichier, appelé AppRecovery.log, est stocké à l'emplacement suivant : C:\ProgramData\AppRecovery\Logs.

REMARQUE : selon vos paramètres, le répertoire AppRecovery peut être masqué sur le Core Rapid Recovery. Pour l'afficher, il peut être nécessaire de changer le panneau de configuration Options de dossier pour afficher les fichiers, dossiers et lecteurs masqués. Si ces paramètres permettent de masquer les extensions des types de fichiers connus, le fichier journal du Core peut apparaître en tant qu'AppRecovery, sans l'extension .log.

Le journal du Core contient des informations sur les tâches du Core terminées, les échecs de connexion, les résultats des tentatives de contact du Portail des licences par le Core, ainsi que d'autres informations. Chaque instruction stockée dans le fichier journal du Core est précédée par l'un des quatre qualificatifs : INFO (Informations), DEBUG (Débogage), ERROR (Erreur) et WARN (Avertissement). Ces qualificatifs permettent de catégoriser la nature des informations stockées dans le journal pendant le diagnostic d'un problème.

REMARQUE : de même, un fichier journal est également stocké sur chaque machine protégée contenant des informations relatives à ses tentatives de communication avec le Core. Pour en savoir plus sur les journaux des machines, voir [Accéder aux diagnostics des machines protégées](#).

La capacité d'accéder aux journaux peut s'avérer utile lorsque vous recherchez les causes d'un problème ou que vous êtes en contact avec le Support Dell Rapid Recovery. Pour accéder aux journaux, voir les procédures suivantes :

- [Téléchargement et affichage du fichier journal du Core](#)
- [Téléchargement et affichage du fichier journal d'une machine protégée](#)

Téléchargement et affichage du fichier journal du Core

Si vous rencontrez des erreurs ou des problèmes avec le Core, vous pouvez télécharger les journaux de ce Core afin de les consulter ou de les transmettre à votre représentant du support technique de Dell.

- 1 Sur la barre d'icônes de la Rapid Recovery Core Console, cliquez sur  (Plus), puis cliquez sur  **Journal du Core**.
- 2 Sur la page **Télécharger le journal du Core**, cliquez sur  **Cliquer ici pour lancer le téléchargement**.
- 3 Si le système vous invite à ouvrir ou à enregistrer le fichier `CoreAppRecovery.log`, cliquez sur **Enregistrer**.
- 4 Si la boîte de dialogue **Ouverture de CoreAppRecovery.log** s'affiche, effectuez l'une des opérations suivantes :
 - Pour ouvrir le fichier journal, sélectionnez **Ouvrir avec**, choisissez une application (par exemple, Bloc-notes) permettant d'afficher le fichier journal texte, puis cliquez sur **OK**.
Le fichier `CoreAppRecovery.log` s'ouvre dans l'application sélectionnée.
 - Pour enregistrer le fichier localement, sélectionnez **Enregistrer le fichier**, puis cliquez sur **OK**.
Le fichier `CoreAppRecovery.log` est enregistré dans votre dossier **Téléchargements**. Il est possible de l'ouvrir à l'aide d'un éditeur de texte.

Liens connexes

[Téléchargement et affichage du fichier journal du Core](#)

[Téléchargement et affichage du fichier journal d'une machine protégée](#)

Schéma de configuration du core

La configuration inclut des tâches comme la création et la configuration du référentiel pour stocker les instantanés de sauvegarde, la définition de clés de chiffrement pour sécuriser les données protégées, et la configuration d'alertes et de notifications. Après avoir terminé la configuration du core, vous pouvez protéger les agents et effectuer la restauration.

Pour configurer le core, vous devez comprendre certains concepts et effectuer les opérations initiales suivantes :

- Créer un référentiel
- Configurer des clés de chiffrement
- Configurer une notification d'événement
- Configurer une stratégie de conservation
- Configurer la capacité d'attachement SQL

Logithèques

Cette section indique comment utiliser les logithèques. Elle présente la logithèque du gestionnaire de volumes de déduplication ainsi que ses fonctions et attributs. Elle décrit également les types de déduplication utilisés dans Rapid Recovery, ainsi que le type d'utilisation de la déduplication dans l'application. Cette section explique ensuite comment gérer des logithèques DVM, en indiquant notamment comment les créer, les afficher, modifier leurs détails et les supprimer. Vous pouvez apprendre à ouvrir une logithèque d'un Core à un autre. Enfin, cette section décrit comment effectuer une migration manuelle des points de restauration d'une logithèque à une autre.

Gestion d'une logithèque DVM

Avant d'utiliser Rapid Recovery, vous devez configurer une ou plusieurs logithèques sur le Core Rapid Recovery. La logithèque stocke les données protégées, plus particulièrement les instantanés capturés depuis les machines protégées dans votre environnement.

La gestion d'une logithèque DVM inclut les opérations suivantes :

- 1 **Création d'une logithèque DVM.** Avant de créer une logithèque, choisissez le type de technologie adéquat.
Pour en savoir plus sur les logithèques, voir [Comprendre les référentiels](#).

Pour en savoir plus sur la création d'une logithèque DVM, voir [Créer un référentiel DVM](#).
- 2 **Ajout d'un nouvel emplacement de stockage.** Pour en savoir plus sur l'ajout d'un nouvel emplacement de stockage à une logithèque DVM, voir [Ajout d'un emplacement de stockage à une logithèque DVM existante](#).
- 3 **Modification des paramètres de la logithèque.** Pour en savoir plus sur la modification des paramètres de la logithèque, voir [Afficher ou modifier les détails d'un référentiel](#).
- 4 **Vérification d'une logithèque.** Pour en savoir plus sur la vérification d'une logithèque DVM, voir [Vérifier une logithèque](#).
- 5 **Exécution d'une tâche d'optimisation de logithèque.** Pour en savoir plus sur la tâche d'optimisation de logithèque, voir [À propos de la tâche d'optimisation de logithèque](#). Pour savoir comment optimiser une logithèque DVM existante, voir [L'optimisation d'une logithèque DVM](#).
- 6 **Suppression d'une logithèque.** Pour en savoir plus sur la suppression d'une logithèque, voir [Supprimer une logithèque](#).

Créer un référentiel DVM

Cette procédure explique comment créer un référentiel sur votre core à l'aide de la technologie DVM (Deduplication Volume Manager ou Gestionnaire de volumes de déduplication).

- Vous devez avoir l'accès administratif à la machine sur laquelle vous souhaitez créer un référentiel DVM.
- Ce type de référentiel nécessite un minimum de 150 Go d'espace de stockage disponible sur le volume que vous définissez comme l'emplacement de stockage.
- L'emplacement de stockage d'un référentiel DVM doit se trouver sur un lecteur local relié au serveur core.
- Le serveur core peut être n'importe quelle appliance DL (y compris le DL1000) ou n'importe quel serveur Windows répondant aux conditions requises.

REMARQUE : Il est recommandé de passer par l'onglet **Appliance** pour créer le référentiel. Pour plus d'informations, consultez la section [Provisionnement du stockage](#).

Procédez comme suit pour créer un référentiel DVM.

- 1 Naviguez jusqu'à la console Core Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Référentiels**.
La page **Référentiels** s'affiche.

Dans la page **Référentiels**, le volet Référentiels DVM s'affiche.
- 3 En haut de la page, cliquez sur **Ajouter un nouveau référentiel DVM**.
La boîte de dialogue **Ajouter un nouveau référentiel** s'affiche.
- 4 Entrez les informations de configuration telles que décrites dans le tableau suivant.

Tableau 25. Ajouter les paramètres du nouveau référentiel

Zone de texte	Description
Nom de référentiel	Entrez le nom d'affichage du référentiel. Par défaut, cette zone de texte contient le mot Repository et un numéro, qui correspond au nombre de référentiels de ce core. Par exemple, s'il s'agit du premier référentiel, son nom par défaut est Repository 1. Modifiez le nom si nécessaire. Les noms de référentiels doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas caractères interdits ni expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que votre référentiel devra prendre en charge. La valeur par défaut est 64.
Commentaires	(Optionnel) Entrez une note décrivant ce référentiel. Vous pouvez entrer jusqu'à 254 caractères. Par exemple, tapez Référentiel DVM 2 .

- 5 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.

⚠ PRÉCAUTION : Définissez un dossier dédié au sein de la racine de l'emplacement de stockage de votre référentiel. Ne spécifiez pas l'emplacement racine. Par exemple, utilisez E:\Repository\ et non E:\. Si le référentiel que vous créez à cette étape est supprimé ultérieurement, tous les fichiers de son emplacement de stockage seront supprimés. Si vous définissez votre emplacement de stockage à la racine, tous les autres fichiers dans le volume (par ex., E:\) seront également supprimés, ce qui pourrait entraîner une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.

- 6 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.
- 7 Dans la zone **Emplacement de stockage**, spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage connecté localement (par exemple en tant que stockage à connexion directe, un réseau de zone de stockage, ou un stockage connecté par réseau). Vous pouvez également spécifier un volume de stockage sur un emplacement partagé CIFS (Common Internet File System).
- Sélectionnez **Ajouter un fichier sur disque local** pour spécifier une machine locale, puis entrez les informations décrites dans le tableau suivant.

Tableau 26. Paramètres du disque local

Zone de texte	Description
Chemin de données	Entrez l'emplacement de stockage des données protégées. Par exemple, entrez X:\Repository\Data. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées. Par exemple, entrez X:\Repository\Metadata. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

- Vous pouvez également cliquer sur **Ajouter le fichier sur un partage CIFS** pour spécifier un emplacement de partage réseau, puis entrez les informations décrites dans le tableau suivant.

Tableau 27. Identifiants pour le partage CIFS

Zone de texte	Description
Chemin UNC	Entrez le chemin de l'emplacement du partage réseau. Si cet emplacement se trouve à la racine, définissez un nom de dossier dédié (par exemple, Repository). L'extension de fichier doit commencer par \\. Lorsque vous spécifiez ce chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Les lettres a à z peuvent être en majuscules ou en minuscules. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe pour accéder à l'emplacement du partage réseau.

- 8 Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails** et entrez les détails de l'emplacement de stockage décrits dans le tableau suivant.

Tableau 28. Détails de la configuration du stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille minimale est de 1 Go. La valeur par défaut est de 250 Go. Vous pouvez choisir parmi les options suivantes : - Go - To REMARQUE : La taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) sous Windows XP ou Windows 7, la taille de fichier est limitée à 16 To. Si l'emplacement de stockage est un volume NTFS sous Windows 8, 8.1, Windows 10, ou Windows Server 2012, 2012 R2, la taille de fichier est limitée à 256 To. REMARQUE : Pour que Rapid Recovery puisse valider le système d'exploitation, WMI (Windows Management Instrumentation) doit être installé sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle l'utilisation du Windows Cache Manager dans le référentiel et facilite le réglage du référentiel pour des performances optimales sur différentes configurations. Définissez l'option sur une des valeurs suivantes : - Activé - Éteint - Synchroniser Si la fonction est définie comme activée (valeur par défaut), Windows contrôle la mise en cache. Cette option est appropriée pour Windows 10, et pour les versions de Windows Server 2012 et ultérieur. REMARQUE : L'activation de la stratégie de mise en cache d'écriture peut améliorer la vitesse des performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, il est recommandé de désactiver cette stratégie. Si la fonction est désactivée, c'est Rapid Recovery qui contrôle la mise en cache. Si la fonction est définie sur Synchroniser, Windows contrôle la mise en cache et les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets que devrait comprendre chaque secteur. La valeur par défaut est 512.

Zone de texte	Description
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

9 Cliquez sur **Enregistrer**.
La boîte de dialogue **Ajouter un emplacement de stockage** se ferme et vos paramètres sont enregistrés. La boîte de dialogue **Ajouter un nouveau référentiel** affiche votre nouvel emplacement de stockage.

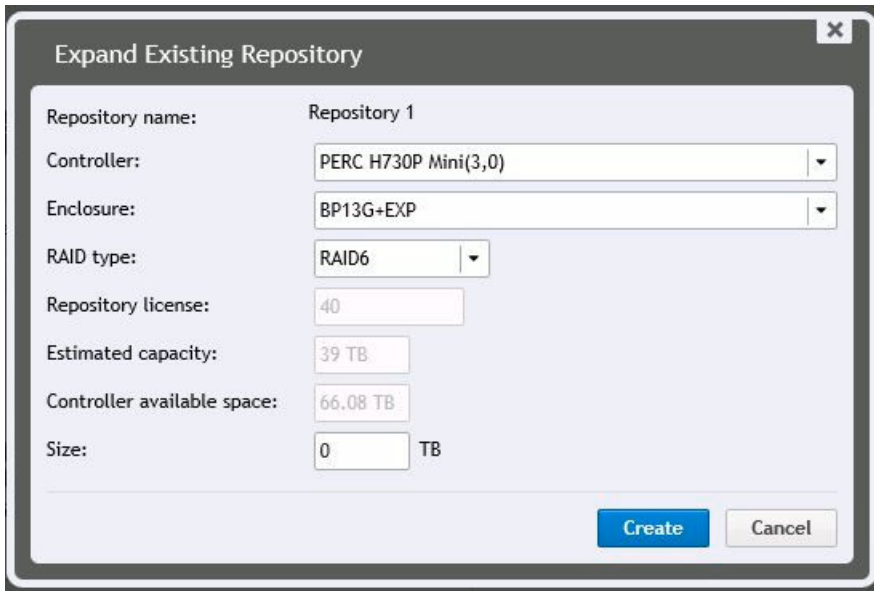
10 Le cas échéant, répétez la procédure de 6 à 9 afin d'ajouter d'autres emplacements de stockage pour le référentiel.

11 Lorsque vous aurez fini de créer tous les emplacements de stockage pour le référentiel, dans la boîte de dialogue **Ajouter un nouveau référentiel**, cliquez sur **Créer**.
La boîte de dialogue **Ajouter un nouveau référentiel** se ferme et vos modifications s'appliquent. La page **Référentiels** apparaît, indiquant votre nouveau référentiel dans le tableau récapitulatif des référentiels DVM.

Étendre le référentiel

La fonction d'expansion du référentiel est disponible sur tous les modèles DL (1300, 4300, 4000), à l'exception du DL1000. Le type de licence appliquée limite la taille du référentiel. Pour développer le référentiel à l'aide du stockage interne non utilisé et de stockage présent sur un boîtier externe, mettez à jour la licence. Pour modifier la clé de licence, voir la section [Mise à jour ou modification d'une licence](#). Pour développer le référentiel existant :

- 1 Cliquez sur **Provisionnement > de l'appliance**.
- 2 Dans la section **Référentiels**, cliquez sur  → **Étendre référentiel existant**, en regard du référentiel que vous souhaitez développer.
La boîte de dialogue **Étendre référentiel existant** s'affiche.



- 3 Dans la zone **Étendre référentiel existant**, spécifiez les informations suivantes :

Tableau 29. Extension de référentiel existant

Zone de texte	Description
Nom de référentiel	Le nom du référentiel qui doit être étendu s'affiche.
Contrôleur	Sélectionnez le contrôleur de stockage approprié selon que vous créez le référentiel sur un stockage interne ou sur un boîtier de stockage à connexion directe.
Enceinte	Sélectionnez le boîtier de stockage approprié.
Type RAID	Sélectionnez la configuration RAID appropriée. Vous avez le choix parmi les options suivantes : 1, 5 ou 6.
Licence du référentiel	La licence du référentiel s'affiche.
Capacité estimée	Affiche la capacité estimée disponible pour la création d'un référentiel.
Espace disponible sur le contrôleur	Affiche l'espace disque disponible sur le contrôleur.
Taille	Entrez la taille du référentiel à créer.

- 4 Cliquez sur **Créer**.
L'emplacement du nouveau référentiel vient s'ajouter au référentiel existant.

Le référentiel est étendu à la taille spécifiée.

Afficher ou modifier les détails d'un référentiel

- 1 Naviguez jusqu'à la console Core Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Référentiels**.
La page **Référentiels** s'affiche.

Le volet **Référentiels DVM** s'affiche.

- 3 Dans le menu de la page **Référentiels**, vous pouvez effectuer les actions générales suivantes :

Option	Description
Ajouter un nouveau référentiel DVM	Permet d'ajouter un nouveau référentiel DVM.
Ouvrir un référentiel DVM existant	Permet d'ouvrir un référentiel DVM existant depuis un autre core, ce qui fait que le référentiel de ce core change de propriétaire. Pour en savoir plus, voir Ouverture d'une logithèque DVM existante .
Actualiser	Permet d'afficher ou d'actualiser la liste des référentiels.

- 4 Dans le volet **Référentiels DVM**, à partir du menu déroulant  de n'importe quel référentiel DVM, vous pouvez effectuer les actions supplémentaires suivantes :

Option	Description
Ajouter un emplacement de stockage	Permet d'étendre le référentiel existant en ajoutant un emplacement de stockage
	 REMARQUE : Lorsque vous étendez un volume de référentiel DVM, commencez par suspendre la protection. Puis étendez le volume, et enfin reprenez la protection. Cette action empêche la création d'une erreur rare qui peut se produire uniquement lorsque l'extension d'un volume s'effectue en même temps qu'une phase de transfert spécifique.
Vérifier	Permet d'effectuer une vérification du référentiel
Paramètres	Permet d'afficher ou modifier les paramètres d'un référentiel. Ces paramètres sont les suivants : • Afficher le nom du référentiel • Afficher ou modifier le nombre maximal d'opérations simultanées

Option	Description
	- Afficher ou modifier une description du référentiel - Activer ou désactiver la déduplication - Activer ou désactiver la compression des données stockées dans le référentiel
Effectuer un travail d'optimisation	Permet d'effectuer une optimisation du référentiel
Supprimer	Supprimer un référentiel

REMARQUE : Lorsque vous étendez un volume de référentiel DVM, commencez par suspendre la protection. Puis étendez le volume, et enfin reprenez la protection. Cette action empêche la création d'une erreur rare qui peut se produire lorsque l'extension d'un volume s'effectue en même temps qu'une phase de transfert spécifique.

Vous pouvez effectuer les actions générales suivantes depuis la page Référentiels :

- Afficher ou actualiser la liste des référentiels
- Ajouter un nouveau référentiel
- Ouvrir un référentiel existant à partir d'un autre core (ce qui entraîne un changement de propriétaire pour ce référentiel)

Ajout d'un emplacement de stockage à une logithèque DVM existante

REMARQUE : Il est recommandé de développer la logithèque via l'onglet **Appliance**. Pour plus d'informations, voir [Étendre le référentiel](#)

L'ajout d'un emplacement de stockage à une logithèque DVM permet de définir l'endroit où la logithèque ou le volume seront stockés.

Effectuez la procédure suivante pour spécifier l'emplacement de stockage de la logithèque ou du volume.

- Accédez à la Rapid Recovery Core Console.
- Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page Référentiels s'affiche.

Le volet Logithèques DVM s'affiche.
- Dans le tableau récapitulatif des logithèques, à partir de la ligne représentant la logithèque DVM pour lequel vous souhaitez ajouter un emplacement de stockage, cliquez sur **Paramètres** et sélectionnez **Ajouter un emplacement de stockage**.
La boîte de dialogue **Ajouter un emplacement de stockage** s'affiche.
- Indique comment ajouter le fichier pour l'emplacement de stockage. Vous pouvez choisir d'ajouter le fichier sur le disque local ou sur un partage CIFS.
 - Cliquez sur **Ajouter le fichier sur le disque local** pour indiquer une machine locale, puis entrez les informations, tel que décrit dans le tableau suivant.

Tableau 30. Paramètres du disque local

Zone de texte	Description
Chemin des données	Indiquez l'emplacement de stockage des données protégées. Par exemple, saisissez X:\Repository\Data. Les mêmes limitations du chemin s'appliquent ; n'utilisez que des caractères alphanumériques, des tirets ou des points, sans espaces et sans caractères spéciaux.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées. Par exemple, saisissez X:\Repository\Metadata.

Zone de texte	Description
	Lorsque vous spécifiez le chemin, n'utilisez que des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôte et les domaines). Les lettres a à z sont sensibles à la casse. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.

- Ou bien cliquez sur **Ajouter le fichier sur le partage CIFS** pour indiquer un emplacement de partage réseau, puis entrez les informations tel que décrit dans le tableau suivant.

Tableau 31. Identifiants du partage CIFS

Zone de texte	Description
Chemin UNC	Entrez le chemin du partage réseau. Si cet emplacement est à la racine, définissez un nom de dossier dédié (par exemple, Repository). Le chemin doit commencer par \\. Lorsque vous spécifiez le chemin, n'utilisez que des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôte et les domaines). Les lettres a à z sont sensibles à la casse. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe permettant d'accéder à l'emplacement du partage réseau.

- 5 Dans le volet Configuration du stockage, cliquez sur **Plus de détails**, puis entrez les détails de l'emplacement de stockage, tel que décrit dans le tableau suivant.

Tableau 32. Détails des emplacements de stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille par défaut est 250 Mo. Vous pouvez choisir parmi les options suivantes : • Go • To REMARQUE : La taille minimale est de 1 To. La taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) qui utilise Windows XP ou Windows 7, la limite de taille du fichier est de 16 To. Si l'emplacement de stockage est un volume NTFS qui utilise Windows 8, 8.1 ou Windows Server 2012, 2012 R2, la limite de taille du fichier est 256 To. REMARQUE : Pour que Rapid Recovery valide le système d'exploitation, vous devez installer Windows Management Instrumentation (WMI) à l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle la façon dont le gestionnaire de cache Windows est utilisé dans la logithèque. Elle vous aide également à paramétrer la logithèque pour optimiser les performances dans différentes configurations. Affectez à ce paramètre l'une des valeurs suivantes : • Activé • Désactivé • Synchroniser Si la valeur est Activé, la valeur par défaut, Windows contrôle la mise en cache. Cette option est pour Windows 10 et pour Windows Server 2012 et versions ultérieures. REMARQUE : Si vous définissez la valeur Activé vous pouvez éventuellement améliorer les performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, la valeur recommandée est Désactivé.

Zone de texte	Description
	Si la valeur est définie sur Désactivé, Rapid Recovery contrôle la mise en cache.
	Si la valeur est Synchroniser, Windows contrôle la mise en cache, ainsi que les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets de chaque secteur. La valeur par défaut est 512.
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

- 6 Si vous souhaitez effectuer une tâche d'optimisation de logithèque pour la logithèque sélectionnée, sélectionnez **Exécuter la tâche d'optimisation pour [nom de la logithèque]**.

Dell recommande d'effectuer la tâche d'optimisation de logithèque lors de l'ajout d'emplacement de stockage à une logithèque existante. Cette tâche optimise l'espace libre en appliquant la déduplication aux données stockées dans la logithèque.

En fonction de facteurs tels que la taille de votre logithèque, la quantité de données dans votre logithèque, la bande passante réseau disponible et la charge existante en entrée et sortie de votre système, l'exécution d'une tâche d'optimisation de logithèque pourrait prendre beaucoup de temps et de bande passante dans votre environnement.

Pour en savoir plus sur la tâche d'optimisation de logithèque, voir [À propos de la tâche d'optimisation de logithèque](#).

- 7 Cliquez sur **Enregistrer**.

La boîte de dialogue se ferme et l'emplacement de stockage est enregistré. Dans le tableau récapitulatif des logithèques, l'emplacement de stockage que vous avez créé est visible uniquement si vous développez les détails de la logithèque.

À propos de la vérification de l'intégrité des référentiels DVM

Rapid Recovery Core, les utilisateurs peuvent définir des stratégies de conservation disparates entre la source et les cores cible. Pour que la réplication fonctionne correctement avec des stratégies de conservation différentes, le core cible doit avoir la même version du logiciel (ou une version plus récente) que le core source.

REMARQUE : Les cores doivent partager les trois mêmes chiffres du numéro de version (par exemple, les deux commencent par 6.0.1.xxxx ou 5.4.3.xxxx). Le numéro de build (représenté par xxxx) ne peut être différent que si le core cible est plus récent.

Les administrateurs peuvent désormais configurer un rollup (cumul) sur un core cible à un débit différent que sur le core source. De même, vous pouvez désormais définir une stratégie personnalisée de conservation pour n'importe quelle machine répliquée. Par exemple, vous pouvez cumuler les points de restauration sur le core cible à un rythme plus rapide et avec moins de granularité sur le core source, ce qui vous fait gagner de la place. Ou, au contraire, vous pouvez cumuler les points de récupération de la machine répliquée sélectionnée à un rythme plus lent sur le core cible, en maintenant une plus grande granularité, ce qui peut être utile à des fins de respect de la conformité. Pour plus d'informations sur l'utilisation d'une stratégie de conservation qui diffère de la stratégie en vigueur par défaut sur le core, voir [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).

Si, à un moment ou à un autre, votre core a été mis à niveau depuis AppAssure 5.3.x et que vous avez utilisé la réplication, vous devrez exécuter ce travail avant de pouvoir configurer des stratégies de conservation différentes entre le core source et un core cible, ou de configurer une stratégie personnalisée de conservation sur une machine répliquée.

Vous ne verrez ce travail ou vous ne pourrez l'exécuter que si vous disposez d'un ou plusieurs référentiels éligibles (créés avant la version 5.4.x et qui n'ont pas encore fonctionné).

L'exécution de ce travail vérifie l'intégrité de tous les données stockées dans le référentiel spécifié, vous garantissant de pouvoir récupérer les données à partir de chaque instantané ou de chaque image de base. Si le contrôle d'intégrité découvre un problème avec les données contenues dans votre référentiel, le travail cesse immédiatement. Les détails d'événement de ce travail sur le core vous invite à prendre rendez-vous avec le support Dell exécuter des procédures supplémentaires permettant d'identifier et réparer les incohérences dans les données.

⚠ PRÉCAUTION : L'exécution de ce travail est censée prendre un certain temps. La durée diffère en fonction de la quantité et du type de données présentes dans votre référentiel et en fonction également du système de stockage utilisé. Pendant que le travail est en cours d'exécution, aucune autre transaction ne peut être effectuée dans ce référentiel : transferts (sauvegardes d'instantanés et d'images de base et réplication), travaux nocturnes, etc.

Vous pouvez procéder à d'autres opérations dans d'autres référentiels pendant que ce travail est en cours d'exécution.

❗ REMARQUE : Ce travail vérifie l'intégrité de tous les contenus au sein d'un référentiel. Pour plus d'informations sur la Integrity Check, que vous pouvez utiliser pour vous assurer qu'un référentiel peut être monté et utilisable, voir [Vérifier une logithèque](#).

Vérifier une logithèque

Rapid Recovery permet d'effectuer une vérification de diagnostic d'une logithèque DVM lorsque des erreurs se produisent. Des codes d'erreur peuvent résulter d'un arrêt effectué incorrectement, d'une défaillance matérielle ou d'autres facteurs affectant l'environnement des couches basses IP et susceptibles d'être exposés dans la fonctionnalité Rapid Recovery.

❗ REMARQUE : Cette procédure doit être strictement réservée au diagnostic. Par exemple, exécutez cette vérification en cas de défaillance matérielle, de fermeture incorrecte du Core ou d'erreur lors de l'importation d'une logithèque.

- 1 Accédez à la console Core Rapid Recovery.
- 2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page **Référentiels** s'affiche.

Le volet Logithèques DVM s'affiche.
- 3 Pour vérifier une logithèque DVM, dans le volet des **Logithèques DVM**, dans n'importe quelle rangée du tableau Synthèse représentant une logithèque DVM, cliquez sur , puis sélectionnez **Vérifier**.
La boîte de dialogue **Vérifier le référentiel** s'affiche.
- 4 Dans la boîte de dialogue **Vérifier la logithèque**, confirmez que vous comprenez que toutes les tâches actives associées à cette logithèque seront annulées et que vous voulez continuer.
Les tâches actives sont annulées et la tâche de vérification de logithèque commence.
- 5 Si vous le désirez, vous pouvez suivre la progression de la tâche en cliquant sur le menu déroulant **Tâches en cours d'exécution** dans la barre de boutons et en sélectionnant Tâche de maintenance de logithèque.

À propos de la tâche d'optimisation de logithèque

Lorsque vous utilisez une logithèque DVM, les données enregistrées dans chaque instantané sont dédupliquées. Cette déduplication se fait de manière incrémentielle, à mesure que des instantanés sont enregistrés dans la logithèque. Une occurrence de chaque chaîne d'informations est enregistrée dans la logithèque. Lorsqu'une chaîne d'informations est dupliquée, une référence à la chaîne d'origine se trouvant dans le cache de déduplication est utilisée, ce qui permet d'économiser l'espace de stockage de la logithèque.

Lorsque le cache de déduplication DVM est plein, seules les données d'instantané déjà référencées dans le cache sont dédupliquées. Pendant la déduplication, le cache continue sa mise à jour avec de nouvelles valeurs uniques, qui viennent écraser les valeurs les plus anciennes du cache. La déduplication qui en résulte n'est pas optimale.

Pour en savoir plus sur la déduplication, voir [Compréhension du cache de déduplication et des emplacements de stockage](#).

Vous pouvez choisir d'augmenter la taille de votre cache de déduplication DVM avant qu'il ne soit plein, garantissant ainsi une déduplication systématiquement optimale de vos données dans cette logithèque. Pour plus d'informations, voir [Configuration des paramètres du cache de déduplication DVM](#).

Vous pouvez également augmenter la taille de votre cache de déduplication une fois celui-ci plein. Si vous souhaitez récupérer l'espace de la logithèque après avoir augmenté la taille de votre cache, vous pouvez optimiser la logithèque. Cette action force une comparaison entre

les données de vos instantanés et les informations du cache de déduplication. Si des chaînes répétées se trouvent dans la logithèque, ces données sont remplacées par des références à celle-ci, ce qui permet d'économiser l'espace de stockage de la logithèque. Cette opération est parfois désignée en tant que « déduplication hors ligne », étant donné que le processus de déduplication est initié à votre demande, et non de manière incrémentielle à mesure que les données d'instantané sont transférées.

Le processus d'optimisation utilise une grande quantité de ressources du processeur. La durée d'exécution de cette tâche dépend de plusieurs facteurs. Ces facteurs incluent la taille de votre logithèque, la quantité de données que celle-ci contient, la bande passante réseau disponible et la charge en entrée et en sortie de votre système. La durée d'exécution de cette tâche est proportionnelle à la quantité de données que contient votre logithèque.

Les actions suivantes sont remplacées ou annulées pendant l'exécution de la tâche d'optimisation de logithèque.

- Tâche de suppression de points de restauration
- Tâche de maintenance de logithèque
- Tâche de vérification de l'intégrité de la logithèque

Les actions suivantes sont remplacées ou annulées pendant l'exécution de la tâche d'optimisation.

- Tâche de suppression de tous les points de restauration
- Tâche de suppression de chaînes de points de restauration
- Tâche de maintenance de logithèque
- Base de tâche de suppression de points de restauration
- Tâche de vérification de l'intégrité de la logithèque

Pour connaître les étapes d'optimisation d'une logithèque DVM existante, voir [L'optimisation d'une logithèque DVM](#).

Vous pouvez interrompre la tâche d'optimisation de logithèque pendant une durée limitée, si nécessaire. Pour plus d'informations, voir [Interruption ou reprise de l'optimisation de la logithèque](#).

L'optimisation d'une logithèque DVM

Votre Core doit disposer d'une logithèque DVM pour effectuer cette procédure.

Vous pouvez effectuer la déduplication hors ligne de données enregistrées dans une logithèque DVM existant. Ceci peut être effectué en lançant la tâche d'optimisation de logithèque.

REMARQUE : Dell recommande d'effectuer la tâche d'optimisation de logithèque uniquement après avoir augmenté la taille de votre cache de déduplication. Cette action vous permet de vous récupérer de l'espace de logithèque et d'utiliser plus efficacement le cache de déduplication DVM.

Effectuez cette procédure pour optimiser une logithèque DVM.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page **Référentiels** s'affiche.
- 3 Dans le volet Logithèques DVM, à partir de la ligne représentant la logithèque que vous souhaitez optimiser, cliquez sur  puis sélectionnez **Exécuter la tâche d'optimisation**.
Un message d'avertissement s'affiche et vous invite à confirmer l'optimisation.
- 4 Cliquez pour confirmer l'optimisation.
La tâche d'optimisation est prioritaire sur la plupart des autres travaux. Si nécessaire, vous pouvez interrompre une tâche d'optimisation en cours. Pour plus d'informations sur l'interruption ou la reprise de cette tâche, voir [Interruption ou reprise de l'optimisation de la logithèque](#).

Interruption ou reprise de l'optimisation de la logithèque

Lorsque vous exécutez l'optimisation de la logithèque, la logithèque DVM sélectionnée est dupliquée. L'optimisation de déduplication est une tâche qui monopolise le processeur afin de gagner de l'espace dans la logithèque. Pour plus d'informations, voir [À propos de la tâche d'optimisation de logithèque](#).

Une fois cette opération lancée, vous pouvez l'interrompre à l'aide de la procédure suivante. Cela interrompt la déduplication. Si vous avez déjà interrompu une optimisation, vous pouvez la reprendre à l'aide de cette procédure.

REMARQUE : Cette procédure s'applique uniquement aux logithèques DVM et seulement lorsque l'optimisation de logithèque est lancée.

Effectuez les étapes de cette procédure pour interrompre ou reprendre une optimisation de logithèque.

1 Naviguez jusqu'à la console Core Rapid Recovery.

2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page **Référentiels** s'affiche.

Le volet Logithèques DVM s'affiche.

3 Si vous souhaitez interrompre une optimisation, procédez comme suit :

- Dans le tableau récapitulatif des logithèques, depuis la ligne représentant la logithèque appropriée, cliquez sur , puis sélectionnez **Interrompre l'optimisation**.
Un message d'avertissement apparaît et vous demande de confirmer l'interruption.
- Cliquez pour confirmer l'optimisation.

4 Si vous souhaitez reprendre une optimisation, procédez comme suit :

- Dans le tableau récapitulatif des logithèques, depuis la ligne représentant la logithèque appropriée, cliquez sur , puis sélectionnez **Continuer l'optimisation**.
Un message d'avertissement apparaît et vous demande de confirmer l'interruption.
- Dans la boîte de dialogue, sélectionnez l'option **Continuer l'optimisation à partir du point interrompu** et cliquez sur **Oui**.

La boîte de dialogue se ferme et l'optimisation de la logithèque reprend à partir du point où elle avait été interrompue la dernière fois.

Ouverture d'une logithèque DVM existante

En tant que logithèque principale pour Rapid Recovery, la logithèque DVM contient les données d'instantané (sous forme de points de restauration) provenant des machines protégées sur un Rapid Recovery Core spécifique. Vous pouvez ouvrir une logithèque existante à partir d'un Core (par exemple, Core A) sur un second Core (Core B).

REMARQUE : L'ouverture d'une logithèque depuis un autre Core change la propriété de la logithèque. Lorsque vous ouvrez une logithèque existante, les informations sont alors accessibles uniquement pour le deuxième Core.

Dans le cas d'une logithèque DVM, le Core d'origine (Core A) ne doit pas être en cours d'utilisation. Par exemple, la machine doit être mise hors tension et non accessible pour le réseau ou les services Core doivent être arrêtés.

La logithèque peut se trouver sur un emplacement réseau partagé ou sur un périphérique de stockage accessible pour le deuxième Core.

Suivez la procédure suivante pour ouvrir une logithèque existante.

1 Accédez à la Rapid Recovery Core Console.

2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page **Référentiels** s'affiche.

Le volet Logithèques DVM s'affiche également.

- 3 Pour ouvrir une logithèque DVM existante, cliquez sur **Ouvrir une logithèque existante** en haut de la page.
La boîte de dialogue **Ouvrir une logithèque DVM existante** s'affiche.
- 4 Dans la boîte de dialogue **Ouvrir une logithèque DVM existante**, entrez les informations suivantes pour la logithèque que vous souhaitez ouvrir, puis cliquez sur **Ouvrir**.

Tableau 33. Ouvrir une logithèque DVM existante

Zone de texte	Description
Chemin	Le chemin d'accès à la logithèque (par exemple, D:\work\machine pour un chemin local ou \10.10.99.155\repositories par adresse IP ou \\servername\sharename pour un chemin réseau).
Nom d'utilisateur	Si la logithèque a un chemin d'accès réseau, entrez le nom d'utilisateur utilisé pour la connexion au partage réseau.
Mot de passe	Si la logithèque a un chemin d'accès réseau, entrez le mot de passe utilisé pour la connexion au partage réseau.

La boîte de dialogue se ferme et la logithèque sélectionnée est ajoutée à votre Core actuel.

Supprimer une logithèque

Effectuez cette procédure pour supprimer une logithèque.

- 1 Accédez à la console Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  Plus, puis sélectionnez **Logithèques**.
La page **Référentiels** s'affiche.

Sur la page **Logithèques**, le volet Logithèques DVM s'affiche.
- 3 Dans le tableau récapitulatif des logithèques, sur la ligne représentant la logithèque que vous souhaitez supprimer, cliquez sur  pour développer le menu déroulant, puis sélectionnez **Supprimer**.
Un message d'avertissement s'affiche pour demander de confirmer la suppression.
- 4 Cliquez sur **Oui** pour confirmer la suppression de la logithèque.

 **PRÉCAUTION :** Lorsqu'une logithèque est supprimée, les données contenues dans la logithèque sont supprimées définitivement et ne peuvent pas être récupérées.

Exécution de la tâche de vérification de logithèque sur une logithèque DVM

Suivez cette procédure pour vérifier l'intégrité d'une logithèque DVM dans sa totalité. Cette méthode est recommandée pour les Cores cibles répliqués lors du passage de la version 5.3.x à la version 5.4 du logiciel AppAssure. Lors de l'exécution de la vérification de l'intégrité, qui peut être un processus assez long, aucune autre opération ne peut être effectuée sur la logithèque.

Si le Core cible dispose de plusieurs logithèques DVM, effectuez ce processus sur chacune des logithèques.

 **REMARQUE :** Si le Core cible dispose d'une autre logithèque DVM dont l'intégrité a déjà été vérifiée, ou si vous créez une nouvelle logithèque pour ce Core cible, vous pouvez effectuer des opérations dans cette logithèque secondaire pendant que la tâche de vérification de l'intégrité s'exécute sur la logithèque DVM indiquée.

- 1 Naviguez jusqu'à la console Core Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Logithèques**.
La page **Logithèques** s'affiche.

Le volet Logithèques DVM s'affiche.

- 3 Dans le tableau récapitulatif des logithèques, sur la ligne représentant la logithèque à vérifier, cliquez sur  , puis sélectionnez **Tâche de vérification de logithèque** dans le menu déroulant.

Un message de confirmation apparaît.

PRÉCAUTION : avant de confirmer que vous souhaitez bien effectuer la tâche, réfléchissez attentivement à la durée requise. Pendant que la tâche s'exécute, aucune autre transaction ne peut être effectuée sur cette logithèque, qu'il s'agisse de transferts (sauvegardes de l'image de base et d'instantanés, réplication), de tâches nocturnes ou de toute autre chose.

- 4 Dans la boîte de dialogue **Tâche de vérification de logithèque**, cliquez sur **Oui** pour effectuer la vérification de l'intégrité. La boîte de dialogue se ferme. Toutes les tâches en attente ou en cours d'exécution sont annulées et la tâche de vérification de l'intégrité commence.

- 5 Pour suivre l'avancement de la tâche de vérification d'une logithèque, notamment pour déterminer si des étapes supplémentaires sont nécessaires après la vérification, cliquez sur  (Événements) dans la barre d'icônes.

- 6 Dans la page **Événements**, cliquez sur l'icône  **Détails de la tâche** de la tâche pour afficher des informations complémentaires sur son état.

- Si vous voyez une erreur dans l'une des sous-tâches de cette tâche, notez l'erreur et communiquez-la au représentant de l'assistance technique de Dell.
- Si toutes les sous-tâches de la tâche de vérification de logithèque se terminent sans erreur, vous pouvez établir une stratégie de rétention personnalisée pour cette logithèque.

Gestion de la sécurité

Le Core peut crypter les données d'instantané de machine protégée dans le référentiel. Au lieu de crypter l'ensemble du référentiel, vous pouvez indiquer une clé de chiffrement au cours de la protection d'une machine dans un référentiel, ce qui permet la réutilisation des clés pour différentes machines protégées. Le cryptage n'affecte pas les performances, car chaque clé de cryptage active crée un domaine de cryptage. Ainsi, un même core peut prendre en charge plusieurs locataires en hébergeant plusieurs domaines de cryptage. Dans un environnement multilocataire, les données sont partitionnées et dédoublées au sein des domaines de cryptage. Comme vous gérez les clés de cryptage, elles ne peuvent pas être révélées suite à une perte de volume. Voici les principaux concepts et considérations de sécurité :

- Le cryptage est réalisé au format AES 256 bits en mode CBC (Cipher Block Chaining), conforme SHA-3.
- La déduplication fonctionne au sein d'un domaine de cryptage pour assurer la confidentialité
- Le cryptage n'a aucun effet sur les performances.
- Vous pouvez ajouter, retirer, importer, exporter, modifier et supprimer des clés de cryptage configurées sur le Core.
- Le nombre de clés de chiffrement que vous pouvez créer sur le Core est illimité.

Application ou retrait du chiffrement d'une machine protégée

Vous pouvez sécuriser les données protégées sur votre Core à n'importe quel moment en définissant une clé de chiffrement et en l'appliquant à une ou plusieurs machines protégées dans votre logithèque. Vous pouvez appliquer une clé de chiffrement unique à n'importe quel nombre de machines protégées, mais une machine protégée donnée ne peut utiliser qu'une clé de chiffrement qui lui est appliquée à la fois.

L'étendue de la déduplication dans Rapid Recovery est limitée aux machines protégées utilisant la même logithèque et la même clé de chiffrement. En conséquence, pour maximiser la valeur de la déduplication, Dell vous conseille d'appliquer une clé de chiffrement à un maximum de machines protégées. Toutefois, le nombre de clés de chiffrement que vous pouvez créer sur le Core est illimité. Ainsi, si la conformité légale, les règles de sécurité, les politiques de confidentialité ou d'autres circonstances l'exigent, vous pouvez ajouter et gérer n'importe quel nombre de clés de chiffrement. Vous pouvez alors appliquer chacune des clés à une seule machine protégée, ou à n'importe quel ensemble de machines de votre logithèque.

Chaque fois que vous appliquez une clé de chiffrement à une machine protégée, ou dissociez une clé de chiffrement d'une machine protégée, Rapid Recovery prend une nouvelle image de base pour cette machine lors du prochain instantané planifié ou forcé. Les données stockées dans cette image de base (et tous les instantanés incrémentiels suivants pris lorsqu'une clé de chiffrement est appliquée) sont protégées par une norme AES 256 bits. Il n'existe aucune méthode connue pour compromettre ce mode de chiffrement.

Lorsque vous modifiez le nom ou la phrase secrète d'une clé de chiffrement actuellement utilisée sur une machine protégée, le Core Rapid Recovery capture et reflète les propriétés mises à jour de la clé lors du prochain instantané planifié ou forcé. Les données stockées dans cette image (et tous les instantanés incrémentiels suivants pris lorsqu'une clé de chiffrement est appliquée) sont protégées par une norme AES 256 bits. Il n'existe aucune méthode connue pour compromettre ce mode de chiffrement.

Une fois une clé de chiffrement créée et appliquée à une machine protégée, il existe deux concepts impliqués dans la suppression de ce chiffrement. Le premier consiste à dissocier la clé de la machine protégée. Lorsque la clé de chiffrement est dissociée de toutes les machines protégées, vous pouvez également la supprimer du Core Rapid Recovery.

Cette section contient les rubriques suivantes :

- [Associer une clé de chiffrement à une machine protégée](#)
- [Application d'une clé de chiffrement depuis la page Machines protégées](#)
- [Dissocier une clé de chiffrement d'une machine protégée](#)

Associer une clé de chiffrement à une machine protégée

Vous pouvez appliquer une clé de chiffrement à une machine protégée en utilisant l'une des deux méthodes suivantes :

- **Dans le cadre de la protection d'une machine.** Lorsque vous utilisez cette méthode, vous pouvez appliquer le chiffrement à une ou plusieurs machines simultanément. Cette méthode vous permet d'ajouter une nouvelle clé de chiffrement, ou d'appliquer une clé existante à la ou les machines sélectionnées.
Pour utiliser le chiffrement lorsque vous avez défini la protection d'une machine pour la première fois, vous devez sélectionner les options avancées dans l'assistant Protéger les machines. Cette sélection ajoute une page Chiffrement au flux de travaux de l'assistant. Depuis cette page, sélectionnez **Activer le chiffrement**, puis sélectionnez une clé de chiffrement existante ou spécifiez les paramètres d'une nouvelle clé. Pour en savoir plus, voir [Protéger une machine](#) ou [À propos de la protection de plusieurs machines](#), respectivement.
- **En modifiant les paramètres de configuration d'une machine.** Cette méthode applique une clé de chiffrement à une machine protégée à la fois. Il existe deux approches pour modifier les paramètres de configuration d'une machine dans l'interface utilisateur de Rapid Recovery :
 - Modifier les paramètres de configuration d'une machine protégée spécifique. La clé de chiffrement à utiliser pour cette approche doit déjà exister sur le Core Rapid Recovery, être une clé universelle et être déverrouillée. Le chiffrement fait partie des paramètres généraux. Pour plus d'informations, voir [Paramètres d'affichage et de modification des machines protégées](#).
 - Cliquer sur l'icône  **Non chiffré** de la page Machines protégées. Avec cette approche, vous pouvez créer et appliquer une nouvelle clé de chiffrement, ou attribuer une clé universelle déverrouillée existante à la machine protégée spécifiée. Pour plus d'informations, voir [Application d'une clé de chiffrement depuis la page Machines protégées](#).

Application d'une clé de chiffrement depuis la page Machines protégées

Lorsqu'une clé de chiffrement a été ajoutée à un Core Rapid Recovery, elle peut être utilisée pour n'importe quel nombre de machines protégées.

Si vous sélectionnez une clé de chiffrement lors de la protection initiale d'une ou plusieurs machines, la clé est automatiquement appliquée à toutes les machines que vous protégez à l'aide de cet assistant. Dans ce cas, cette procédure n'est pas nécessaire.

Effectuez cette procédure :

- Si vous souhaitez appliquer une clé de chiffrement existante, universelle, déverrouillée à n'importe quelle machine protégée dans votre Core.

- Si vous venez d'ajouter une nouvelle clé de chiffrement en suivant la procédure décrite dans la rubrique [Ajout d'une clé de chiffrement](#) et que vous souhaitez appliquer cette clé à une machine protégée.
- Si une clé de chiffrement est déjà appliquée à une machine protégée dans votre Core, mais que vous souhaitez remplacer cette clé par une autre clé universelle et déverrouillée disponible dans votre Core.

⚠ PRÉCAUTION : Après avoir appliqué une clé de chiffrement à une machine protégée, Rapid Recovery prend une nouvelle image de base pour cette machine lors du prochain instantané programmé ou forcé.

- 1 Naviguez jusqu'au Rapid Recovery Core et cliquez sur **Machines protégées**.

La page **Machines protégées** s'affiche, répertoriant toutes les machines protégées par ce Core. Un cadenas ouvert  s'affiche

pour toutes les machines qui ne possèdent pas de clé de chiffrement. Un cadenas fermé  indique qu'une clé de chiffrement est appliquée à la machine protégée.

- 2 Dans le volet Machines protégées, cliquez sur l'icône représentant un cadenas pour la machine protégée que vous souhaitez configurer.

La boîte de dialogue **Configuration du chiffrement** s'affiche.

- 3 Effectuez l'une des opérations suivantes :

- Si vous souhaitez appliquer une clé de chiffrement à cette machine, sélectionnez **Chiffrer les données grâce au chiffrement de Core avec une clé de chiffrement existante**, puis sélectionnez la clé appropriée dans le menu déroulant. Cliquez sur **OK** pour confirmer.
- Si vous souhaitez remplacer une clé de chiffrement par une autre clé universelle et déverrouillée, sélectionnez **Chiffrer les données grâce au chiffrement de Core avec une nouvelle clé de chiffrement**, puis sélectionnez la clé appropriée dans le menu déroulant. Cliquez sur **OK** pour confirmer.
- Si vous souhaitez créer une nouvelle clé de chiffrement et l'appliquer à cette machine protégée, sélectionnez **Chiffrer les données grâce au chiffrement de Core avec une nouvelle clé de chiffrement**. Puis entrez les détails de la clé tel que décrit dans le tableau suivant.

Tableau 34. Détails de la nouvelle clé de chiffrement

Zone de texte	Description
Nom	Entrez le nom de la clé de chiffrement. Les noms des clés de chiffrement doivent contenir entre 1 et 64 caractères alphanumériques. N'utilisez pas de caractères interdits ni d' expressions interdites .
Description	Entrez un commentaire descriptif pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lorsque vous regardez la liste des clés de chiffrement dans Rapid Recovery Core Console. Les descriptions peuvent contenir jusqu'à 254 caractères. Il est conseillé d'éviter d'utiliser les caractères interdits et les expressions interdites .
Phrase secrète	Entrez une phrase secrète servant à contrôler les accès. Il est conseillé d'éviter d'utiliser les caractères interdits . Conservez la phrase secrète à un emplacement sûr. Le support technique de Dell ne peut pas retrouver une phrase secrète. Après avoir créé une clé de chiffrement et après l'avoir appliquée à une ou plusieurs machines protégées, vous ne pourrez plus récupérer les données si vous perdez la phrase secrète.
Confirmez la phrase secrète	Entrez à nouveau la phrase secrète. Permet de confirmer la saisie de la phrase secrète.

- 4 Cliquez sur **OK**.

La boîte de dialogue se ferme. La clé de chiffrement que vous avez spécifiée a été appliquée aux futures sauvegardes pour cette machine protégée, et l'icône cadenas s'affiche maintenant fermée.

De manière facultative, si vous souhaitez que la clé de chiffrement soit appliquée immédiatement, forcez un instantané. Pour plus d'informations, reportez-vous à [Forcer un instantané](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous conseille vivement d'établir une clé de chiffrement et de protéger la phrase secrète que vous définissez. Conservez la phrase secrète dans un lieu sûr, car elle est indispensable à la restauration des données. Sans phrase secrète, la restauration des données est impossible.

Dissocier une clé de chiffrement d'une machine protégée

Lorsqu'une clé de chiffrement a été appliquée à une machine protégée, toutes les données d'instantané suivantes sont chiffrées sur le Core de Rapid Recovery.

Vous pouvez dissocier une clé de chiffrement d'une machine protégée. Cette opération ne déchiffre pas les données d'instantané existantes, mais entraîne la création d'une nouvelle image de base pour cette machine lors du prochain instantané planifié ou forcé.

REMARQUE : Si vous voulez supprimer une clé de chiffrement du Core, comme il est décrit dans la rubrique [Supprimer une clé de chiffrement](#), vous devez d'abord dissocier cette clé de chiffrement de toutes les machines protégées.

Suivez cette procédure pour dissocier une clé de chiffrement d'une machine protégée spécifique.

- 1 Naviguez jusqu'au Core de Rapid Recovery et cliquez sur **Machines protégées**.

La page Machines protégées s'affiche, répertoriant toutes les machines protégées par ce Core. Un cadenas ouvert  s'affiche

pour toutes les machines qui ne possèdent pas de clé de chiffrement. Un cadenas fermé  indique qu'une clé de chiffrement est appliquée à la machine protégée.

- 2 Dans le volet Machines protégées, cliquez sur l'icône  **Chiffré** pour la machine protégée que vous souhaitez configurer. La boîte de dialogue **Configuration du chiffrement** s'affiche.
- 3 Sélectionnez **Chiffrer les données en utilisant un chiffrement basé sur le Core avec une clé existante** et sélectionnez **(Aucun)** dans le menu déroulant, puis cliquez sur **OK**.
- 4 Si vous souhaitez supprimer cette clé de chiffrement du Core de Rapid Recovery, répétez d'abord cette procédure pour toutes les machines protégées utilisant cette clé. Suivez ensuite la procédure décrite dans la rubrique [Supprimer une clé de chiffrement](#).

Gérer les clés de chiffrement

Pour gérer les clés de chiffrement du Core Rapid Recovery, dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**. La page **Clés de chiffrement** s'affiche. Pour chaque clé de chiffrement ajoutée à votre Core Rapid Recovery (le cas échéant), les informations indiquées dans le tableau suivant s'affichent.

Tableau 35. Informations sur chaque clé de chiffrement

Élément de l'IU	Description
Sélection d'éléments	Pour chaque clé de chiffrement, vous pouvez cocher la case pour réaliser des actions dans la liste des options de menu se trouvant au-dessus du tableau.
Nom	Le nom associé à la clé de chiffrement.
Empreinte	Ce paramètre est une chaîne de 26 caractères alphabétiques générés de façon aléatoire et combinant des majuscules et des minuscules de l'alphabet anglais, qui sert à identifier de façon unique chaque clé de chiffrement.
Type	Le type décrit le point d'origine d'une clé de chiffrement et la possibilité de l'appliquer. Une clé de chiffrement peut contenir l'un des deux types suivants : Universel. Le type Universel est le type défini par défaut pour la création d'une clé de chiffrement. Lorsqu'une clé est de type Universel et que son état est Déverrouillé, elle peut être appliquée à une machine protégée. Vous ne

Élément de l'IU	Description
	pouvez pas verrouiller manuellement un type de clé Universel ; vous devez d'abord modifier son type en suivant la procédure Modifier le type de clé de chiffrement. Réplication. Lorsque le chiffrement est activé sur une machine protégée d'un Core source, et que les points de restauration de cette machine sont répliqués sur un Core cible, toutes les clés de chiffrement utilisées dans la source apparaissent automatiquement avec le type Réplication sur le Core cible. L'état par défaut après réception d'une clé répliquée est Verrouillé. Vous pouvez déverrouiller une clé de chiffrement de type Réplication à l'aide de la phrase secrète. Si une clé est de type Déverrouillé, vous pouvez la verrouiller manuellement. Pour en savoir plus, voir la rubrique Déverrouillage d'une clé de chiffrement.
État	L'état indique si une clé de chiffrement peut être utilisée. Les deux états possibles sont : • Déverrouillé. Un état Déverrouillé indique que la clé peut être utilisée immédiatement. Par exemple, vous pouvez chiffrer des snapshots pour une machine protégée, ou effectuer une restauration des données à partir d'un point de restauration répliqué sur le Core cible. • Verrouillé. Un état Verrouillé indique que la clé ne peut pas être utilisée tant qu'elle n'est pas déverrouillée en fournissant la phrase secrète. L'état Verrouillé est l'état par défaut pour une clé de chiffrement nouvellement importée ou répliquée. Si l'état d'une clé de chiffrement est Verrouillé, cette clé doit être déverrouillée avant de pouvoir être utilisée. Si vous avez préalablement déverrouillé une clé de chiffrement verrouillée et que le délai pendant lequel elle reste déverrouillée a expiré, l'état repasse de Déverrouillé à Verrouillé. Après le verrouillage automatique de la clé, vous devez la déverrouiller une nouvelle fois avant de pouvoir l'utiliser. Pour en savoir plus, voir la rubrique Déverrouillage d'une clé de chiffrement.
Description	La description est un champ facultatif qu'il est recommandé de remplir pour fournir des informations utiles concernant la clé de chiffrement, comme son utilisation prévue ou un indice pour retrouver la phrase secrète.

Au niveau supérieur du volet Clés de chiffrement, vous pouvez ajouter une clé de chiffrement ou importer une clé à l'aide d'un fichier exporté à partir d'un autre Core Rapid Recovery. Vous pouvez également supprimer des clés sélectionnées dans le tableau récapitulatif.

Lorsqu'une clé de chiffrement existe pour un Core, vous pouvez gérer les clés existantes en modifiant le nom ou les propriétés de la description, en modifiant la phrase secrète, en déverrouillant une clé de chiffrement verrouillée ou en supprimant la clé du Core Rapid Recovery. Vous pouvez également exporter une clé dans un fichier, qui peut à son tour être importé dans un autre Core Rapid Recovery.

Lorsque vous ajoutez une clé de chiffrement sur la page **Clés de chiffrement**, la clé en question s'affiche dans la liste des clés de chiffrement, mais elle n'est appliquée à aucune machine protégée spécifique. Pour plus d'informations sur l'application d'une clé de chiffrement créée à partir du volet **Clés de chiffrement**, ou pour supprimer complètement une clé du Core Rapid Recovery, voir [Application ou retrait du chiffrement d'une machine protégée](#).

Dans le volet **Clés de chiffrement**, vous pouvez gérer la sécurité des données de sauvegarde enregistrées sur le Core de toutes les machines protégées dans votre logithèque, en procédant comme suit :

- [Ajout d'une clé de chiffrement](#)
- [Importer une clé de chiffrement](#)
- [Déverrouillage d'une clé de chiffrement](#)
- [Modifier une clé de chiffrement](#)
- [Modifier la phrase secrète d'une clé de chiffrement](#)
- [Exporter une clé de chiffrement](#)
- [Supprimer une clé de chiffrement](#)
- [Modifier le type de clé de chiffrement](#)

Ajout d'une clé de chiffrement

Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous conseille vivement d'établir une clé de chiffrement et de protéger la phrase secrète que vous définissez.

⚠ PRÉCAUTION : conservez la phrase secrète dans un lieu sûr. Sans elle, vous ne pourrez pas récupérer de données depuis un point de restauration chiffré.

Après avoir défini une clé de chiffrement, vous pouvez l'utiliser pour protéger vos données. Les clés de chiffrement peuvent être utilisées par n'importe quel nombre de machines protégées.

Cette étape décrit comment ajouter une clé de chiffrement depuis la Rapid Recovery Core Console. Cette procédure n'applique pas la clé aux machines actuellement protégées sur le Core. Vous pouvez également ajouter une clé de chiffrement lors du processus de protection d'une machine. Pour en savoir plus sur l'ajout du chiffrement dans le cadre de la protection d'une machine, voir [Protéger une machine](#). Pour en savoir plus sur l'ajout du chiffrement pour deux machines ou plus tout en les protégeant pour la première fois, voir [À propos de la protection de plusieurs machines](#).

Effectuez les étapes de cette procédure pour ajouter une clé de chiffrement.

- 1 Naviguez jusqu'à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- 3 Cliquez sur **Ajouter une clé de chiffrement**.
La boîte de dialogue **Créer une clé de chiffrement** s'affiche.
- 4 Dans la boîte de dialogue **Créer une clé de chiffrement**, entrez les détails de la clé comme indiqué dans le tableau suivant.

Tableau 36. Détails de la création d'une clé de chiffrement

Zone de texte	Description
Nom	Entrez le nom de la clé de chiffrement. Les noms des clés de chiffrement doivent contenir entre 1 et 64 caractères alphanumériques. N'utilisez pas de caractères interdits ni d' expressions interdites .
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lorsque vous regardez les clés de chiffrement de la Core Console. Vous pouvez entrer jusqu'à 254 caractères. Il est conseillé d'éviter d'utiliser des caractères interdits et des expressions interdites .
Phrase secrète	Entrez une phrase secrète servant à contrôler les accès. Il est conseillé d'éviter d'utiliser des caractères interdits . ⚠ PRÉCAUTION : conservez la phrase secrète à un emplacement sûr. Le support Dell ne peut pas retrouver une phrase secrète. Après avoir créé une clé de chiffrement et après l'avoir appliquée à une ou plusieurs machines protégées, vous ne pourrez plus récupérer les données si vous perdez la phrase secrète.
Confirmer la phrase secrète	Entrez à nouveau la phrase secrète. Permet de confirmer la saisie de la phrase secrète.

- 5 Cliquez sur **OK**.
La boîte de dialogue se ferme et la clé de chiffrement que vous avez créée devient visible sur la page Clés de chiffrement.

- 6 Pour appliquer la clé de chiffrement à une machine protégée, voir [Application d'une clé de chiffrement depuis la page Machines protégées](#).

Importer une clé de chiffrement

Vous pouvez importer une clé de chiffrement depuis un autre Core de Rapid Recovery et utiliser cette clé pour chiffrer les données d'une machine protégée sur votre Core. Pour importer la clé, vous devez pouvoir y accéder depuis le core, soit localement, soit par le biais de votre réseau. Vous devez également connaître la phrase secrète pour la clé de chiffrement.

Effectuez cette procédure pour importer une clé de chiffrement.

REMARQUE : Cette procédure n'applique la clé à aucune des machines protégées. Pour en savoir plus sur la façon d'appliquer la clé, voir [Application d'une clé de chiffrement depuis la page Machines protégées](#).

- 1 Naviguez jusqu'au Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- 3 Cliquez sur  **Importer**.
La boîte de dialogue **Charger un fichier** apparaît.
- 4 Dans la boîte de dialogue **Charger un fichier**, naviguez jusqu'au répertoire de réseau ou local contenant la clé de chiffrement à importer.
Par exemple, naviguez vers le fichier **Téléchargements** pour l'utilisateur connecté.

Le nom de fichier de la clé commence par « EncryptionKey- », suivi de l'identifiant de clé, et se termine par l'extension de fichier .key.
Par exemple, un nom de clé de chiffrement pourra être EncryptionKey-RandomAlphabeticCharacters.key.

- 5 Sélectionnez la clé à modifier, puis cliquez sur **Ouvrir**.
- 6 Dans la boîte de dialogue **Importer une clé**, cliquez sur **OK**.
La boîte de dialogue se ferme et la clé de chiffrement que vous avez importée apparaît sur la page **Clés de chiffrement**. Si la clé de chiffrement a été utilisée pour protéger un volume avant son importation, l'état de la clé est Verrouillé.

Déverrouillage d'une clé de chiffrement

Les clés de chiffrement peuvent afficher l'état Déverrouillé ou Verrouillé. Une clé de chiffrement déverrouillée peut être appliquée à une machine protégée pour sécuriser les données sauvegardées pour cette machine dans la logithèque. Vous pouvez également récupérer des données depuis un point de restauration sur un Core Rapid Recovery à l'aide d'une clé de chiffrement déverrouillée.

Lorsque vous importez une clé de chiffrement dans un Core Rapid Recovery, son état par défaut est Verrouillé. Cela reste toujours valable, que vous ayez explicitement importé la clé, ou que vous l'ayez ajoutée au Core Rapid Recovery en répliquant des machines protégées chiffrées ou en important une archive de points de restauration chiffrés.

Pour les clés de chiffrement ajoutées au Core Rapid Recovery par réplication uniquement, lorsque vous déverrouillez une clé, vous pouvez spécifier une durée (en heures, en jours ou en mois) pendant laquelle cette clé restera déverrouillée. Chaque journée repose sur une période de 24 heures, qui démarre à partir du moment où la demande de déverrouillage est enregistrée sur le Core Rapid Recovery. Par exemple, si la clé est déverrouillée à 11:24 le mardi, et que la durée choisie est de 2 jours, la clé se reverrouillera automatiquement à 11:24 le jeudi suivant.

REMARQUE : vous ne pouvez pas utiliser une clé de chiffrement verrouillée pour récupérer des données ou pour l'appliquer à une machine protégée. Vous devez d'abord fournir la phrase secrète pour déverrouiller la clé.

Vous pouvez aussi verrouiller une clé de chiffrement déverrouillée, pour empêcher qu'elle puisse être appliquée à une machine protégée tant qu'elle n'a pas été déverrouillée. Pour verrouiller une clé de chiffrement dans l'état Universel, vous devez d'abord définir son type sur Répliqué.

Si une clé de chiffrement déverrouillée est actuellement utilisée pour protéger une machine dans le Core, vous devez d'abord dissocier cette clé de chiffrement de la machine protégée avant de pouvoir la verrouiller.

Suivez les étapes de cette procédure pour déverrouiller une clé de chiffrement verrouillée.

- 1 Accédez au Core Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche. La colonne État indique quelles clés de chiffrement sont verrouillées.
- 3 Localisez la clé de chiffrement à déverrouiller, cliquez sur le menu déroulant  (Paramètres), puis sélectionnez **Déverrouiller**.
La boîte de dialogue **Déverrouiller une clé de chiffrement** apparaît.
- 4 Dans le champ Phrase secrète de la boîte de dialogue, saisissez la phrase secrète pour déverrouiller cette clé.
- 5 Pour spécifier la durée pendant laquelle la clé doit rester déverrouillée, accédez à l'option Durée et effectuez l'une des opérations suivantes :
 - Pour spécifier que la clé doit rester déverrouillée tant que vous ne la verrouillez pas explicitement vous-même, accédez à Rapid Recovery et sélectionnez **Jusqu'à verrouillage manuel**.
 - Pour spécifier que la clé doit rester verrouillée pendant une durée donnée (en heures, en jours ou en mois), procédez comme suit :
 - Sélectionnez le champ Numéro et saisissez une valeur comprise entre 1 et 999.
 - Spécifiez la durée souhaitée en heures, en jours ou en mois.
 - Cliquez ensuite sur **OK**.Cette option est proposée pour toutes les clés de chiffrement ajoutées par réplication.

La boîte de dialogue se ferme et les modifications de la clé de chiffrement sélectionnée apparaissent sur la page Clés de chiffrement.
- Pour spécifier que la clé doit rester verrouillée jusqu'à la date et l'heure indiquées, procédez comme suit :
 - Sélectionnez l'option **Jusqu'à**.
 - Dans la boîte de texte (ou à l'aide des widgets Calendrier et Horloge), spécifiez explicitement les données et l'heure à laquelle vous souhaitez que la clé de cryptage se verrouille.
 - Cliquez ensuite sur **OK**.Cette option est proposée pour toutes les clés de chiffrement ajoutées par réplication.

La boîte de dialogue se ferme et les modifications de la clé de chiffrement sélectionnée apparaissent sur la page Clés de chiffrement.

Verrouillage d'une clé de chiffrement

Lorsqu'une clé de chiffrement est à l'état verrouillé, elle ne peut pas être appliquée à une machine protégée avant son déverrouillage. Pour verrouiller une clé de chiffrement avec le type Universel, vous devez d'abord changer son type en Répliqué.

Suivez cette procédure pour verrouiller une clé de chiffrement.

- 1 Naviguez jusqu'au Core de Rapid Recovery.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche. La colonne État indique quelles clés de chiffrement sont déverrouillées, et indique le type de chaque clé.
- 3 Localisez la clé de chiffrement que vous souhaitez verrouiller. Si son type est Universel, cliquez sur son menu déroulant , puis sélectionnez **Changez le type en Répliqué**.
La boîte de dialogue **Modifier le type de clé de chiffrement** apparaît.
- 4 Dans la boîte de dialogue, confirmez que vous voulez modifier le type en **Répliqué**.

- Si vous avez modifié avec succès l'état de la clé de chiffrement sur Répliqué, cliquez sur son menu déroulant , puis sélectionnez **Verrouiller**.

La boîte de dialogue **Verrouiller une clé de chiffrement** apparaît.

- Dans la boîte de dialogue, confirmez que vous voulez verrouiller la clé de chiffrement.
La boîte de dialogue se ferme et l'état de la clé de chiffrement sélectionnée est maintenant « Verrouillé ».

 **REMARQUE :** Cette option est proposée pour toutes les clés de chiffrement ajoutées par réplication.

Modifier une clé de chiffrement

Après avoir défini une clé de chiffrement, vous pouvez modifier le nom de la clé de chiffrement ou la description de la clé. Ces propriétés sont visibles lorsque vous affichez la liste des clés de chiffrement dans le volet Clés de chiffrement.

Effectuez les étapes de cette procédure pour modifier le nom ou la description d'une clé de chiffrement déverrouillée existante.

 **PRÉCAUTION :** Une fois que vous avez modifié le nom ou la description d'une clé de chiffrement utilisée pour protéger une ou plusieurs machines, Rapid Recovery prend une nouvelle image de base. Cet instantané d'image de base se produira pour cette machine lors du prochain instantané planifié ou forcé.

- Naviguez jusqu'au Core de Rapid Recovery.
- Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- Localisez la clé de chiffrement que vous souhaitez modifier et effectuez les opérations suivantes :
 - Si la clé est verrouillée, vous devez d'abord la déverrouiller. Voir [Déverrouillage d'une clé de chiffrement](#)
 - Si la clé est déverrouillée, procédez comme décrit ci-dessous.
- Cliquez sur le menu déroulant  pour la clé de chiffrement spécifiée et sélectionnez **Modifier**.
La boîte de dialogue **Modifier la clé de cryptage** apparaît.
- Dans la boîte de dialogue, modifiez le nom ou la description de la clé de chiffrement, puis cliquez sur **OK**.
La boîte de dialogue se ferme et les modifications de la clé de chiffrement sélectionnée apparaissent sur la page **Clés de chiffrement**.

Modifier la phrase secrète d'une clé de chiffrement

Pour assurer un maximum de sécurité, vous pouvez modifier la phrase de passe pour n'importe quelle clé de chiffrement existante. Effectuez cette procédure pour modifier la phrase secrète d'une clé de chiffrement.

 **PRÉCAUTION :** Après la modification de la phrase secrète d'une clé de chiffrement utilisée pour protéger une ou plusieurs machines, le Core de Rapid Recovery capture un instantané incrémentiel pour cette machine lors du prochain instantané planifié ou forcé.

- Naviguez jusqu'au Core de Rapid Recovery.
- Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- Recherchez la clé de chiffrement que vous souhaitez mettre à jour, cliquez sur son menu déroulant , puis sélectionnez **Modifier la phrase secrète**.
La boîte de dialogue **Modifier la phrase d'authentification** s'affiche.
- Dans le champ **Phrase secrète** de la boîte de dialogue, entrez la nouvelle phrase secrète pour le chiffrement.
- Dans le champ **Confirmez la phrase secrète**, saisissez de nouveau la phrase secrète.
- Cliquez sur **OK**.

La boîte de dialogue se ferme et la phrase secrète est mise à jour.

- Vous pouvez aussi, si vous utilisez un conseil dans le champ Description, modifier la clé de chiffrement pour mettre à jour le conseil. Pour plus d'informations, voir [Modifier une clé de chiffrement](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining) avec des clés de 256 bits. Dell recommande d'enregistrer la phrase secrète dans un emplacement sûr et de maintenir ces informations à jour. Le support technique de Dell ne peut pas retrouver une phrase secrète. Sans cette phrase secrète, vous ne pourrez pas récupérer d'informations de points de restauration chiffrés.

Exporter une clé de chiffrement

Vous pouvez exporter une clé de chiffrement à partir de n'importe quel Core de Rapid Recovery si vous souhaitez expressément l'utiliser sur un autre Core. Lorsque vous suivez cette procédure, la clé est enregistrée dans le dossier **Téléchargements** du compte d'utilisateur Windows actif.

Effectuez cette procédure pour exporter une clé de chiffrement.

- Naviguez jusqu'au Core de Rapid Recovery.
- Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- Localisez la clé de chiffrement à exporter, cliquez sur le menu déroulant  et sélectionnez **Exporter**.
La boîte de dialogue **Ouverture de la clé de chiffrement-[nom.clé]** s'affiche.
- Dans la boîte de dialogue, cliquez sur **Enregistrer le fichier** pour enregistrer et stocker les clés de chiffrement dans un emplacement sécurisé, puis cliquez sur **OK**.
La clé de chiffrement est téléchargée en tant que fichier texte à l'emplacement par défaut, tels que le dossier **Téléchargements** du compte d'utilisateur Windows actif.
- Si vous souhaitez importer cette clé dans un autre Core, copiez le fichier dans un emplacement accessible à partir de ce Core.

Supprimer une clé de chiffrement

Lorsque vous retirez une clé de chiffrement de la page Clé de chiffrement, la clé est supprimée du Core Rapid Recovery.

REMARQUE : Supprimer une clé de chiffrement ne permet pas de déchiffrer les points de restauration déjà enregistrés utilisant la clé. Vous devez quand même conserver et fournir la phrase secrète pour que la clé puisse récupérer les données des points de restauration chiffrés existants.

Vous ne pouvez pas supprimer une clé de chiffrement déjà associée à une machine protégée. Vous devez d'abord afficher les paramètres de chiffrement de chacune des machines protégées qui utilisent la clé, puis dissocier la clé de chiffrement que vous souhaitez supprimer. Pour plus d'informations, consultez la rubrique [Dissocier une clé de chiffrement d'une machine protégée](#).

Effectuez cette procédure pour supprimer une clé de chiffrement.

- Naviguez jusqu'au Core Rapid Recovery.
- Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche.
- Localisez la clé de chiffrement que vous souhaitez retirer. Cliquez sur le menu déroulant  et sélectionnez **Retirer**.
La boîte de dialogue **Retirer la clé de chiffrement** s'affiche. Un message s'affiche demandant de confirmer la suppression de la clé de chiffrement.
- Dans la boîte de dialogue, confirmez que vous souhaitez supprimer la clé de chiffrement.

REMARQUE : Supprimer une clé de chiffrement ne permet pas de déchiffrer les points de restauration utilisant la clé déjà enregistrés. Vous devez quand même conserver et fournir la clé pour récupérer les données des points de restauration chiffrés existants.

La boîte de dialogue se ferme et la clé de chiffrement que vous avez supprimée disparaît dans la page **Clés de chiffrement**.

Modifier le type de clé de chiffrement

Dans le volet **Clés de chiffrement**, les clés de chiffrement apparaissent sous l'un ou l'autre des deux types possibles suivants : **Universel** ou **Réplication**. Ce type indique l'origine probable de la clé de chiffrement, et détermine si vous pouvez modifier ses détails ou sa phrase secrète. Vous pouvez modifier ces attributs uniquement si le type est **Universel**. Si vous devez modifier ces attributs pour une clé de type **Répliqué**, vous devez changer son type en **Universel** en utilisant cette procédure. Si vous modifiez le type d'une clé de chiffrement en **Universel**, elle est déverrouillée manuellement et peut être utilisée pour chiffrer d'autres machines protégées.

REMARQUE : Vous devez connaître la phrase secrète pour modifier le type de **Répliqué** en **Universel**.

Les clés de chiffrement ont également deux états possibles : **Verrouillé** ou **Déverrouillé**. L'état contrôle votre capacité à appliquer une clé de chiffrement à une machine protégée, ou à restaurer des données à partir d'un point de restauration chiffré. Vous pouvez modifier le type d'une clé de chiffrement manuellement uniquement si l'état est **Déverrouillé**.

Lorsque vous créez une clé de chiffrement pour la première fois, son type est **Universel**, et son état est **Déverrouillé**. Vous pouvez utiliser une telle clé immédiatement (par exemple, pour chiffrer les sauvegardes d'une machine protégée). Cependant, le type de clé **Universel** ne peut pas être verrouillé manuellement. Si vous souhaitez verrouiller manuellement une clé de chiffrement de type **Universel**, vous devez changer le type en **Répliqué** à l'aide de cette procédure.

Vous ne pouvez pas modifier un type de clé de chiffrement si celle-ci est déjà en cours de chiffrement de points de restauration sur une ou plusieurs machines protégées.

Suivez cette procédure pour modifier le type de clé de chiffrement.

- 1 Naviguez jusqu'au **Core de Rapid Recovery**.
- 2 Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Clés de chiffrement**.
La page **Clés de chiffrement** s'affiche. Les clés de chiffrement accessibles pour le Core apparaissent dans un tableau récapitulatif. Chaque clé fait apparaître un type **Universel** ou **Répliqué**.
- 3 Localisez la clé de chiffrement que vous souhaitez mettre à jour.
- 4 Si vous souhaitez modifier une clé de chiffrement **Universel** en **Réplication**, procédez comme suit :
 - a Cliquez sur le menu déroulant , puis sélectionnez **Changez le type en Répliqué**.
La boîte de dialogue **Modifier le type de clé de chiffrement** apparaît. Un message vous demandant de confirmer que vous voulez modifier le type en **Répliqué** s'affiche.
 - Dans la boîte de dialogue, confirmez que vous voulez modifier le type en **Répliqué**.
- La boîte de dialogue se ferme et le type de la clé de chiffrement se met à jour en **Répliqué**.
- 5 Si vous souhaitez modifier une clé de chiffrement **Réplication** en **Universel**, effectuez les opérations suivantes :
 - a Cliquez sur le menu déroulant , puis sélectionnez **Changez le type en Universel**.
La boîte de dialogue **Modifier le type de clé de chiffrement** apparaît. Un message vous demandant de confirmer que vous voulez modifier le type en **Universel** s'affiche.
 - Dans le champ **Phrase secrète** de la boîte de dialogue, saisissez la phrase secrète, puis cliquez sur **OK** pour confirmer que vous souhaitez modifier le type en **Universel**.

La boîte de dialogue se ferme et le type de la clé de chiffrement se met à jour en **Universel**.

Gestion des comptes Cloud

Cette section décrit comment définir des liens vers des comptes de fournisseur de stockage Cloud existants, et comment gérer ces comptes Cloud pour les utiliser avec Rapid Recovery. Par exemple, vous pouvez archiver des données de Rapid Recovery sur le Cloud, ou importer des données archivées depuis le Cloud.

À propos des comptes Cloud

Rapid Recovery permet d'archiver des données sur un grand nombre de Clouds de fournisseurs différents, ou d'importer des données archivées stockées sur un compte Cloud. Les Clouds compatibles incluent Microsoft Azure, Amazon™, Rackspace et tout fournisseur OpenStack.

Vous pouvez ajouter votre compte Cloud existant à la console Core Rapid Recovery. Une fois celui-ci ajouté, vous pouvez modifier les informations, configurer les options de connexion au compte, ou supprimer le compte de Rapid Recovery.

Ajouter un compte cloud

Avant de pouvoir déplacer les données dans un sens ou dans l'autre entre un compte Cloud et votre Core, vous devez ajouter les informations relatives au compte du fournisseur de Cloud à la Rapid Recovery Core Console. Ces informations identifient le compte Cloud dans la Core Console tout en mettant en cache les informations de connexion en toute sécurité. Ce processus permet au Rapid Recovery Core de se connecter au compte Cloud pour effectuer les opérations que vous spécifiez.

Pour ajouter un compte Cloud, procédez comme suit.

- 1 Sur la barre d'icône de la Rapid Recovery Core Console, cliquez sur l'icône  **Plus**, puis sélectionnez **Comptes Cloud**. La page **Comptes Cloud** s'affiche.
- 2 Sur la page **Comptes Cloud**, cliquez sur **Ajouter un nouveau compte**. La boîte de dialogue **Ajouter un nouveau compte** s'ouvre.
- 3 Sélectionnez un fournisseur Cloud compatible dans la liste déroulante Type de cloud.
- 4 Entrez les informations décrites dans le tableau suivant en fonction du type de Cloud sélectionné à l'étape 3.

Tableau 37. Détails du compte cloud

Type de cloud	Zone de texte	Description
Microsoft Azure	Nom du compte de stockage	Entrez le nom du compte de stockage Microsoft Azure.  REMARQUE : Le nom doit être strictement identique au nom du compte de stockage dans Azure. Il ne doit contenir que des lettres en minuscules et des chiffres et comprendre entre 3 et 24 caractères.
	Clé d'accès	Entrez la clé d'accès du compte.  REMARQUE : Vous pouvez entrer la clé primaire ou secondaire. Pour obtenir la clé d'accès depuis votre compte Azure, cochez Clés sous Paramètres.
	Utiliser le protocole https	Sélectionnez cette option pour utiliser le protocole sécurisé https au lieu du protocole http standard.

Type de cloud	Zone de texte	Description
Amazon™ S3	Nom d'affichage	Entrez un nom d'affichage pour ce compte Cloud à afficher sur la Rapid Recovery Core Console, par exemple, Microsoft Azure 1.
	Clé d'accès	Entrez la clé d'accès du compte Cloud Amazon™.
	Clé secrète	Entrez la clé secrète du compte.
OpenStack	Nom d'affichage	Entrez un nom d'affichage pour ce compte Cloud à afficher sur la Rapid Recovery Core Console, par exemple, Amazon 1.
	Région	Entrez la région pour votre compte Cloud.
	Nom d'utilisateur	Entrez le nom d'utilisateur du compte Cloud OpenStack.
	Mot de passe ou clé API	Indiquez si vous souhaitez utiliser un mot de passe ou une clé API, puis entrez votre sélection pour ce compte.
	ID du propriétaire	Entrez l'ID de propriétaire du compte.
	URL d'authentification	Entrez l'URL d'authentification du compte.
Fichiers Rackspace Cloud	Nom d'affichage	Entrez un nom d'affichage pour ce compte Cloud à afficher sur la Rapid Recovery Core Console. (Par exemple, OpenStack 1).
	Région	Utilisez la liste déroulante pour sélectionner une région pour votre compte.
	Nom d'utilisateur	Entrez le nom d'utilisateur du compte Rackspace Cloud.
	Mot de passe ou clé API	Indiquez si vous souhaitez utiliser un mot de passe ou une clé API, puis entrez votre sélection pour ce compte.
	ID du propriétaire	Entrez l'ID de propriétaire du compte.
	URL d'authentification	Entrez l'URL d'authentification du compte.
	Nom d'affichage	Entrez un nom d'affichage pour ce compte Cloud à afficher sur la Rapid Recovery Core Console, par exemple, Rackspace 1.

5 Cliquez sur **Enregistrer**.

La boîte de dialogue se ferme et le compte s'affiche dans la page **Comptes Cloud** de la Core Console.

Modifier un compte Cloud

Si vous devez changer les informations de connexion à votre compte Cloud, par exemple, pour mettre à jour le mot de passe ou modifier le nom d'affichage, utilisez la page Comptes Cloud de la Rapid Recovery Core Console. Pour modifier un compte Cloud, procédez comme suit.

- 1 Sur la barre d'icône de la Rapid Recovery Core Console, cliquez sur l'icône  **Plus**, puis sélectionnez **Comptes Cloud**. La page **Comptes Cloud** s'affiche.
- 2 En regard du compte Cloud à modifier, cliquez sur le menu déroulant et sur **Modifier**. La fenêtre **Modifier le compte** s'ouvre.
- 3 Modifiez les informations, si nécessaire, puis cliquez sur **Enregistrer**.

 **REMARQUE :** Vous ne pouvez pas changer le type de Cloud.

Configurer les paramètres d'un compte cloud

Les paramètres de configuration du Cloud permettent de déterminer le laps de temps entre chaque tentative de connexion de Rapid Recovery au compte Cloud avant expiration du délai. Pour définir les paramètres de connexion du compte Cloud, procédez comme suit.

- 1 Dans la barre d'icônes de la console Core Rapid Recovery, cliquez sur  **Paramètres**.
L'écran Paramètres s'affiche.
- 2 Dans le menu de gauche, cliquez sur **Comptes Cloud**.
- 3 Dans le tableau des comptes Cloud, cliquez sur le menu déroulant en regard du compte Cloud à configurer, puis effectuez l'une des opérations suivantes :
 - Pour modifier les paramètres de connexion du compte Cloud, cliquez sur **Modifier**.
 - 1 Dans la boîte de dialogue Configuration Cloud, effectuez l'une des opérations suivantes :
 - Pour **Expiration du délai d'attente de la requête**, utilisez les flèches vers le haut et vers le bas pour déterminer la durée en minutes et secondes que Rapid Recovery doit consacrer à une tentative de connexion au compte Cloud quand il existe un retard. Les tentatives de connexion s'arrêtent après le délai défini.
 - Pour la **Taille du tampon d'écriture** :, entrez la taille de la mémoire tampon que vous souhaitez réserver à l'écriture des données archivées dans le Cloud.
 - Pour la **Taille du tampon de lecture** :, entrez la taille de bloc que vous souhaitez réserver à la lecture des données archivées à partir du Cloud.
 - 2 Cliquez sur **OK**.
 - Pour rétablir les paramètres par défaut qui suivent la configuration Cloud, cliquez sur **Réinitialiser**.
 - **Délai d'expiration de la demande** : 01:30 (minutes et secondes)
 - **Taille du tampon d'écriture** : 8388608 (octets)
 - **Taille du tampon de lecture** : 8388608 (octets)

Suppression d'un compte Cloud

Si vous arrêtez le service Cloud ou décidez de ne plus l'utiliser pour un Core donné, vous pouvez supprimer le compte Cloud de la Core Console. Pour supprimer un compte Cloud, procédez comme suit.

- 1 Sur la barre d'icône de la Rapid Recovery Core Console, cliquez sur l'icône  **Plus**, puis sélectionnez **Comptes Cloud**.
La page **Comptes Cloud** s'affiche.
- 2 En regard du compte à modifier, cliquez sur le menu déroulant, puis sur **Supprimer**.
- 3 Dans la boîte de dialogue **Supprimer le compte**, cliquez sur **Oui** pour confirmer que vous souhaitez supprimer le compte.
- 4 Si le compte Cloud est en cours d'utilisation, une seconde boîte de dialogue vous invite à confirmer la suppression du compte. Cliquez sur **Oui** pour confirmer.

 **REMARQUE** : la suppression d'un compte en cours d'utilisation fait échouer toutes les tâches planifiées du compte.

Archivage

Cette section présente des cas concrets pour créer une archive et explique comment créer une archive avec Rapid Recovery et où la stocker.

Description des archives

Les stratégies de rétention appliquent les périodes de stockage des sauvegardes sur des supports à court terme (rapide et onéreux). Parfois, certaines obligations techniques ou commerciales imposent de conserver longtemps ces sauvegardes. Cependant, l'utilisation d'un stockage rapide est onéreux. Cette exigence crée donc un besoin de stockage à long terme (lent et financièrement avantageux). Les entreprises utilisent généralement le stockage à long terme pour l'archivage des données qu'impose ou non la réglementation. La fonction d'archivage de Rapid Recovery permet de conserver de manière prolongée les données qu'impose ou non la réglementation. Elle permet également d'implanter les données de réplication sur une réplique du Core distante.

Une fois votre archive créée, vous pouvez :

- la monter en tant que système de fichiers afin de restaurer des fichiers ou des dossiers simples ;
- l'utiliser comme source dans le cadre d'une restauration BMR ;
- l'importer dans une logithèque.

Création d'une archive

Vous pouvez utiliser cette procédure pour créer une archive ponctuelle ou programmée.

Si vous envisagez de créer une archive sur un emplacement Cloud, commencez par ajouter votre compte Cloud à la console Core Rapid Recovery. Pour plus d'informations, voir [Ajouter un compte cloud](#).

Une archive ponctuelle est une archive créée à la demande pour une machine donnée. Une archive programmée est une archive qui se reproduit automatiquement à la date et à l'heure que vous spécifiez dans l'assistant. Programmer une archive périodique vous permet de sauvegarder les archives fréquentes d'une machine sans avoir à créer des archives manuellement à chaque fois.

- 1 Dans la barre de boutons de la console Core Rapid Recovery, cliquez sur  **Archiver**.
L'assistant d'archive s'ouvre.
- 2 Sur la page **Type d'archive** de l'assistant, sélectionnez l'une des options suivantes :
 - Archive ponctuelle
 - Archive continue (par planification)
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Emplacement**, sélectionnez une option dans la liste déroulante **Type d'emplacement**, puis entrez les informations de configuration tel que décrit dans le tableau suivant.

Tableau 38. Options de type d'emplacement d'archive

Option	Zone de texte	Description
Local	Emplacement	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, d:\work\archive.
Réseau	Emplacement	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.

Option	Zone de texte	Description
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud.		
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.
	Nom du dossier	Entrez le nom du dossier d'enregistrement des données archivées.

- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Machines** de l'assistant, sélectionnez la ou les machines protégées contenant les points de restauration à archiver.
- 7 Cliquez sur **Suivant**.
- 8 Effectuez l'une des opérations suivantes :
 - Si vous avez choisi de créer une archive ponctuelle, passez à l'étape 15.
 - Si vous avez choisi de créer une archive programmée, passez à l'étape 9
- 9 Sur la page **Planification**, sélectionnez l'une des options de la liste déroulante **Envoyer les données** :
 - Tous les jours
 - Toutes les semaines
 - Tous les mois
- 10 Entrez les informations décrites dans le tableau suivant en fonction de votre choix lors de l'étape 9.

Tableau 39. Options d'envoi de données

Option	Zone de texte	Description
Tous les jours	À	Sélectionnez l'heure du jour de création d'une archive quotidienne.
Toutes les semaines	Jour de la semaine	Sélectionnez le jour de la semaine de création automatique de l'archive.
	À	Sélectionnez l'heure de création souhaitée pour une archive.
Tous les mois	Jour des mois	Sélectionnez le jour du mois de création automatique de l'archive.
	À	Sélectionnez l'heure de création souhaitée pour une archive.

- 11 Si vous ne voulez pas que la tâche d'archivage commence lors de la prochaine heure de début programmée, une fois que vous avez terminé l'assistant, sélectionnez **Mettre en pause l'archivage initial**.

REMARQUE : Vous pouvez suspendre l'archivage planifié si vous avez besoin de temps pour préparer l'emplacement cible avant la reprise de l'archivage. Si vous ne sélectionnez pas cette option, l'archivage commence à l'heure planifiée.

- 12 Cliquez sur **Suivant**.
- 13 Sur la page **Options** pour une archive continue, sélectionnez une des actions de recyclage décrites dans le tableau suivant.

Tableau 40. Options de recyclage d'une archive continue

Zone de texte	Description
Incrémentielle	Permet d'ajouter des points de restauration à une archive existante. La fonction compare les points de restauration pour éviter de dupliquer les données qui existent déjà dans l'archive.
Remplacer ce Core	Remplace les données archivées existantes du core, mais laisse intactes les données des autres cores.

Zone de texte	Description
Effacer complètement	Efface toutes les données archivées dans le répertoire avant d'écrire une nouvelle archive.
14	Vous pouvez aussi sélectionner Construire des chaînes de points de restauration (réparer les orphelins) si vous le souhaitez et passer à l'étape 18.
15	Dans la page Options pour une archive ponctuelle, saisissez les informations décrites dans le tableau suivant.

Tableau 41. Options d'archivage ponctuel

Zone de texte	Description
Taille maximale	Les archives de données de grande taille peuvent être divisées en plusieurs segments. Sélectionnez l'espace maximal à réserver à la création de l'archive en procédant comme suit : - Sélectionnez Cible entière pour réserver tout l'espace disponible dans le chemin fourni sur la destination définie lors de l'étape 4. (Par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le lecteur D est réservé). - Cliquez sur la zone de texte vierge, utilisez les flèches Haut et Bas pour entrer la quantité, puis choisissez une unité de mesure dans la liste déroulante pour personnaliser l'espace maximal à réserver. REMARQUE : Les archives cloud Amazon™ Amazon sont divisées automatiquement en segments de 50 Go. Les archives cloud Microsoft Azure sont divisées automatiquement en segments de 200 Go.
Action de recyclage	Sélectionnez l'une des options d'action de recyclage suivantes : - Ne pas réutiliser. Ne remplace pas ou n'efface pas les données archivées existantes dans l'emplacement. Si l'emplacement n'est pas vide, Rapid Recovery vous permet de sélectionner un autre emplacement. - Remplacer ce core. Remplace les données archivées existantes du core, mais laisse intactes les données des autres cores. - Effacer complètement. Efface toutes les données archivées dans le répertoire avant d'écrire une nouvelle archive. - Incrémentiel. Permet d'ajouter des points de restauration à une archive existante. La fonction compare les points de restauration pour éviter de dupliquer les données qui existent déjà dans l'archive.
Commentaire	Entrez toute information supplémentaire nécessaire pour l'archive. Le commentaire s'affiche si vous importez l'archive ultérieurement.
Construire des chaînes de points de restauration (réparer les orphelins)	Sélectionnez cette option pour archiver intégralement la chaîne de points de restauration. Cette option est sélectionnée par défaut.

- 16 Cliquez sur **Suivant**.
- 17 Sur la page **Plage de dates**, choisissez manuellement la date de début et la date de fin pour les points de restauration à archiver ou sélectionnez la date et l'heure en cliquant sur l'icône Calendrier, puis sur l'icône Horloge en dessous de la fenêtre du calendrier.
- 18 Cliquez sur **Terminer**.
L'assistant se ferme.

Archivage dans un Cloud

Lorsque les données atteignent la fin d'une période de conservation, vous pouvez étendre la période en créant une archive des anciennes données. Lorsque vous archivez les données, se pose toujours le problème du choix de leur emplacement de stockage. Rapid Recovery vous permet d'envoyer l'archive à divers fournisseurs de Cloud directement depuis la Core Console. Les Clouds compatibles incluent Microsoft Azure, Amazon™, Rackspace et tout fournisseur OpenStack.

L'exportation d'une archive vers un Cloud en utilisant Rapid Recovery implique d'exécuter les procédures suivantes :

- Ajouter votre compte Cloud à la Rapid Recovery Core Console. Pour plus d'informations, voir [Ajouter un compte cloud](#).
- Archiver les données et les exporter vers votre compte Cloud. Pour plus d'informations, voir [Création d'une archive](#).
- Extraire les données archivées en les important depuis l'emplacement du Cloud. Pour en savoir plus, voir [Importer une archive](#).

Modification d'une archive planifiée

Rapid Recovery permet de changer les informations d'une archive planifiée. Pour modifier une archive planifiée, procédez comme suit.

- 1 Dans la console Core Rapid Recovery, cliquez sur le menu déroulant  **Plus** sur la barre d'icônes, puis sélectionnez **Archives**.
- 2 Sur la page Archives, dans Archives planifiées, cliquez sur le menu déroulant en regard de l'archive à changer, puis cliquez sur **Modifier**.
L'assistant d'ajout d'archive s'ouvre.
- 3 Sur la page **Emplacement** de l'assistant d'archivage, sélectionnez l'une des options suivantes dans la liste déroulante **Type d'emplacement** :
 - Local
 - Réseau
 - Cloud
- 4 Entrez les détails de l'archive comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape 3.

Tableau 42. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, d:\work\archive.
Réseau	Emplacement	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
	 REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud.	
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.
	Nom du dossier	Entrez un nom pour le dossier dans lequel vous souhaitez enregistrer les données archivées ; par exemple, Archive Rapid-Recovery - [DATE DE CRÉATION] - [HEURE DE CRÉATION].

- 5 Cliquez sur **Suivant**.
- 6 Dans la page **Machines** de l'Assistant, sélectionnez la ou les machines protégées contenant les points de restauration que vous souhaitez archiver. Effacez les machines que vous ne souhaitez pas archiver.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page **Planification**, sélectionnez une des options dans la liste déroulante **Envoyer des données** :
 - Tous les jours
 - Toutes les semaines
 - Tous les mois

- 9 Entrez les informations décrites dans le tableau suivant en fonction de la sélection dans l'étape 8.

Tableau 43. Options pour l'envoi de données

Option	Zone de texte	Description
Tous les jours	À	Sélectionnez l'heure du jour de création d'une archive quotidienne.
Toutes les semaines	Jour de la semaine	Sélectionnez le jour de la semaine de création automatique de l'archive.
	À	Sélectionnez l'heure du jour de création d'une archive quotidienne.
Tous les mois	Jour des mois	Sélectionnez le jour du mois de création automatique de l'archive.
	À	Sélectionnez l'heure du jour de création d'une archive quotidienne.

- 10 Si vous le désirez, vous pouvez suspendre l'archivage pour le reprendre ultérieurement, sélectionnez **Mettre en pause l'archivage initial**.

REMARQUE : Vous pouvez suspendre l'archivage planifié si vous avez besoin de temps pour préparer l'emplacement cible avant la reprise de l'archivage. Si vous ne sélectionnez pas cette option, l'archivage commence à l'heure planifiée.

- 11 Cliquez sur **Suivant**.
- 12 Sur la page **Options**, utilisez la liste déroulante **Action de recyclage** pour sélectionner l'une des options décrites dans le tableau suivant :

Tableau 44. Options de recyclage d'archive

Zone de texte	Description
Incrémentielle	Permet d'ajouter des points de restauration à une archive existante. La fonction compare les points de restauration pour éviter de dupliquer les données qui existent déjà dans l'archive.
Remplacer ce Core	Remplace les données archivées existantes du core, mais laisse intactes les données des autres cores.
Effacer complètement	Efface toutes les données archivées dans le répertoire avant d'écrire une nouvelle archive.

- 13 Vous pouvez sélectionner, **Construire des chaînes de points de restauration (réparer les orphelins)**.
- 14 Cliquez sur **Terminer**.
Rapid Recovery applique vos modifications à l'archive.

Suspension ou reprise de l'archivage planifié

Si vous avez une tâche d'archivage répétée de programmée , vous pouvez suspendre ou reprendre cette action, si nécessaire.

Il peut arriver que vous vouliez suspendre une tâche d'archivage programmée, par exemple pour modifier l'emplacement de l'archive de destination. En outre, si vous avez suspendu initialement l'archivage lorsque vous avez exécuté la procédure [Création d'une archive](#), vous voudrez sans doute relancer l'archivage programmé plus tard. Pour suspendre ou reprendre un archivage planifié, procédez comme suit.

- 1 À partir de la console Core Rapid Recovery, cliquez sur le menu  **Plus** sur la barre d'icônes, puis cliquez sur **Archives**.
- 2 Dans la page **Archives**, sous les Archives programmées, effectuez l'une des tâches suivantes :
 - Sélectionnez l'archive appropriée, puis dans les actions suivantes, cliquez sur l'action à exécuter :
 - Suspendre
 - Reprendre

- En regard de l'archive appropriée, cliquez sur le menu déroulant, puis dans les actions suivantes, cliquez sur l'action à exécuter :
 - Suspendre
 - Reprendre

L'état de l'archive s'affiche dans la colonne Planification.

Tâche d'archivage forcée

Avec cette procédure, vous pouvez forcer Rapid Recovery à effectuer la tâche d'archivage sur une archive programmée à tout moment.

Pour forcer un travail d'archivage, vous devez disposer d'une archive programmée sur le Core.

- 1 À partir de la console Core Rapid Recovery, dans la barre d'icônes, cliquez sur l'icône  **Plus**, puis sélectionnez **Archives**.
- 2 Sur la page Archives, sous Archives programmées, cliquez sur le menu déroulant à côté de l'archive que vous souhaitez utiliser, puis cliquez sur **Forcer**.

Rapid Recovery archive les points de restauration en fonction des paramètres que vous avez sélectionnés pour cette archive, indépendamment de l'opération d'archivage planifiée l'heure à laquelle vous avez défini.

Vérification d'une archive

La vérification d'archive permet de vérifier si une archive et son contenu peuvent être restaurés.

Vous pouvez analyser l'intégrité de la structure, les segments de données et les fichiers d'index d'une archive en exécutant une vérification d'archive. L'outil contrôle l'intégrité des fichiers et vérifie si l'archive contient bien tous les fichiers nécessaires. Pour vérifier une archive, procédez comme suit.

- 1 Dans la Rapid Recovery Core Console, cliquez sur le menu déroulant  **Plus** dans la barre d'icônes, puis sélectionnez **Archives**.
- 2 Sur la page **Archives**, cliquez sur **Vérifier**.
La boîte de dialogue **Vérifier l'archive** s'affiche.
- 3 Dans **Type d'emplacement**, sélectionnez l'une des options suivantes dans la liste déroulante :
 - Local
 - Réseau
 - Cloud
- 4 En fonction du type d'emplacement choisi à l'étape 3, entrez les détails de l'archive comme indiqué dans le tableau suivant.

Tableau 45. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement	Entrez le chemin de l'archive.
Réseau	Emplacement	Entrez le chemin de l'archive.
	Nom d'utilisateur	Entrez le nom d'utilisateur. Permet de définir les informations d'identification de connexion du partage réseau.
	Mot de passe	Entrez le mot de passe du chemin d'accès réseau. Permet de définir les informations d'identification de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.

Option	Zone de texte	Description
 REMARQUE : pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans la Core Console. Pour en savoir plus, voir Ajouter un compte cloud .		
Conteneur		Sélectionnez un conteneur associé au compte dans le menu déroulant.
Nom du dossier		Sélectionnez le dossier dans lequel les données archivées sont enregistrées ; par exemple, Rapid Recovery -5-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION]

- 5 Sélectionnez ou décochez les options de vérification décrites dans le tableau suivant. Tous les options sont sélectionnées par défaut.

 **REMARQUE :** ne décochez pas l'ensemble des options de vérification. Vous devez sélectionner au moins une option.

Option	Description
Décalages du mappage des fichiers d'indexation	Cette option vérifie que toutes les données de la structure interne de l'archive se trouvent au bon endroit.
Intégrité structurelle	Cette option vérifie la présence de certains fichiers internes et la structure des dossiers de l'archive. Si certains fichiers ou dossiers sont introuvables, la vérification échoue.
Intégrité de somme de contrôle	Cette option vérifie et garantit l'intégrité des segments de données de l'archive.

- 6 Cliquez sur **Vérifier le fichier**.
Rapid Recovery exécute les vérifications sélectionnées sur l'archive.

Attachement d'une archive

Attacher une archive vous permet de voir les points de restauration de l'archive.

Vous devez disposer d'une archive préexistante créée avec Rapid Recovery Core 6.0.1 ou version ultérieure pour terminer cette procédure. Pour plus d'informations, voir [Création d'une archive](#).

Lorsque vous attachez une archive, le nom de l'archive que vous fournissez apparaît comme un menu d'archive dans le menu de navigation de gauche de la console Core. Toutes les machines protégées avec les points de restauration de l'archive sont répertoriées séparément en dessous du menu Archives. Vous pouvez cliquer sur n'importe quel nom de machine dans l'archive et parcourir ses points de restauration. Vous pouvez ensuite effectuer les mêmes actions comme avec n'importe quel autre point de restauration actuellement visible dans votre Core.

Attacher une archive permet également de mettre en cache les informations d'identification pour accéder à l'information. Tant que vous ne supprimez pas la définition de l'archive attachée, vous pouvez facilement réattacher et détacher l'archive, ce qui rend ses points de restauration faciles d'accès.

Utilisez cette procédure pour attacher une archive.

- Sur la console Core Rapid Recovery, cliquez sur le menu déroulant  **Archive** puis sélectionnez  **Attacher archive**.
La boîte de dialogue **Attacher une archive** apparaît.
- Dans la zone de texte **Nom**, entrez un nom pour cette archive attachée.
La valeur que vous entrez dans ce champ apparaît dans le menu de navigation de gauche en tant que nom du menu de l'archive.

Selon les meilleures pratiques d'affichage des noms, le nom de l'archive doit contenir entre 1 et 64 caractères alphanumériques, y compris des espaces. N'utilisez pas les [caractères interdits](#). Ou les [expressions interdites](#).
- Dans la liste déroulante de **Type d'emplacement**, sélectionnez le type d'emplacement de votre archive à partir des options suivantes :
 - Local
 - Réseau
 - Cloud

- 4 Entrez les détails de l'archive comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape 3.

Tableau 46. Détails de type d'emplacement

Option	Zone de texte	Description
Local	Emplacement	Entrez le chemin d'accès à l'archive ; par exemple, D:\work\archive.
Réseau	Emplacement	Entrez le chemin d'accès à l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez le nom d'utilisateur pour la connexion au partage réseau.
	Mot de passe	Entrez le mot de passe pour la connexion au partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
		REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud .
	Conteneur	Sélectionnez le conteneur de l'archive associé au compte dans le menu déroulant.
	Nom du dossier	Entrez le nom du dossier des données archivées ; par exemple, Archive-Rapid-Recovery-[DATE DE CRÉATION]-[HEURE DE CRÉATION].

- 5 Cliquez sur **Attach (Connecter)**.

L'archive s'attache à ce Core et monte le contenu comme un système de fichiers.

Importer une archive

Cette procédure permet d'importer ponctuellement une archive ou de planifier son importation de façon récurrente.

Lorsque vous souhaitez récupérer des données archivées, vous pouvez importer la totalité de l'archive vers l'emplacement que vous spécifiez.

PRÉCAUTION : N'exécutez cette étape qu'après avoir pris le temps de la réflexion. L'importation d'une archive modifie le contenu du référentiel, en remplaçant dans celui-ci les données nouvelles depuis la capture de l'archive.

Pour importer une archive, procédez comme suit.

- 1 Dans la barre de menu de la console Core Rapid Recovery, cliquez sur  le menu déroulant **Archive**, puis sélectionnez **Importer une archive**.
L'**Assistant d'importation d'archive** s'ouvre.
- 2 Dans la page **Type d'importation** de l'assistant, sélectionnez l'une des options suivantes :
 - Importation ponctuelle
 - Importation en continu (par planification)
- 3 Cliquez sur **Suivant**.
- 4 Dans la page **Emplacement**, sélectionnez dans la liste déroulante l'emplacement de l'archive , puis entrez les informations décrites dans le tableau suivant :

Tableau 47. Options de type importé d'emplacement de l'archive importée

Option	Zone de texte	Description
Local	Emplacement	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où l'archive doit résider. Par exemple, d:\travail\archive.
Réseau	Emplacement	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où l'archive doit résider. Par exemple, \\nom-serveur\nom-partage.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Il est utilisé pour établir les références de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe pour le partage réseau. Il est utilisé pour établir les références de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
	REMARQUE : Pour sélectionner un compte cloud, vous devez l'avoir ajouté dans la console Core. Pour plus d'informations, reportez-vous à Ajouter un compte cloud.	
	Conteneur	Sélectionnez un conteneur associé à votre compte dans le menu déroulant.
	Nom de dossier	Entrez le nom du dossier dans lequel vous souhaitez enregistrer les données archivées.

- 5 Cliquez sur **Suivant**.
- 6 Dans la page **Informations sur l'archive** de l'assistant, si vous souhaitez importer chacune des machines incluses dans l'archive, sélectionnez **Importer toutes les machines**.
- 7 Effectuez l'une des options suivantes en fonction de votre sélection :
 - Si vous avez sélectionné **Importation ponctuelle** en 2, si vous avez choisi **Importer toutes les machines** en 6, et que toutes les machines sont présentes sur le core en tant que machines protégées, répliquées ou points de récupération uniquement, passez à l'étape 12.
 - Si vous avez sélectionné **Importation en continu (par planification)** en 2, si vous avez choisi **Importer toutes les machines** en 6, et qu'au moins une machine n'est pas présente sur le core en tant que machine protégée, répliquée ou point de récupération uniquement, cliquez sur **Suivant**, puis passez à l'étape 9.
 - Si vous n'avez pas importé toutes les machines en 6, cliquez sur **Suivant**, puis passez à l'étape 8.
- 8 Dans la page **Machines**, sélectionnez les machines que vous voulez importer depuis l'archive.
 - Si vous avez sélectionné **Importation ponctuelle** en 2 et qu'au moins une machine n'est pas présente sur le core en tant que machine protégée, répliquée ou point de récupération uniquement, sélectionnez dans la liste déroulante un référentiel pour chacune des machines à importer, puis passez à l'étape 12.
 - Si toutes les machines sont déjà présentes sur le core en tant que machines protégées, répliquées ou points de récupération uniquement, passez à l'étape 12.
- 9 Cliquez sur **Suivant**.
- 10 Dans la page **Référentiel**, effectuez l'une des options suivantes :
 - Si un référentiel est associé avec le core, sélectionnez l'une des options dans le tableau suivant.

Tableau 48. Options de référentiel :

Option	Description
Utiliser un référentiel existant	Sélectionnez dans la liste déroulante un référentiel actuellement associée à ce core.
Créer un référentiel	Dans la zone de texte Serveur, entrez le nom du serveur sur lequel vous souhaitez enregistrer le nouveau référentiel : par exemple, nom_serveur ou localhost, puis reportez-vous à Créer un référentiel DVM .
•	Si aucun référentiel n'est associé au core, entrez le nom du serveur sur lequel vous souhaitez enregistrer le nouveau référentiel : par exemple, nom_serveur ou localhost, puis reportez-vous à Créer un référentiel DVM .

- 11 Si vous avez choisi **Importation en continu (par planification)** en 2, dans la page **Planification**, sélectionnez les options décrites dans le tableau suivant.

Tableau 49. Options de planification d'importation

Option	Description
Tous les jours	Cliquez sur l'icône d'horloge et utilisez les flèches vers le haut et vers le bas pour sélectionner l'heure à laquelle vous souhaitez que commence le travail d'archivage. Si vous utilisez un système 12 heures, cliquez sur le bouton AM ou PM pour spécifier l'heure du jour.
Toutes les semaines	Sélectionnez le jour de la semaine, puis l'heure à laquelle vous souhaitez que commence le travail d'archivage. Si vous utilisez un système 12 heures, cliquez sur le bouton AM ou PM pour spécifier l'heure du jour.
Tous les mois	Sélectionnez le jour du mois et l'heure à laquelle vous souhaitez que commence le travail d'archivage. Si vous utilisez un système 12 heures, cliquez sur le bouton AM ou PM pour spécifier l'heure du jour.
Suspendre l'importation initiale	Sélectionnez cette option si vous ne souhaitez pas que le travail d'importation commence à la prochaine heure de début planifiée une fois que vous en aurez terminé avec l'assistant.

REMARQUE : Il se peut que vous souhaitiez suspendre l'importation planifiée si vous avez besoin de temps pour préparer l'emplacement cible avant que l'importation ne reprenne. Si vous ne sélectionnez pas cette option, l'importation commencera à l'heure planifiée.

- 12 Cliquez sur **Terminer**.

Événements

Le Rapid Recovery Core inclut des ensembles prédéfinis d'événements. Ces événements peuvent être utilisés pour notifier les administrateurs de problèmes critiques sur le Core ou avec les tâches relatives aux sauvegardes, exportations virtuelles, répliquions et ainsi de suite.

Cette section explique comment afficher les événements affichés dans la Rapid Recovery Core Console. Vous pouvez également obtenir davantage de connaissances sur les méthodes de notifications d'événements et leur configuration (notamment la configuration des notifications par e-mail). Enfin, vous pouvez configurer des notifications de façon à modifier la période de conservation des journaux des événements et réduire les notifications en cas d'événements répétitifs.

Événements de la Rapid Recovery

Le Noyau de la Rapid Recovery inclut des ensembles prédéfinis d'événements, pouvant servir à avertir les administrateurs des problèmes critiques dont peut souffrir le Noyau ou être utilisés avec des opérations de sauvegarde sur les machines protégées.

- Vous définissez quels types d'événements déclenchent les alertes, ainsi que les méthodes utilisées par le système pour vous en avertir (courriers électroniques, alertes de toast, etc.), lors de la configuration des notifications de groupe. Pour plus d'informations, veuillez consulter [Configurer les groupes de notification](#).
- Si vous souhaitez que les administrateurs reçoivent des notifications par courrier électronique, alors, en plus de la configuration d'un groupe de notifications, vous devez configurer un serveur de messagerie et définir un modèle de notification par courrier électronique. Pour plus d'informations, veuillez consulter [Configurer un serveur de messagerie électronique](#) et [Configurer un modèle de notification par e-mail](#), respectivement.
- Vous pouvez réduire le nombre d'événements de même type et de même portée apparaissant dans la page Événements en utilisant la fonction de réduction des répétitions. Cette fonction est activée par défaut. Vous pouvez la désactiver, ou définir la durée pendant laquelle les événements seront fusionnés en une seule occurrence dans le journal d'événements. Pour plus d'informations, veuillez consulter [À propos de la configuration de la réduction des répétitions](#).
- Vous pouvez définir la durée pendant laquelle l'historique des événements et des opérations sera conservé dans la page Événements de la console du Noyau. Pour plus d'informations, veuillez consulter [Configurer la rétention des événements](#).

Affichage des événements à l'aide des tâches, des alertes et du journal

Dans la console Core, vous pouvez afficher les événements pour le Core, ainsi que les événements pour une machine protégée ou répliquée spécifique.

La page **Événements** de la console Core affiche le journal de tous les événements système concernant le Core de Rapid Recovery. Pour

accéder et afficher les événements pour le Core, cliquez sur  (Événements).

La page **Événements** d'une machine protégée ou répliquée spécifique affiche le journal des événements associés à cette machine. Pour accéder et afficher les événements pour une machine sélectionnée, cliquez sur le nom de la machine dans le menu Machines protégées, puis sur la page **Résumé** de la machine, cliquez sur le menu **Événements**.

Le contenu de la page Événements (sur le Core ou une machine spécifique) est divisé en trois sections : Tâches, Alertes et Journal. Ces vues vous permettent de filtrer les détails sur les différents événements, selon vos besoins.

Vous pouvez définir la façon dont vous allez être notifié des différents événements en configurant des groupes de notifications. Pour plus d'informations, voir [Configurer les groupes de notification](#).

Suivez les étapes décrites dans les procédures ci-dessous pour afficher les tâches, les alertes ou le journal de tous les événements :

- [Affichage des tâches](#)
- [Afficher les alertes](#)
- [Afficher tous les événements](#)

Affichage des tâches

Une tâche est un travail que le Core Rapid Recovery doit effectuer, par exemple le transfert de données lors d'une sauvegarde programmée de manière régulière, ou une restauration à partir d'un point de restauration.

Lorsqu'une tâche est en cours d'exécution, elle apparaît dans le menu déroulant **Tâches en cours d'exécution** dans la partie supérieure de la console Core. Lorsque vous cliquez sur une tâche en cours d'exécution, la boîte de dialogue Surveiller la tâche active s'ouvre.

Vous pouvez également afficher toutes les tâches du Core Rapid Recovery, ou toutes les tâches associées à une machine spécifique.

- 1 Pour afficher toutes les tâches du Core Rapid Recovery, dans la barre d'icônes, cliquez sur  (Événements).
Pour afficher les tâches d'une machine protégée en particulier, accédez à la page **Synthèse** de la machine en question, puis cliquez sur le menu **Événements**.
- 2 Pour afficher uniquement les tâches, cliquez sur **Tâches** dans la partie supérieure gauche de la page. Il s'agit de la vue par défaut.
La liste des tâches est filtrée de manière à n'afficher que les tâches du Core ou de la machine que vous avez sélectionnées.
- 3 De manière optionnelle, pour filtrer l'analyse des tâches par mot-clé, par date de début, par date de fin, ou en utilisant n'importe quelle combinaison de ces éléments, procédez comme suit :
 - a Pour filtrer par mot-clé, saisissez le mot-clé dans la boîte de texte **Rechercher par mot-clé**.
Par exemple, vous pouvez filtrer à l'aide des mots-clés suivants : « consolidation », « archivage » ou « transfert ».
 - b Pour filtrer par date et heure de début, saisissez la date et l'heure de début en utilisant l'une des options suivantes :
 - Dans la boîte de texte **De**, saisissez la date et l'heure au format MM/JJ/AAAA HH:MM. Par exemple, pour lancer une recherche à partir du 1er janvier 2016 à 08 h 00, saisissez 01/01/2016 8:00.

- Pour sélectionner la date et l'heure actuelles, cliquez sur le widget  **Calendrier** dans la boîte de texte **De**, puis cliquez sur la date actuelle. L'heure actuelle s'affiche automatiquement.
- Cliquez sur le widget  **Calendrier**, sélectionnez la date, puis cliquez sur le widget  Horloge et sélectionnez l'heure de votre choix à l'aide des commandes. Cliquez en dehors du calendrier pour accepter les modifications sélectionnées.
- c Pour affiner la liste des tâches qui s'affichent, vous pouvez également définir une heure et une date de fin de même format. La liste des tâches est filtrée immédiatement selon les critères que vous avez sélectionnés.

4 De manière optionnelle, vous pouvez filtrer les tâches qui apparaissent dans la liste de la manière suivante :

Option	Description
	Pour afficher uniquement les tâches actives, cliquez sur l'icône Tâches actives .
	Pour afficher uniquement les tâches placées dans la file d'attente, cliquez sur l'icône Tâches en file d'attente .
	Pour afficher uniquement les tâches en attente d'exécution, cliquez sur l'icône Tâches en attente .
	Pour afficher uniquement les tâches terminées, cliquez sur l'icône Tâches terminées .
	Pour afficher uniquement les tâches qui ont échoué, cliquez sur l'icône Tâches ayant échoué .

5 Pour exporter la liste des tâches, sélectionnez un format dans la liste, puis cliquez sur  **Exporter**. Dans la boîte de dialogue qui s'affiche, confirmez l'exportation, puis cliquez sur **OK**.

Vous pouvez exporter en utilisant les formats suivants :

Tableau 50. Formats d'exportation

Format	Description
PDF	Portable Document Format (format d'exportation par défaut)
HTML	Format de page Web
CSV	Valeurs séparées par des virgules
XLS	Classeur Microsoft Excel® 1997 - 2003
XLSX	Classeur Excel

Le type de fichier sélectionné est téléchargé vers l'emplacement par défaut indiqué sur le serveur Core.

- 6 Cliquez sur l'icône  **Détails de la tâche** d'une tâche pour ouvrir une nouvelle fenêtre affichant les détails de la tâche, notamment :
- État
 - Travail total (taille ou pourcentage effectué)
 - Date et heure de début
 - Date et heure de fin
 - Vitesse
 - Temps écoulé
 - Phase (pour les tâches enfants)

Afficher les alertes

Une alerte est une notification concernant une tâche ou un événement. Les types d'alertes incluent les erreurs, les avertissements et les informations.

Vous pouvez afficher toutes les alertes du Core Rapid Recovery, ou les alertes importantes associées à une machine.

- 1 Pour afficher les alertes pour le Core Rapid Recovery, depuis la barre d'icônes, cliquez sur  (Événements), puis cliquez sur **Alertes**.
Si vous souhaitez afficher les alertes spécifiques pour une machine protégée, accédez à la page **Synthèse** de cette machine, cliquez sur le menu **Événements**, puis cliquez sur **Alertes**.

La liste des événements est filtrée de manière à n'afficher que les alertes importantes du Core ou de la machine que vous avez sélectionné(e).
- 2 Si vous le souhaitez, pour filtrer la liste des alertes importantes par date de début, la date de fin description du message d'alerte, ou toute combinaison, effectuez les opérations suivantes :
 - a Pour filtrer par date et heure de début, saisissez la date et l'heure de début en utilisant l'une des options suivantes :
 - Dans la boîte de texte **De**, saisissez la date et l'heure au format MM/JJ/AAAA HH:MM. Par exemple, pour rechercher à partir du premier jour de janvier 2016 à 08 h 00, entrez 1/1/2016 8:00 AM.
 - Pour sélectionner les données et l'heure actuelle, cliquez sur le widget  **Calendrier** dans la boîte de texte **De**, puis cliquez sur la date actuelle. L'heure actuelle s'affichera automatiquement.
 - Cliquez sur la flèche  **Calendrier**, sélectionnez la date, puis cliquez sur le widget  Horloge et sélectionnez l'heure de votre choix à l'aide des commandes. Cliquez en dehors du calendrier pour accepter les modifications sélectionnées.
 - b Pour filtrer par description de message d'alerte, saisissez la description dans la zone de texte **Message de recherche**.
Par exemple, pour voir uniquement les alertes concernant les agents, entrez « agent; ». Pour voir les alertes relatives aux transferts, entrez « transfert; » et ainsi de suite.
 - c Pour affiner la liste des alertes qui s'affichent, vous pouvez également définir une heure et une date de fin de même format.
La liste des alertes est filtrée immédiatement selon les critères que vous avez sélectionnés.
- 3 Si vous souhaitez supprimer toutes les alertes de la page, cliquez sur **Supprimer tout**.

Afficher tous les événements

Vous pouvez afficher tous les événements du Core Rapid Recovery, ou tous les événements d'une machine.

- 1 Pour afficher un journal de tous les événements du Core Rapid Recovery, depuis la barre d'icônes, cliquez sur  (Événements), puis cliquez sur **Journal**. Pour afficher tous les événements du Core Rapid Recovery, naviguez jusqu'à la page d'accueil du Core Rapid Recovery, puis cliquez sur  (Événements).
Si vous souhaitez afficher un journal de tous les événements spécifiques pour une machine protégée, accédez à la page **Synthèse** de la machine, cliquez sur le menu **Événements**, puis cliquez sur **Journal**.
- 2 Si vous le souhaitez, pour filtrer la liste de tous les événements selon la date de début, la date de fin, la description du message d'alerte, ou toute combinaison, effectuez les opérations suivantes :
 - a Pour filtrer par date et heure de début, saisissez la date et l'heure de début en utilisant l'une des options suivantes :
 - Dans la boîte de texte **De**, saisissez la date et l'heure au format MM/JJ/AAAA HH:MM. Par exemple, pour rechercher à partir du premier jour de janvier 2016 à 08 h 00, entrez 1/1/2016 8:00 AM.
 - Pour sélectionner les données et l'heure actuelles, cliquez sur le widget  **Calendrier** dans la boîte de texte **De**, puis cliquez sur la date actuelle. L'heure actuelle s'affichera automatiquement.
 - Cliquez sur le widget  **Calendrier**, sélectionnez la date, puis cliquez sur le widget  Horloge et sélectionnez l'heure de votre choix à l'aide des commandes. Cliquez en dehors du calendrier pour accepter les modifications sélectionnées.
 - b Pour filtrer par description de message d'alerte, saisissez la description dans la zone de texte **Message de recherche**.
Par exemple, pour voir uniquement les alertes concernant les agents, entrez « agent; ». Pour voir les alertes relatives aux transferts, entrez « transfert; » et ainsi de suite.

- c Pour affiner la liste des événements qui s'affiche, vous pouvez également définir une heure et une date de fin selon le même format.
- La liste des événements est immédiatement filtrée selon les critères que vous avez sélectionnés.

Comprendre les notifications par courrier électronique

Vous pouvez configurer le Noyau de la Rapid Recovery pour qu'il vous avertisse par courrier électronique des événements spécifiques survenant dans le système. Ce courrier électronique est envoyé à une adresse que vous aurez préalablement spécifiée. Les événements déclenchant une alerte sont définis dans le groupe de notifications, de même que les autres méthodes de notification.

REMARQUE : les groupes de notifications doivent être établis, même si vous n'utilisez pas la méthode de notification par courrier électronique. Pour plus d'informations, veuillez consulter [Configurer les groupes de notification](#).

Si vous choisissez le courrier électronique comme une des options de notification, vous devrez également configurer un serveur de messagerie SMTP. Le Noyau de la Rapid Recovery utilise le serveur que vous avez défini pour envoyer des alertes en fonction des paramètres du groupe de notifications.

En outre, vous devez également définir un modèle de notification par courrier électronique. Le Noyau utilise ce modèle pour définir l'objet et le corps du courrier électronique pour chaque alerte. Le modèle dispose de paramètres par défaut ; vous pouvez utiliser ces paramètres tels quels ou vous pouvez procéder à quelques essais et apporter des modifications en fonction de vos besoins.

Cette section aborde les sujets suivants :

- [Configurer un serveur de messagerie électronique](#)
- [Configurer un modèle de notification par e-mail](#)

Configurer un serveur de messagerie électronique

Suivez cette procédure pour configurer un serveur de messagerie électronique.

REMARQUE : Vous devez également configurer les paramètres du groupe de notification, notamment l'activation de l'option **Notifier par e-mail** pour que des alertes par courrier électronique puissent être envoyées par le système. Pour plus d'informations sur la façon de spécifier des événements pour pouvoir recevoir des alertes par e-mail, voir [Configurer les groupes de notification](#).

1 Accédez à la console Core Rapid Recovery.

- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
- Dans la liste des paramètres du Core sur le côté gauche de la page Paramètres, cliquez sur **Serveur SMTP**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à voir l'en-tête **Serveur SMTP**.

Les paramètres Core du serveur SMTP s'affichent.

3 Cliquez sur les paramètres que vous souhaitez modifier.

L'option sélectionnée devient modifiable.

4 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Option	Description
Serveur SMTP	Entrez le nom du serveur de messagerie que doit utiliser le modèle de notification par courrier électronique. La convention de dénomination comprend le nom d'hôte, le domaine et le suffixe ; par exemple, smtp.gmail.com.
From	Entrez une adresse e-mail d'expéditeur. Sert à indiquer l'adresse e-mail de l'expéditeur du modèle de notification par courrier électronique, par exemple, noreply@localhost.com.
Nom d'utilisateur	Entrez un nom d'utilisateur pour le serveur de messagerie.
Mot de passe	Entrez le mot de passe du nom d'utilisateur nécessaire pour accéder au serveur de messagerie électronique.
Port	Entrez un numéro de port. Sert à identifier le port du serveur de messagerie ; par exemple, le port 587 pour Gmail.

Option	Description
	La valeur par défaut est 25.
Délai d'attente (secondes)	Entrez un nombre entier pour spécifier la durée pendant laquelle le système va tenter de se connecter au serveur de messagerie électronique. Cette valeur est utilisée pour définir le délai en secondes de la tentative de connexion. La valeur par défaut est 60 secondes.
TLS	Sélectionnez cette option si le serveur de messagerie utilise une connexion sécurisée comme Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

- 5 Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur la  pour enregistrer les modifications et quitter le mode écriture, ou cliquez sur  pour quitter le mode édition sans enregistrer.

 **PRÉCAUTION :** Si vous ne confirmez pas chaque modification, vos paramètres ne changeront pas.

- 6 Cliquez sur **Envoyer l'e-mail test**, puis procédez comme suit :
- Dans la boîte de dialogue **Envoyer l'e-mail de test**, entrez l'adresse e-mail du destinataire du courrier électronique et cliquez sur **Envoyer**.
 - Si l'e-mail de test échoue, fermez les boîtes de dialogue d'erreur et **Envoyer l'e-mail de test**, puis vérifiez les paramètres de configuration du serveur de messagerie. Renvoyez ensuite le message de test.
 - Lorsque le test de courrier électronique aboutit, cliquez sur **OK** pour confirmer la réussite de l'opération.
 - Vérifiez le compte de messagerie vers lequel vous avez envoyé le test.

Configurer un modèle de notification par e-mail

Lorsque vous activez les notifications par e-mail des événements Rapid Recovery, un modèle par défaut est créé pour vous. Le serveur de messagerie SMTP défini pour le core utilise ce modèle pour envoyer par e-mail des notifications concernant les événements Rapid Recovery.

Cette rubrique explique comment configurer le modèle de notification par e-mail ou comment personnaliser son contenu. L'option Restaurer les paramètres par défaut vous permet de revenir à tout moment au modèle de notification par défaut.

 **PRÉCAUTION :** Vous pouvez modifier le modèle à vos propres risques. Il vous incombe de tester les modifications que vous lui apportez. Aucun support ne vous sera apporté pour un modèle personnalisé.

Pour configurer un modèle de notification par e-mail, procédez comme indiqué ci-après.

 **REMARQUE :** Vous devez également configurer un serveur de messagerie et des paramètres de groupes de notifications, notamment en activant l'option Notifier par e-mail, afin de pouvoir envoyer des messages d'alerte par e-mail. Pour plus d'informations sur la configuration d'un serveur de messagerie pour l'envoi d'alertes, voir [Configurer un serveur de messagerie électronique](#). Pour en savoir plus sur la spécification des événements pour lesquels recevoir des alertes, voir [Configurer les groupes de notification](#).

- Naviguez jusqu'à la console Core Rapid Recovery.
- Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez  **Notifications**.
La page **Notifications** s'affiche.
- Dans le volet Paramètres de messagerie, cliquez sur  **Modifier**.
La boîte de dialogue **Modifier la configuration des notifications par e-mail** apparaît.
- Sélectionnez **Activer l'envoi de notifications par e-mail**.
Le modèle d'e-mail est activé et visible. Les valeurs par défaut du modèle d'e-mail sont décrites dans l'étape suivante.
- Examinez le contenu de la boîte de dialogue Modifier la configuration des notifications par e-mail pour voir si le contenu par défaut correspond bien à vos besoins.

Option	Description
Activer les notifications par e-mail	Ce paramètre permet d'activer ou de désactiver le modèle de notification par e-mail. - Pour activer la notification par e-mail, sélectionnez cette option. - Pour désactiver la notification par e-mail, désélectionnez cette option.
Objet de l'e-mail	Le contenu de ce champ de texte contrôle la ligne d'objet des e-mails envoyés en tant que notifications d'événements système. La valeur par défaut est la suivante : <pre><hostName> <level>: <name> for <agentName></pre>
Email (E-mail)	Le contenu de ce champ de texte contrôle le texte des e-mails envoyés en tant que notifications d'événements système. La valeur par défaut est la suivante : <pre><shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>" Date/Time: <localTimestamp> <message> <if(details.errorDetails)> <details.ErrorDetails.Message> <details.ErrorDetails.Details> <endif> ---</pre> About this event: <description> <coreAdminUrl>
Envoyer un e-mail de test	Cliquer sur ce bouton envoie un e-mail de test à l'adresse indiquée par vous dans la boîte de dialogue Envoyer un e-mail de test qui s'affiche.
Restaurer les paramètres par défaut	Cliquer sur ce bouton supprime toute les modifications personnalisées du modèle par e-mail et restaure les champs Objet et E-mail par défaut décrits dans ce tableau.
OK	Cliquer sur ce bouton confirme et enregistre les paramètres dans la boîte de dialogue Modifier la configuration des notifications par e-mail.
Annuler	Cliquer sur ce bouton annule les modifications effectuées dans la boîte de dialogue Modifier la configuration des notifications par e-mail.

- 6 Si vous souhaitez personnaliser le modèle d'e-mail, apportez des modifications dans le texte ou dans les variables décrites à l'étape précédente. Les variables utilisées dans le modèle par défaut sont décrites dans le tableau suivant.

Option	Description
hostName	Le nom d'hôte du core.
details	Les détails de l'événement spécifique.
agentName	Le nom de la machine protégée associée à cet événement, si l'événement ne s'applique qu'à une seule machine protégée.
repositoryName	Le nom du référentiel associé à cet événement, si l'événement s'applique à un référentiel.
jobSummary	Le résumé du travail associé à cet événement, si l'événement s'applique à un travail.
remoteSlaveCoreName	Le nom du core cible distant associé à cet événement, si l'événement s'applique à un core cible.
remoteMasterCoreName	Le nom du core source distant associé à cet événement, si l'événement s'applique à un core source.
productName	Le nom du produit, Rapid Recovery Core. Ce nom de produit peut être modifié pour un marquage de labellisation.
companyName	Le nom de l'entreprise qui vend le produit.

- 7 Dans la zone de texte **Objet de l'e-mail**, entrez l'objet du modèle d'e-mail.
L'objet de l'e-mail sert à définir le sujet du modèle de notification par e-mail, par exemple, <hostname> – <level> <name>.
- 8 Dans la zone de texte **E-mail**, entrez le texte décrivant l'événement, le moment où il s'est produit et sa gravité.
- 9 Cliquez sur **Envoyer un e-mail de test**, puis effectuez l'une des actions suivantes :

- a Dans la boîte de dialogue Envoyer un e-mail de test, entrez l'adresse de destination du message de test, puis cliquez sur **Envoyer**.
- b Si le test échoue, quittez la boîte de dialogue d'erreur et la boîte de dialogue Envoyer un e-mail de test, cliquez sur **OK** pour enregistrer les paramètres actuels du modèle d'e-mail. Ensuite, modifiez vos paramètres de serveur de messagerie comme indiqué dans la procédure [Configurer un serveur de messagerie électronique](#). Entrez à nouveau le mot de passe de ce compte de messagerie. Enregistrez ces paramètres, puis revenez à cette procédure.
- c Une fois que l'envoi du message de test a réussi, cliquez sur **OK** pour confirmer la réussite de l'opération.
- d Consultez le compte de messagerie auquel vous avez envoyé l'e-mail de test.

Une fois que vous êtes satisfait des résultats de vos tests, revenez à la boîte de dialogue Modifier la configuration des notifications par e-mail et cliquez sur **OK** pour refermer la boîte de dialogue et enregistrer vos paramètres.

Modèles de notifications, paramètres SMTP et groupes de notifications pour les événements système

Les groupes de notifications vous permettent de définir des alertes lorsque des événements spécifiques surviennent, ainsi que la manière dont ces alertes sont notifiées. Pour configurer ou modifier des groupes de notifications, veuillez consulter [Configurer les groupes de notification](#).

Vous devez aussi configurer les paramètres du serveur SMTP (Simple Mail Transfer Protocol) si vous souhaitez envoyer des alertes sous forme de courrier électronique. Pour plus d'informations sur la configuration des paramètres d'un serveur de messagerie, veuillez consulter [Configurer un serveur de messagerie électronique](#).

La notification d'événements prend la forme d'un courrier électronique envoyé par le système. Vous pouvez personnaliser ce modèle. Pour plus d'informations sur la configuration ou la personnalisation du modèle de notification par courrier électronique, veuillez consulter [Configurer un modèle de notification par e-mail](#).

Configurer les groupes de notification

❶ REMARQUE : Vous devez également définir les paramètres du serveur SMTP (Simple Mail Transfer Protocol) si vous voulez envoyer les alertes par courrier électronique, tel que décrit dans la procédure suivante. Pour plus d'informations sur la définition des paramètres de configuration du serveur de messagerie, voir [Configurer un serveur de messagerie électronique](#).

Les groupes de notification vous permettent de définir des ensembles d'événements spécifiques pour lesquels les utilisateurs sont avertis, ainsi que la manière dont cette notification va avoir lieu. Vous pouvez configurer l'envoi d'alertes selon les méthodes suivantes :

- Par e-mail
- Dans le journal des événements Windows
- Avec syslogd
- Avec des alertes toast
- Avec des alertes
- Avec les notifications trap NSMP

Vous pouvez configurer plus d'un groupe de notification avec différents paramètres de notification.

Les groupes de notification peuvent être configurés au niveau du Core ou au niveau de chacune des machines protégées.

Suivez cette procédure pour configurer les groupes de notification des alertes.

1 Effectuez l'une des opérations suivantes :

- Pour configurer des notifications au niveau du Core, à partir de la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Notifications**.

La page **Notifications** apparaît.

- Pour configurer des notifications pour une machine protégée spécifique, effectuez les opérations suivantes :
 - 1 À partir du menu Machines protégées, cliquez sur la machine pour laquelle vous souhaitez spécifier les notifications. L'écran **Personnaliser des groupes de notification** apparaît.
 - 2 Dans la page Synthèse de la machine protégée, à partir du menu déroulant Plus, sélectionnez **Notifications**.

L'écran **Personnaliser des groupes de notification** apparaît.

- 2 Cliquez sur  **Ajouter un groupe**

La boîte de dialogue **Ajouter un groupe de notification** apparaît.

Les groupes de notification vous permettent de définir des ensembles d'événements spécifiques pour lesquels les utilisateurs sont avertis, ainsi que la manière dont cette notification va avoir lieu. Vous pouvez configurer l'envoi d'alertes selon les méthodes suivantes :

La boîte de dialogue **Ajouter un groupe de notifications** contient une zone de description générale et deux onglets :

- Activer les alertes
- Options de notification

- 3 Dans la zone de description, entrez les informations de base du groupe de notification, tel que décrit dans le tableau suivant.

Option	Description

Nom	Entrez un nom pour le groupe de notification d'événements. Cette information est obligatoire.

 **PRÉCAUTION : La valeur que vous saisissez pour le nom du groupe de notification ne peut pas être modifiée par la suite.**

Description Entrez une description qui clarifie la finalité d'un groupe de notification d'événements. Cette information est facultative.

- 4 Sur l'onglet **Activer les alertes**, définissez l'ensemble d'événements système à suivre, pour lesquels vous souhaitez créer des rapports et être alerté comme suit :

Option	Description

Toutes les alertes	Pour créer des alertes pour tous les événements, sélectionnez Toutes les alertes .

Erreurs	Pour créer des alertes pour des erreurs, à partir du menu Sélectionner les types , cliquez sur Erreur . Représenté par un X rouge. 

Avertissement	Pour créer des alertes pour les erreurs, à partir du menu Sélectionner les types , cliquez sur Avertissement . Représenté par une icône de point d'exclamation jaune. 

Infos	Pour créer des alertes pour les messages d'information, à partir du menu Sélectionner les types , cliquez sur Informations . Représenté par un i bleu. 

Restaurer les valeurs par défaut	Pour restaurer les types d'alerte par défaut, à partir du menu Sélectionner les types , cliquez sur Restaurer les valeurs par défaut . Représenté par une flèche bleu foncé orientée vers la gauche. 

- 5 Pour créer des alertes pour un type d'événement spécifique (erreur, avertissement ou message d'information), effectuez les tâches suivantes :
- a Si l'option **Toutes les alertes** n'affiche pas de groupes d'alertes, cliquez sur le signe supérieur > précédant l'étiquette Toutes les alertes. Le symbole devient une flèche orientée vers le bas, et l'affichage s'agrandit pour faire apparaître les groupes.
 - b Cliquez ensuite sur le signe supérieur > en regard de n'importe quel groupe de notification pour afficher les événements liés à ce groupe.
Les catégories des groupes d'événements sont les suivantes :

- Archivage
- Rapport auto
- Capacité d'attachement
- Mise à jour auto
- Logithèque de sauvegarde

- CD d'amorçage
 - Clouds
 - Clusters
 - Service core
 - Rétention de la base de données
 - Cache de déduplication
 - Logithèque DVM
 - Exchange
 - Exportation
 - Tâches
 - Licences
 - Montage local
 - Troncature de journal
 - Métadonnées
 - Tâches nocturnes
 - Notification
 - Mettre en mode persistant l'état du Core
 - PowerShell Scripting
 - Protection
 - Installation Push
 - Vérification des points de restauration
 - Montage distant
 - Logithèque commune
 - Réplication
 - Restaurer
 - Consolidation
 - Archives programmées
 - Sécurité
 - Journaux serveur
 - vSphere
- Pour définir des alertes pour tous les événements dans chaque groupe, cochez la case correspondant à **toutes les alertes**.
 - Dans n'importe quel groupe d'alerte, pour définir des alertes pour tous les événements, cochez la case correspondante en regard du groupe.
 - Pour sélectionner uniquement certains types d'alerte au sein d'un groupe d'alerte, développez le groupe, puis sélectionnez uniquement les événements spécifiques que vous souhaitez suivre, enregistrer et pour lesquels vous souhaitez définir des alertes.

6 Cliquez sur l'onglet **Options de notification**.

7 Dans l'onglet **Options de notification**, spécifiez la méthode de prise en charge du processus de notification.

Option	Description
Notifier par e-mail	Indiquez les destinataires des notifications par courrier électronique. Vous pouvez décider de spécifier des adresses électroniques séparées, ainsi que des copies carbone ou des copies cachées. Choisissez une des options suivantes : • À : • CC : • CCI :
Notifier via le journal d'événements Windows	Sélectionnez cette option si vous voulez que les alertes soient signalées par l'intermédiaire du journal d'événements Windows.

Option	Description
Notifier par syslogd	Sélectionnez cette option si vous voulez que les alertes soient signalées par l'intermédiaire de syslogd. Spécifiez les détails syslogd dans les champs suivants : · Hôte : · Port :
Notifier via des alertes Toast	Sélectionnez cette option si vous voulez que l'alerte apparaisse dans une fenêtre dans la partie inférieure droite de l'écran.
Notifier par des alertes	Sélectionnez cette option si vous souhaitez que les alertes apparaissent en tant que fenêtres contextuelles situées en bas à droite de la console Core.
Notifier par des notifications trap SNMP	Le Core Rapid Recovery fait office d'agent SNMP et envoie des interruptions (notifications à propos d'événements spécifiques) à un gestionnaire SNMP. Cela entraîne la communication d'informations sur le core, comme des alertes, ou encore l'état des logithèques et des machines protégées. Sélectionnez cette option si vous voulez notifier les événements du core par le biais d'une notification trap SNMP. Vous devez également spécifier un numéro de notification trap. Par exemple, le numéro d'interruption utilisé par défaut par le Core Rapid Recovery est 162.

8 Cliquez sur **OK**.

Un message s'affiche indiquant que le nom du groupe de notification que vous avez défini ne peut pas être modifié après la création du groupe. Les autres propriétés du groupe de notification peuvent être modifiées à tout moment.

- Après avoir défini le nom du groupe, confirmez ce message et enregistrer votre travail.
- Si vous voulez modifier le nom du groupe, cliquez sur **Non** pour retourner à la fenêtre Créer un groupe de notification, changez le nom du groupe et les autres paramètres de notification éventuels du groupe, puis enregistrez votre travail.

Le groupe de notification s'affiche dans le tableau récapitulatif. Vous pouvez créer différents groupes de notification à l'aide de n'importe quel ensemble de paramètres.

À propos de la configuration de la réduction des répétitions

Il est d'importance critique que les administrateurs puissent recevoir des alertes sur certains événements. Néanmoins, dans certaines circonstances, le fait de recevoir des notifications répétées sur des événements dont vous êtes déjà informé peut s'avérer gênant et énervant. Même si l'alerte générée découle d'une panne de la plateforme dont vous souhaitez être informé immédiatement, cette même erreur peut également générer des centaines, voire des milliers d'événements dans le journal des événements. Afin de diminuer le nombre de doublons dans le journal des événements et de limiter le nombre de notifications par e-mail reçues pour un même événement dans la console Core, Rapid Recovery dispose d'un paramètre de réduction des répétitions, activé par défaut et fixé à 5 minutes. Ce paramètre peut être réglé sur une valeur plus basse (1 minute au minimum) ou plus haute (60 minutes au maximum). Vous pouvez également le désactiver entièrement.

Lorsque la réduction des répétitions est désactivée, chaque fois que des événements se produisent, ils sont enregistrés dans la base de données, même s'il s'agit d'événements de même type et de même portée. Indépendamment du temps qui s'est écoulé depuis que cet événement s'est produit la dernière fois, chaque nouvelle occurrence est affichée dans la partie Alertes de l'onglet Événements.

Lorsque la réduction des répétitions est activée (par exemple, avec une valeur par défaut de 5 minutes), à sa première occurrence, l'événement spécifique est enregistré dans la base de données des événements et s'affiche dans le journal des alertes. Si par la suite un événement du même type et de la même portée est de nouveau journalisé au cours du laps de temps spécifié, le nombre d'occurrences de l'événement enregistré dans la base de données augmente de 1 à chaque nouvelle occurrence survenant pendant ce laps de temps. Le journal est accessible dans la section Alertes de la page Événements. Cependant, il n'affiche l'événement qu'une seule fois en précisant la date et l'heure de la dernière occurrence. L'événement ne s'affiche à nouveau dans le journal que lorsque le délai de la première occurrence expire. Par exemple, si vous avez défini un délai de 5 minutes et que l'événement se produit à nouveau 6 minutes plus tard, celui-ci s'affiche dans le journal et vous recevez un autre e-mail.

Configurer la réduction des répétitions

Suivez cette procédure pour configurer la réduction des répétitions des événements.

- 1 Accédez à la console Core de Rapid Recovery. Dans la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Notifications**.
La page **Notifications** s'affiche.
 - 2 Dans le volet Réduction des répétitions, affichez les paramètres existants.
 - 3 Pour activer, désactiver ou modifier le seuil de temps des événements stockés, cliquez sur  **Modifier**.
La boîte de dialogue **Modifier la réduction des répétitions** apparaît.
 - 4 Effectuez l'une des opérations suivantes :
 - Pour désactiver la réduction des répétitions, décochez l'option **Activer la réduction des répétitions**.
 - Pour activer la réduction des répétitions, sélectionnez l'option **Désactiver la réduction des répétitions**.
 - Pour modifier le seuil de temps (en minutes) pour lequel les événements identiques répétés sont ignorés, entrez un nombre compris entre 1 et 60 dans la zone de texte **___ minute(s)**.
-  **REMARQUE :** L'option **Activer la réduction des répétitions** doit être cochée pour modifier cette valeur.
- 5 Cliquez sur **OK** pour enregistrer les paramètres et fermer la boîte de dialogue.

Configurer la rétention des événements

Les événements et tâches suivies sur le Core sont enregistrés pour une période de temps spécifiée. Le paramètre par défaut est 30 jours. Ce nombre peut être défini entre 0 et 3652 jours (environ 10 ans).

Suivez cette procédure pour configurer la rétention des événements.

- 1 Naviguez jusqu'à la console Core Rapid Recovery.
- 2 Sur la barre d'icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Dans la liste des paramètres Core, sur le côté gauche de la page Paramètres, cliquez sur **Connexion à la base de données**.
 - Faites défiler vers le bas sur le côté droit de la page Paramètres jusqu'à ce que l'en-tête **Connexion à la base de données** soit affiché.

Les paramètres de connexion de la base de données s'affichent.
- 3 Pour modifier le nombre de jours pour lesquels les informations d'événement sont enregistrés à la base de données, cliquez sur le champs de texte **Période de rétention (jours)**, entrez une valeur comprise entre 0 et 3652, puis cliquez sur  pour enregistrer la modification.
La période de rétention des événements est réglée selon les indications.

Rapid Appliance Self Recovery

RASR (Rapid Appliance Self Recovery) est un processus de restauration BMR (bare metal restore) qui ramène rapidement votre appliance en bon état de fonctionnement.

RASR propose deux options de récupération :

- Restaurer les paramètres définis en usine

- Récupérer votre appliance vers l'état qui était le sien juste avant la panne (l'OS, les configurations et les paramètres sont récupérés)

Création de la clé USB RASR

Pour créer une clé USB RASR :

- 1 Allez à l'onglet **Appliance**.
- 2 Dans le volet de navigation de gauche, sélectionnez **Appliance > Sauvegarde**.
La fenêtre **Créer un lecteur USB RASR** s'affiche.
REMARQUE : Insérez une clé USB 16 Go ou plus, avant de tenter de créer la clé RASR.
- 3 Après avoir inséré une clé USB de 16 Go ou plus, cliquez sur **Créer un lecteur USB RASR maintenant**.
Un message de **vérification de conditions** s'affiche.
Une fois les prérequis vérifiés, la fenêtre **Créer un lecteur USB RASR** affiche la taille minimale requise pour créer le lecteur USB et la **liste des chemins cible possible**.
- 4 Sélectionnez la cible et cliquez sur **Créer**.
Une boîte de dialogue de confirmation s'affiche.
- 5 Cliquez sur **Oui**.
La clé de lecteur USB RASR est créée.
- 6 **REMARQUE :** Veillez à utiliser la fonction Windows d'éjection de lecteur pour préparer le retrait de la clé USB. Sinon, le contenu de celle-ci risque d'être endommagé et la clé USB risque de ne pas fonctionner comme prévu.
Retirez la clé USB RASR créée pour chaque appliance DL, étiquetez-la et rangez-la en vue d'une utilisation ultérieure.

Exécution du RASR

- REMARQUE :** Dell recommande de créer une clé USB RASR une fois que vous avez configuré l'appliance. Pour créer une clé USB RASR, reportez-vous à la section **Création de la clé USB RASR**.
- REMARQUE :** Assurez-vous que vous disposez des derniers RUU disponibles et accessibles sur votre appliance.
- REMARQUE :** Pour savoir comment effectuer une récupération du système à l'aide de RASR, reportez-vous au document *Récupérer une appliance Dell™ DL de sauvegarde et de récupération à l'aide de RASR (Rapid Appliance Self Recovery)* sur Dell.com/support/home.

Pour effectuer une réinitialisation des paramètres d'usine :

- 1 Insérez la clé USB RASR créée.
- 2 Redémarrez l'appliance et sélectionnez **Gestionnaire d'amorçage (F11)**.
- 3 Dans le **menu principal du Gestionnaire d'amorçage**, sélectionnez le **menu d'amorçage ponctuel du BIOS**.
- 4 Dans le **menu d'amorçage du gestionnaire d'amorçage**, sélectionnez le lecteur USB relié.
- 5 Sélectionnez votre configuration de clavier.
- 6 Cliquez sur **Dépanner > Rapid Appliance Self Recovery**.
- 7 Sélectionnez le système d'exploitation cible (SE).
RASR démarre, et l'écran d'**accueil** s'affiche.
- 8 Cliquez sur **Suivant**.
L'écran de vérification **Conditions** s'affiche.
REMARQUE : Veillez à ce que tous les matériels et les autres spécifications soient vérifiés avant d'exécuter RASR.
- 9 Cliquez sur **Suivant**.

L'écran de **sélection du mode de restauration** s'affiche avec trois options :

- **Restauration du système**
- **Assistant de récupération Windows**
- **Restauration des paramètres définis en usine**

10 Sélectionnez l'option **Restaurer les paramètres définis en usine** .

This option will recover the operating system disk from the factory image.

11 Cliquez sur **Suivant**.

Le message d'avertissement suivant s'affiche dans une boîte de dialogue : `This operation will recover the operating system. All OS disk data will be overwritten.`

12 Cliquez sur **Oui**.

Le disque du système d'exploitation commence la restauration du système d'exploitation d'origine.

13 La page **RASR terminé** s'affiche à la fin de la récupération. Cliquez sur **Terminer**.

14 Démarrez le système après la restauration.

15 ⓘ **REMARQUE : Ne continuez que si vous voyez l' Assistant de configuration d'appliance AppAssure ; sinon, passez à l'étape 17.**

Attendez que l'Assistant de configuration de l'appliance AppAssure ait fini de se charger. Vous devez le fermer. Fermez l'assistant à l'aide du Gestionnaire des tâches de Windows.

16 Exécutez le fichier **launchRUU.exe** dans le package RUU. Laissez-vous guider par les instructions qui s'affichent et sélectionnez l'option permettant de poursuivre l'installation de RUU.

17 L'**Assistant de configuration de l'appliance DL** se lance et vous guide dans la restauration.

Votre appliance fonctionne normalement à présent.

Utilitaire Local Mount Utility (LMU)

Cette section décrit la procédure de téléchargement, d'installation et d'utilisation de l'utilitaire de montage local (LMU) de Rapid Recovery pour monter des points de restauration et explorer le contenu à partir d'un niveau des fichiers à l'aide d'une machine qui n'héberge pas le Core Rapid Recovery.

À propos de l'Utilitaire LMU (Local Mount Utility)

L'utilitaire LMU est une application Windows téléchargeable qui vous permet de monter un point de restauration Rapid Recovery dans l'un des trois modes disponibles sur une machine Windows. L'utilitaire léger peut être installé sur des systèmes d'exploitation Windows 32 bits / 64 bits et inclut les pilotes rapidrecovery-vdisk (ancien aavdisk) et aavstor, mais il ne s'exécute pas en tant que service. Lorsque vous installez l'utilitaire, il est installé par défaut dans le répertoire **C:\Program Files\AppRecovery\Local Mount Utility** et un raccourci apparaît sur le bureau de la machine.

Bien que l'utilitaire soit conçu pour accéder à distance à un Core Rapid Recovery, vous pouvez également installer l'utilitaire LMU sur la même machine qu'un Core Rapid Recovery. Lorsqu'elle est exécutée sur un Core, l'application reconnaît et affiche tous les montages de ce Core, y compris les montages effectués via la console Core Rapid Recovery. De même, les montages effectués sur l'utilitaire LMU apparaissent également dans la console Core.

Lorsque l'utilitaire LMU est installé sur la même machine que Mailbox Restore, l'utilitaire LMU lance automatiquement Mailbox Restore lorsque vous l'utilisez pour ouvrir une base de données Exchange. Mailbox Restore est l'application Rapid Recovery de Dell utilisée pour restaurer les magasins et éléments de données Microsoft Exchange. Vous pouvez l'installer lors de l'installation de l'utilitaire LMU ou du Core Rapid Recovery. Pour plus d'informations sur Mailbox Restore, reportez-vous au *Dell Data Protection | Rapid Recovery Guide de l'utilisateur de Mailbox Restore pour Microsoft Exchange*.

REMARQUE : les machines Linux utilisent un utilitaire de ligne de commande, `local_mount`, pour effectuer une requête sur les machines protégées du Core et leurs points de restauration correspondants. De manière similaire, cet outil permet aux utilisateurs de monter à distance un volume de points de restauration ; il permet aux utilisateurs d'explorer le contenu du volume au niveau des fichiers ; et il permet aux utilisateurs de restaurer des fichiers individuels ou de restaurer un volume entier à partir du point de restauration, y compris la BMR du volume système. Pour plus d'informations, voir [Monter un volume d'un point de restauration sur une machine Linux](#), [Restaurer les volumes d'une machine Linux à l'aide de la ligne de commande](#) et [Effectuer une restauration Bare Metal Restore de machines Linux](#), respectivement.

Utilisation des Cores Rapid Recovery de l'utilitaire de montage local

L'utilitaire de montage local (LMU) vous permet de travailler localement ou à distance avec un nombre illimité de Cores. Si vous installez l'utilitaire LMU sur un Core Rapid Recovery, cette machine apparaît automatiquement dans l'utilitaire LMU en tant que localhost. Tous les Cores distants supplémentaires apparaissent sous leurs noms de machine ou adresses IP, selon les informations que vous avez saisies lors de leur ajout. Avec l'utilitaire LMU, vous pouvez ajouter, modifier et supprimer des Cores. Pour en savoir plus, reportez-vous aux procédures suivantes :

Liens connexes

- [Ajout d'un Core à l'utilitaire Local Mount Utility](#)
- [Modification des options de l'utilitaire de montage local](#)
- [Modification des paramètres de connexion de Core dans l'utilitaire Local Mount Utility](#)
- [Reconnexion à un Core](#)
- [Suppression d'une machine Core Rapid Recovery de l'utilitaire Local Mount Utility](#)

Ajout d'un Core à l'utilitaire Local Mount Utility

Pour monter un point de restauration, vous devez ajouter un Core à l'utilitaire LMU. Le nombre de Cores que vous pouvez ajouter est illimité.

Pour paramétrer l'utilitaire LMU en ajoutant un Core, procédez comme suit.

- Depuis l'ordinateur sur lequel l'utilitaire LMU est installé, lancez l'utilitaire LMU en double-cliquant sur l'icône du bureau.
- Effectuez l'une des opérations suivantes :
 - Dans le menu Utilitaire de montage local, en haut à gauche de l'écran, cliquez sur **Ajouter un Core**.
 - Cliquez avec le bouton droit sur l'espace vide dans le panneau gauche, puis cliquez sur **Ajouter un Core**.

La boîte de dialogue **Ajouter un Core** s'affiche.

- Dans la fenêtre **Ajouter un Core**, entrez les informations d'identification demandées décrites dans le tableau suivant.

Tableau 51. Informations d'identification du Core Rapid Recovery

Option	Description
Nom d'hôte	Nom ou adresse IP du Core à partir duquel vous souhaitez monter les points de restauration.
	REMARQUE : lors de son installation sur une machine du Core Rapid Recovery, l'utilitaire LMU ajoute automatiquement la machine localhost.
Port	Numéro de port utilisé pour communiquer avec le Core. Le numéro de port par défaut est 8006.

Option	Description
Utiliser mes références utilisateur Windows	Sélectionnez cette option si les références que vous utilisez pour accéder au Core sont les mêmes que vos références Windows.
Utiliser des références spécifiques	Sélectionnez cette option si les références que vous utilisez pour accéder au Core sont différentes de celles de Windows.
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder à la machine Core.
 REMARQUE : cette option n'est disponible que si vous choisissez d'utiliser des informations d'identification spécifiques.	
Mot de passe	Mot de passe utilisé pour accéder à la machine Core.
 REMARQUE : cette option n'est disponible que si vous choisissez d'utiliser des informations d'identification spécifiques.	

- 4 Cliquez sur **Connexion**.
- 5 Si vous ajoutez plusieurs Cores, répétez ces étapes autant de fois que nécessaire.

Modification des options de l'utilitaire de montage local

Suivez la procédure ci-après pour modifier les options de tous les Cores Rapid Recovery connectés au LMU.

- 1 Depuis l'interface utilisateur de l'utilitaire Local Mount Utility, cliquez sur **Options**.
- 2 La boîte de dialogue **Options** vous permet de modifier les paramètres décrits dans le tableau suivant.

Tableau 52. Paramètres du Core

Option	Description
Référentiel de point de montage par défaut	Utilisez le bouton Parcourir ou saisissez un chemin d'accès à l'emplacement que vous souhaitez utiliser pour le montage des points de restauration.
Utiliser mes informations de connexion de compte d'utilisateur Windows	Sélectionnez cette option pour toujours utiliser vos références Windows par défaut lorsque vous ouvrez une session sur un Core.
Utiliser des références spécifiques	Sélectionnez cette option pour utiliser les références suivantes pour chaque Core connecté : • Nom d'utilisateur : saisissez le nom d'utilisateur à utiliser pour tous les Cores. • Mot de passe : saisissez le mot de passe à utiliser pour tous les Cores.
Délai d'attente de connexion au Core (s)	Saisissez le délai pendant lequel le LMU doit continuer d'essayer de se connecter à un Core avant que la connexion ne s'interrompe (en minutes : secondes : millisecondes).
Langue	Sélectionnez la langue dans laquelle vous souhaitez que le LMU s'affiche. Vous pouvez choisir parmi les options suivantes : • Anglais • Français • Allemand • Portugais • Espagnol • Chinois simplifié • Japonais

Option	Description
	Coréen

Modification des paramètres de connexion de Core dans l'utilitaire Local Mount Utility

Pour modifier les paramètres que vous avez définis lorsque vous avez ajouté un Core à l'utilitaire LMU (Local Mount Utility), suivez la procédure ci-dessous.

REMARQUE : Cette procédure ne s'applique pas au Core localhost. Elle s'applique uniquement aux machines Core distantes.

- 1 Sur l'interface utilisateur de l'utilitaire Local Mount Utility, cliquez avec le bouton droit sur le Core dont vous souhaitez modifier les paramètres, puis cliquez sur **Modifier le Core**.
- 2 La boîte de dialogue **Modifier le Core** permet de modifier les paramètres décrits dans le tableau suivant.

Tableau 53. Paramètres du Core

Option	Description
Nom d'hôte	Nom du core à partir duquel vous souhaitez monter les points de restauration. REMARQUE : Lors de son installation sur une machine Core Rapid Recovery, l'utilitaire LMU ajoute automatiquement la machine hôte local.
Port	Numéro de port utilisé pour communiquer avec le core. Le numéro de port par défaut est 8006.
Utiliser mes références utilisateur Windows	Sélectionnez cette option si les références que vous utilisez pour accéder au core sont les mêmes que vos références Windows.
Utiliser des références spécifiques	Sélectionnez cette option si les références que vous utilisez pour accéder au core sont différentes de celles de Windows.
Nom d'utilisateur	Nom d'utilisateur utilisé pour accéder à la machine core. REMARQUE : Cette option est disponible uniquement si vous choisissez d'utiliser des informations d'identification spécifiques.
Mot de passe	Mot de passe utilisé pour accéder à la machine core. REMARQUE : Cette option est disponible uniquement si vous choisissez d'utiliser des informations d'identification spécifiques.

- 3 Une fois que vous avez apporté vos modifications, cliquez sur **OK**.

Reconnexion à un Core

Si vous perdez la connexion à un Core Rapid Recovery, vous pouvez actualiser la connexion en effectuant l'étape suivante.

Depuis l'interface utilisateur de l'utilitaire de montage local, effectuez l'une des opérations suivantes :

- Si le Core est hors ligne, double-cliquez sur le Core auquel vous souhaitez rétablir la connexion.
L'utilitaire LMU tente de rétablir une connexion au Core.

- Si le Core est en ligne, effectuez un clic droit sur le Core puis cliquez sur Reconnecter au Core.
L'utilitaire LMU actualise la connexion.

Suppression d'une machine Core Rapid Recovery de l'utilitaire Local Mount Utility

Suivez la procédure ci-dessous pour supprimer un Core de l'utilitaire LMU (Local Mount Utility).

❗ REMARQUE : Cette option n'est pas disponible pour un Core Rapid Recovery situé sur et étiqueté comme localhost.

- 1 À partir de l'interface utilisateur de l'utilitaire Local Mount Utility, cliquez avec le bouton droit de la souris sur le Core que vous souhaitez supprimer, puis cliquez sur **Supprimer le Core**.
- 2 Pour confirmer la commande, cliquez sur **Oui** dans la boîte de dialogue.
L'utilitaire LMU supprime le Core et ses machines protégées de l'arborescence de navigation.

Utilisation de machines protégées dans l'utilitaire Local Mount Utility

Avec l'utilitaire Local Mount Utility (LMU), vous pouvez monter et parcourir les points de restauration de machines protégées sans avoir à être connecté à la Rapid Recovery Core Console associée à cette machine. Pour en savoir plus, reportez-vous aux procédures suivantes :

- [Monter un point de restauration à l'aide de Local Mount Utility](#)
- [Exploration d'un point de restauration monté à l'aide de l'utilitaire Local Mount Utility](#)
- [Actualisation des points de restauration](#)
- [Démontage de certains points de restauration avec l'utilitaire Local Mount Utility](#)
- [Démontage de tous les points de restauration à partir d'un Core Rapid Recovery ou d'une machine protégée unique](#)
- [Démontage de tous les points de restauration montés à l'aide de l'utilitaire de montage local](#)

Monter un point de restauration à l'aide de Local Mount Utility

À l'aide de l'utilitaire LMU, vous pouvez monter n'importe quel point de récupération associé à une machine Core connectée, y compris des machines protégées, des machines répliquées et des machines de points de récupération uniquement.

Pour pouvoir monter un point de restauration, l'utilitaire Local Mount Utility (LMU) doit être connecté au core sur lequel le point de restauration est stocké. Comme indiqué dans la procédure [Ajout d'un Core à l'utilitaire Local Mount Utility](#), vous pouvez ajouter à l'utilitaire LMU autant de Cores que vous le souhaitez. Cependant, l'application ne peut se connecter qu'à un seul Core à la fois. Par exemple, si vous montez un point de restauration d'une machine protégée par un Core, puis montez un point de restauration d'une machine protégée par un Core différent, l'utilitaire LMU se déconnecte automatiquement du premier Core pour établir une connexion avec le second.

- 1 Dans la fenêtre principale de l'interface utilisateur de l'utilitaire Local Mount Utility, développez le Core dans l'arborescence pour afficher les machines protégées.
- 2 Dans l'arborescence, sélectionnez la machine à partir de laquelle vous souhaitez monter un point de restauration.
Les points de restauration s'affichent dans le cadre principal.
- 3 Facultativement, développez le point de restauration que vous souhaitez monter pour afficher les bases de données ou les volumes de disque individuels.
- 4 Cliquez avec le bouton droit sur le point de restauration à monter, puis sélectionnez l'une des options suivantes :

Option	Description
Montage	Cette option permet de monter le point de restauration en lecture seule.
Monter en lecture-écriture	Cette option permet de modifier le point de restauration monté.

Option	Description
Monter en lecture seule avec les écritures précédentes	Cette option monte le point de restauration en lecture seule et prend en compte toutes les modifications qui ont déjà été apportées.
Montage avancé...	Cette option ouvre la boîte de dialogue Montages avancés.

- 5 Si vous avez sélectionné **Montage avancé**, définissez les options décrites dans le tableau suivant.

Tableau 54. Options de montage avancées

Option	Description
Chemin du point de montage	Cliquez sur Parcourir pour choisir un chemin autre que le chemin de montage par défaut pour les points de restauration, ou saisissez manuellement le chemin de votre choix.
Type de montage	Sélectionnez l'une des options suivantes : • Monter en lecture seule • Monter en lecture-écriture • Monter en lecture seule avec les écritures précédentes Pour obtenir la description de chaque option, voir l'étape 4.

- Cliquez sur **Monter**.

L'utilitaire LMU ouvre automatiquement le dossier qui contient le point de restauration monté.

REMARQUE : Si vous sélectionnez un point de restauration déjà monté, la boîte de dialogue Montage demande de confirmer le démontage du point de restauration.

Exploration d'un point de restauration monté à l'aide de l'utilitaire Local Mount Utility

L'exploration d'un point de restauration ouvre les données sauvegardées dans une fenêtre de l'Explorateur Windows, et vous permet de rechercher le ou les éléments à restaurer dans les volumes et les dossiers correspondants.

Vous pouvez ensuite restaurer des éléments en les copiant dans votre emplacement préféré à l'aide d'un gestionnaire de fichiers tel que l'Explorateur Windows (ou de façon planifiée à l'aide des API Windows). Suivez cette procédure pour explorer un point de restauration monté.

REMARQUE : cette procédure n'est pas nécessaire si vous explorez un point de restauration immédiatement après l'avoir monté, car le dossier contenant le point de restauration s'ouvre automatiquement à la fin de la procédure de montage.

- 1 Dans l'interface utilisateur de Local Mount Utility, cliquez sur **Montages actifs**.
La fenêtre Montages actifs s'ouvre et affiche tous les points de restauration montés.
- 2 Développez l'arborescence de navigation pour afficher les points de restauration montés sur chaque machine et chaque volume.
- 3 Cliquez sur **Explorer** en regard du volume à explorer.

Actualisation des points de restauration

L'utilitaire LMU ne reçoit pas les mises à jour en temps réel à partir du Core et des machines protégées. Pour actualiser une machine protégée et afficher ses derniers points de restauration, effectuez la procédure suivante.

À partir de l'interface utilisateur de l'utilitaire de montage local, cliquez avec le bouton droit de la souris sur la machine protégée que vous souhaitez actualiser, puis cliquez sur Actualiser les points de restauration.

Démontage de certains points de restauration avec l'utilitaire Local Mount Utility

Suivez cette procédure pour démonter un point de restauration sur un Core distant à l'aide de l'utilitaire LMU.

- 1 Dans l'interface utilisateur de Local Mount Utility, cliquez sur **Montages actifs**.
La fenêtre **Montages actifs** s'ouvre et affiche tous les points de restauration montés.
- 2 Vous pouvez également cliquer sur l'icône Plus ou Moins pour développer ou réduire les volumes affichés de chaque point de restauration monté dans la fenêtre **Montages actifs**.
- 3 Dans la fenêtre **Montages actifs**, cliquez sur **Démonter** en regard de chaque point de restauration ou volume à démonter.
La fenêtre de progression indique lorsque les points de restauration sélectionnés sont démontés.
- 4 Cliquez sur la croix **x** en haut à droite de la fenêtre **Montages actifs** pour fermer la fenêtre et revenir à l'utilitaire LMU.

Démontage de tous les points de restauration à partir d'un Core Rapid Recovery ou d'une machine protégée unique

Suivez cette procédure pour démonter uniquement les points de restauration qui sont montés à partir d'un seul Core ou machine protégée.

- 1 Depuis l'interface utilisateur de l'utilitaire de montage local, effectuez l'une des opérations suivantes :
 - Effectuez un clic droit sur le Core pour lequel vous souhaitez démonter tous les points de restauration.
 - Effectuez un clic droit sur la machine protégée pour laquelle vous souhaitez démonter tous les points de restauration.
- 2 Cliquez sur **Tout démonter pour [nom_machine]**.
- 3 Pour confirmer la commande, dans la boîte de dialogue, cliquez sur **Oui**.

 **REMARQUE :** lorsqu'il y a des tâches actives utilisant les montages existants, le démontage de ces montages entraîne l'échec des tâches.

Tous les points de restauration montés sélectionnés sont démontés.

Démontage de tous les points de restauration montés à l'aide de l'utilitaire de montage local

Il existe deux manières principales de démonter tous les points de restauration en une fois dans l'utilitaire LMU. Vous pouvez démonter tous les points de restauration sans voir les points de restauration qui sont actuellement montés, ou vous pouvez afficher tous les points de restauration actuellement montés, puis tous les démonter. Reportez-vous à la procédure correspondante pour chaque cas.

Démontage de tous les points de restauration à l'aide du bouton Démonter tous les montages

Suivez la procédure ci-dessous pour démonter tous les points de restauration montés en une seule fois.

- 1 Dans le menu de l'utilitaire Local Mount Utility (LMU), cliquez sur **Démonter tous les montages**.
- 2 Pour confirmer la commande, dans la boîte de dialogue, cliquez sur **Oui**.

 **REMARQUE :** Lorsqu'il y a des tâches actives utilisant les montages existants, le démontage de ces montages entraîne l'échec des tâches.

Démontage de tous les points de restauration à l'aide de la fenêtre Montages actifs

Suivez la procédure suivante pour démonter tous les points de restauration montés en une seule fois à partir de la fenêtre Montages actifs.

- 1 Depuis l'interface utilisateur de l'utilitaire de montage local, cliquez sur **Montages actifs**.
- 2 Dans la fenêtre **Montages actifs**, cliquez sur **Démonter tout**.
- 3 Pour confirmer la commande, dans la fenêtre, cliquez sur **Oui**.
- 4 Dans la boîte de dialogue **Montages actifs**, cliquez sur **Fermer**.

Utiliser la zone de notification de Local Mount Utility

La zone de notification de l'utilitaire LMU est située dans la barre des tâches de votre bureau. Faites un clic droit pour faire apparaître les options décrites dans le tableau suivant :

Tableau 55. Options de la zone de notification

Option	Description
Parcourir les points de restauration	Ouvre l'écran principal de l'utilitaire LMU.
Montages actifs	Ouvre la boîte de dialogue Montages actifs au-dessus de la fenêtre principale de LMU.
Options	Ouvre la boîte de dialogue Options au-dessus de la fenêtre principale de LMU. Dans la boîte de dialogue Options, vous pouvez modifier le répertoire du point de montage par défaut et les informations d'identification du Core par défaut pour l'interface utilisateur de l'utilitaire LMU.
À propos de	Fait apparaître les informations concernant la licence de Local Mount Utility.
Quitter	Ferme l'application LMU.

Gestion de l'appliance

La Core Console inclut l'onglet **Appliance**, qui vous permet de provisionner l'espace, de surveiller l'intégrité de l'appliance et d'accéder aux outils de gestion.

Sujets :

- [Surveillance de l'état de l'appareil](#)
- [Sauvegarde Windows](#)
- [Provisionnement du stockage](#)
- [Supprimer une allocation d'espace pour un disque virtuel](#)
- [Utilitaire de récupération et de mise à jour](#)

Surveillance de l'état de l'appareil

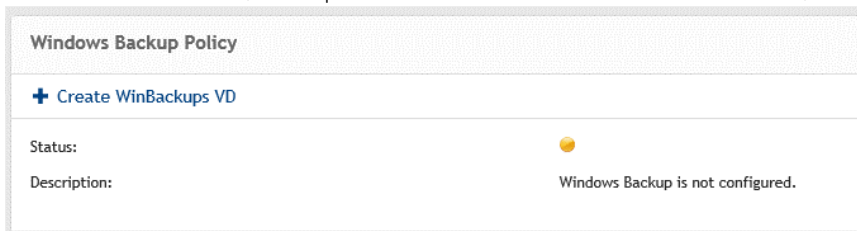
Vous pouvez surveiller l'état des sous-systèmes de l'appareil par l'intermédiaire de la page **Intégrité > de l'appareil**. La page **Intégrité** affiche un voyant d'état à côté de chaque sous-système, ainsi qu'une description de l'état indiquant l'intégrité du sous-système.

La page **Intégrité** fournit également des liens vers des outils accédant à l'ensemble des détails de chaque sous-système, permettant d'aider la détermination des causes d'erreurs et d'alarmes et d'y remédier. Le lien **État de l'approvisionnement**, disponible pour le sous-système Approvisionnement du stockage, ouvre l'écran **Approvisionnement** qui affiche l'état de l'approvisionnement de ce sous-système. Le lien **Récupération automatique et rapide de l'appareil**, disponible pour le sous-système Récupération automatique et rapide de l'appareil, ouvre la page **Sauvegarde**, dans laquelle vous pouvez créer la clé USB RASR, surveiller l'état de la sauvegarde de Windows et configurer la stratégie de sauvegarde de Windows. Le lien **Gestion des MV** ouvre la page **Mise en veille virtuelle** depuis laquelle vous pouvez gérer les machines virtuelles. Le lien **Administrateur serveur**, disponible pour le sous-système Matériel de stockage, ouvre la page relative à l'intégrité de votre système dans laquelle vous pouvez analyser l'état du contrôleur, du boîtier, des disques physiques, etc. Le lien **Contrôleurs**, disponible pour le sous-système Matériel de l'appareil, ouvre la page **Contrôleurs**, qui présente les informations détaillées des contrôleurs et des disques physiques associés à un contrôleur.

Sauvegarde Windows

La fonction de sauvegarde de Windows est disponible pour toute la gamme DL, à l'exception des DL 1000. L'onglet de **Sauvegarde > de l'appareil** vous permet de configurer la stratégie de sauvegarde de Windows et d'afficher l'état de la dernière sauvegarde, ainsi que les éléments précédemment sauvegardés. Pour utiliser cette fonction de sauvegarde de Windows, un disque virtuel de sauvegarde de Windows doit exister.

- Après avoir mis votre appareil à niveau au moyen de l'utilitaire de mise à jour de la ROM, ou RUU, le plus récent (3.0.x) et si le disque virtuel de sauvegarde de Windows (créé dans l'environnement AppAssure) n'existe pas, ce disque est créé après avoir suivi les étapes de l'assistant de configuration de l'appareil DL. Au cas où le disque virtuel de sauvegarde de Windows n'existerait pas, cliquez sur **+ Créer un disque virtuel de sauvegarde de Windows** sur la page **Sauvegarde** de la section **Stratégie de sauvegarde Windows**. Pour les DL 4000 et DL 4300, un disque virtuel de 295 Go est créé. Pour les DL 1300, le disque virtuel est de 210 Go.



- Après avoir mis votre appareil à niveau au moyen du RUU le plus récent et si le disque virtuel de sauvegarde de Windows créé dans l'environnement AppAssure existe, procédez aux étapes suivantes pour créer un disque virtuel de sauvegarde de Windows dans l'environnement de la Récupération rapide :

- Modifiez **ApplianceProvisioningConfiguration.xml** (ce fichier se trouve dans la racine de chaque volume, vous pouvez donc le modifier une fois et le copier à l'endroit nécessaire) :

⚠ PRÉCAUTION : ne supprimez pas un disque virtuel de sauvegarde de Windows déjà existant.

- 1 Supprimez tout le texte se trouvant entre les balises **<BackupVolumes>**.
 - 2 Supprimez la balise **</BackupVolumes>**.
 - 3 Modifiez la balise **<BackupVolumes>** pour qu'elle devienne **<Backupvolume/>**.
 - 4 Enregistrez et fermez.
- Accédez à la console du Noyau.
 - Cliquez sur l'onglet **RASR** de l'appareil.
 - Cliquez sur le bouton **Créer un volume de sauvegarde de Windows**.
 - Un disque virtuel de sauvegarde de Windows est créé si l'espace disponible est suffisant.

REMARQUE : vous pouvez également configurer la sauvegarde de Windows par le biais de la fonctionnalité de sauvegarde de Windows Server et conserver ces sauvegardes à n'importe quel endroit, cependant, dans un tel cas, une erreur est affichée sur la page RASR car ces sauvegardes ne peuvent être contrôlées et il est impossible de garantir qu'elles soient homogènes pour une restauration au moyen de RASR.

État de la sauvegarde

L'état de la sauvegarde Microsoft Windows est disponible sous l'onglet **Dernière sauvegarde**. Si une sauvegarde est actuellement en cours d'exécution, les informations s'affichent sous l'onglet **Sauvegarde actuelle**. Pour afficher la dernière sauvegarde, effectuez les opérations suivantes :

- 1 Dans la console du Noyau, accédez à l'onglet **Sauvegarde > de l' appareil**.
- 2 Cliquez sur la flèche en regard du bouton **État** pour afficher l'état de la sauvegarde.
- 3 Le volet **Dernière sauvegarde** affiche les informations suivantes :
 - État
 - État
 - Emplacement de sauvegarde
 - Heure de début
 - Heure de fin
 - Description de l'erreur
 - Éléments qui ont été sauvegardés

REMARQUE : les informations ci-dessus s'affichent que la stratégie de sauvegarde de Windows soit exécutée ou non.

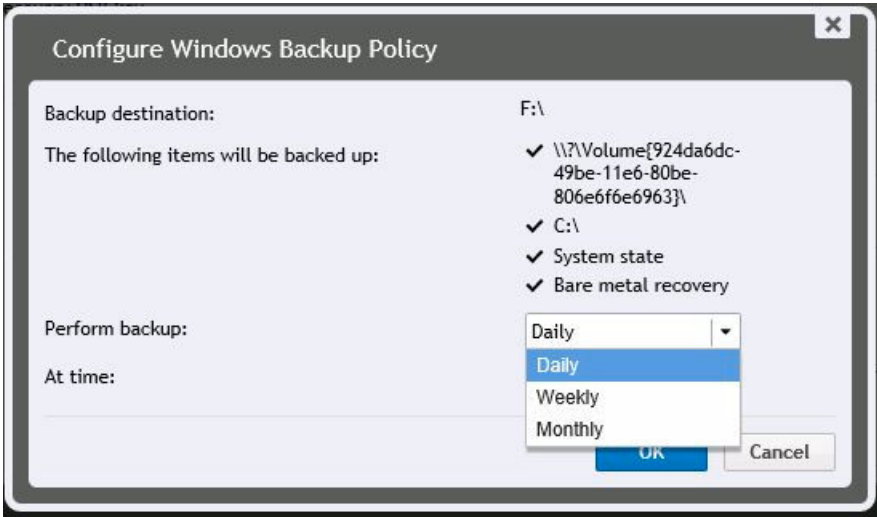
Backup Status	
Last Backup	
Status:	🟢 (Completed successfully)
Backup Location:	F:
Start Time:	8/16/2016 7:34:00 PM
End Time:	8/16/2016 7:39:00 PM
Error Description:	
Error Actions:	
Items Backed Up	
State	Name
1	VolumeList
1	SystemState
1	BareMetalRecovery

Si une sauvegarde est en cours d'exécution, les informations concernant la **Progression de la sauvegarde actuelle** et l'**Heure de début** s'affichent.

Stratégie de sauvegarde Windows

Pour configurer une stratégie de sauvegarde Windows, effectuez les opérations suivantes :

- 1 Dans la console Core, allez à **Appliance > Sauvegarde**.
- 2 Cliquez sur le bouton **Configurer une stratégie**.
La fenêtre **Stratégie de sauvegarde Windows** s'affiche.



- 3 Entrez les paramètres décrits ci-dessous :

Zone de texte	Description

Les éléments suivants seront sauvegardés :	• Volume OS • Partition récupération • Fichiers binaires d'une récupération complète

Tous les éléments ci-dessus sont sélectionnés par défaut.

Effectuer la sauvegarde	Sélectionnez la fréquence à laquelle Winbackup doit être effectué. Vous avez le choix entre les options suivantes : Tous les jours, Toutes les semaines et Tous les mois.

Sélectionnez l'heure de programmation de la sauvegarde :	Entrez la durée pour planifier une sauvegarde.

- 4 Cliquez sur **Configurer**.
La stratégie Winbackup est configuré et les détails s'affichent dans la section **Stratégie de sauvegarde Windows**.

Une fois la configuration effectuée, l'option **Sauvegarder maintenant** vous permet de sauvegarder quand vous le voulez les éléments sélectionnés. Vous pouvez également supprimer la stratégie de sauvegarde à l'aide de **Supprimer la stratégie** dans la section **Stratégie de**

Windows Backup Policy

➤ Backup now

🗑 Delete

⚙ Configure

Backup destination:

F:\

Perform backup:

Daily

At time:

1:00 PM

The following items will be backed up:

✓ \\?\Volume{924da6dc-49be-11e6-80be-806e6f6e6963}\

✓ C:\

✓ System state

✓ Bare metal recovery

sauvegarde Windows.

Provisionnement du stockage

L'appliance configure pour les éléments suivants le stockage interne disponible et tous les boîtiers de stockage externe connectés :

- Référentiels\
- Volumes de disques pour VM de secours ou pour une autre utilisation

Avant de commencer à provisionner le stockage sur le disque, déterminez la quantité de stockage que vous souhaitez allouer aux machines virtuelles de secours. Vous pouvez allouer à ces machines virtuelles n'importe quel pourcentage de la capacité disponible restant après la création du référentiel Rapid Recovery. Par exemple, si vous utilisez SRM (Storage Resource Management), vous pouvez allouer jusqu'à 100 % de la capacité de stockage restante après la création du référentiel Rapid Recovery. L'espace peut être alloué pour des VM de secours uniquement sur les appliances provisionnées sur des machines virtuelles hôtes. La fonction Live Recovery de Rapid Recovery vous permet d'utiliser ces machines virtuelles pour remplacer rapidement un serveur défaillant protégé par l'appliance.

Sur la base d'un environnement de taille moyenne qui ne nécessite aucune machine virtuelle de secours, vous pouvez utiliser l'intégralité du stockage pour sauvegarder un nombre significatif d'agents. Toutefois, si vous avez besoin de davantage de ressources pour les VM de secours et que vous sauvegardez moins de machines d'agent, vous pouvez allouer plus de ressources aux VM de plus grande taille.

Lorsque vous sélectionnez l'onglet **Provisionnement > de l'appliance**, le logiciel Rapid Recovery repère l'espace de stockage disponible sur l'ensemble des contrôleurs pris en charge dans le système et vérifie que le matériel répond aux conditions requises.

Pour effectuer le provisionnement de disque pour tout le stockage disponible :

- 1 Cliquez sur **Provisionnement > de l'appliance**.
L'écran **Provisionnement** affiche les sections **Référentiels** et **Volumes de stockage**.
⚠ PRÉCAUTION : Avant de continuer, s'assurer que les étapes 2 à 4 sont suivies dans cette procédure.
- 2 Provisionnez du stockage disponible pour créer :
 - Référentiel
 - Volumes de disques pour VM de secours ou pour une autre utilisation
- 3 Pour créer un référentiel :
 - a Dans la page **Provisionnement**, section **Référentiels**, cliquez sur **Ajouter un nouveau référentiel**.
La boîte de dialogue **Ajouter un nouveau référentiel** s'affiche.
 - b Entrez les informations de configuration telles que décrites dans le tableau suivant.

Tableau 56. Provisionnement du stockage

Zone de texte	Description
Nom de référentiel	Entrez le nom d'affichage du référentiel. Par défaut, cette zone de texte contient le mot Référentiel et un numéro, qui correspond au nombre de référentiels de ce core. Par exemple, s'il s'agit du deuxième référentiel, son nom par défaut est Référentiel 2. Modifiez le nom si nécessaire.

Zone de texte	Description
	Les noms doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas de caractères ou d'expressions interdits. Pour plus d'informations à ce sujet, reportez-vous aux rubriques « Caractères interdits » et « Expressions interdites » dans le manuel <i>Dell Data Protection Rapid Recovery 6.0 – Guide d'utilisation</i> .
Contrôleur	Sélectionnez le contrôleur de stockage approprié selon que vous créez le référentiel sur un stockage interne ou sur un boîtier de stockage à connexion directe.
Enceinte	Sélectionnez le boîtier de stockage appropriés.
Type RAID	Sélectionnez le niveau de RAID approprié. Vous avez le choix parmi les options suivantes pour la configuration du RAID : 1, 5 ou 6.

REMARQUE : Votre système vous permet de créer un référentiel uniquement dans les niveaux de RAID dans lesquels le stockage est configuré en sortie d'usine. Pour créer un référentiel dans la configuration RAID souhaitée, vous devez configurer le stockage dans le niveau de RAID souhaité. Pour configurer le stockage dans le niveau de RAID souhaité, reportez-vous à la documentation [Dell Adapters](http://www.dell.com/support/home) sur www.dell.com/support/home.

Capacité estimée Affiche la capacité estimée disponible pour la création d'un référentiel.

Espace disponible sur le contrôleur Affiche l'espace disque disponible sur le contrôleur.

Size (Taille) Entrez la taille du référentiel.

c Cliquez sur **Créer**.

Un nouveau référentiel est créé.

4 Pour créer des volumes de disque pour VM de secours ou pour une autre utilisation :

a Dans la section **Volume de stockage**, cliquez sur **Créer un volume**.

b Dans la boîte de dialogue **Créer un volume**, spécifiez les informations suivantes pour un nouveau volume de disque Nom de volume, Contrôleur, Boîtier, Type RAID et Taille.

L'espace disponible sur le contrôleur s'affiche par défaut. Vous pouvez sélectionner l'une des configurations RAID suivantes : 1, 5 ou 6.

c Cliquez sur **Créer**.

Un nouveau volume de stockage est créé.

Supprimer une allocation d'espace pour un disque virtuel

Si vous avez besoin de modifier la configuration du provisionnement, contactez le support technique. Pour savoir comment faire, reportez-vous à la section **Contacteur Dell**.

Utilitaire de récupération et de mise à jour

L'utilitaire RUU de récupération et de mise à jour est un programme d'installation tout-en-un permettant de récupérer et de mettre à jour le logiciel des appliances DL (DL1000, DL1300, DL4000 et DL4300). Il comprend le logiciel Rapid Recovery Core et les composants spécifiques à l'appliance.

RUU se compose de versions mises à jour des rôles et fonctionnalités de Windows Server, .Net 4.5.2, un fournisseur LSI, les applications DL et les logiciels OpenManage Server Administrator et Rapid Recovery Core. En outre, l'utilitaire met également à jour le contenu de RASR (Rapid Appliance Self Recovery).

- ❗ **REMARQUE :** Si vous utilisez actuellement l'une des versions AppAssure Core, la version 6.0.2.144 (ou antérieure) de Rapid Recovery Core, RUU force la mise à jour vers la version la plus récente disponible dans la charge utile. Il n'est pas possible d'ignorer cette mise à jour et celle-ci n'est pas réversible. Si vous ne souhaitez pas effectuer la mise à niveau du logiciel Core, n'exécutez pas RUU.

Mettre à niveau votre appliance

Pour mettre à niveau votre appliance, procédez comme suit :

- 1 Allez sur le portail de licences sous la section Téléchargements ou rendez-vous sur le site **support.dell.com** et téléchargez le programme d'installation de l'utilitaire RUU.
 - 2 Copiez l'utilitaire sur le bureau de l'appliance et extrayez les fichiers.
 - 3 Double-cliquez sur l'icône **launchRUU**.
 - 4 À l'invite, cliquez sur **Oui** pour confirmer que vous n'exécutez aucun des processus énumérés.
 - 5 Lorsque l'écran **Recovery and Update Utility** s'affiche, cliquez sur **Démarrer**.
 - 6 Lorsque le programme vous invite à redémarrer, cliquez sur **OK**.
Les versions mises à jour des rôles et fonctionnalités Windows Server, d' .Net 4.5.2, du fournisseur LSI, des applications DL, d'OpenManage Server Administrator et Rapid Recovery Core sont installées dans le cadre de Recovery and Update Utility. En outre, ce dernier actualise également le contenu de RASR.
- ❗ **REMARQUE :** Si vous utilisez actuellement l'une des versions AppAssure Core, la version 6.0.2.144 (ou antérieure) de Rapid Recovery Core, RUU force la mise à jour vers la version la plus récente disponible dans la charge utile. Il n'est pas possible d'ignorer cette mise à jour et celle-ci n'est pas réversible. Si vous ne souhaitez pas effectuer la mise à niveau du logiciel Core, n'exécutez pas RUU.
- 7 Si le programme vous y invite, redémarrez votre système.
 - 8 Après avoir installé tous les services et applications, cliquez sur **Continuer**.
La console Core est lancée automatiquement.

Réparation de votre appliance

Pour réparer l'appliance :

- 1 Allez sur le portail de licences sous la section Téléchargements ou rendez-vous sur le site **support.dell.com** et téléchargez le programme d'installation de l'utilitaire RUU.
 - 2 Copiez l'utilitaire sur le bureau de l'appliance et extrayez les fichiers.
 - 3 Double-cliquez sur l'icône **launchRUU**.
 - 4 À l'invite, cliquez sur **Oui** pour confirmer que vous n'exécutez aucun des processus énumérés.
 - 5 Lorsque l'écran Recovery and Update Utility s'affiche, cliquez sur **Démarrer**.
 - 6 Lorsque le programme vous invite à redémarrer, cliquez sur **OK**.
Les versions mises à jour des rôles et fonctionnalités Windows Server, d' .Net 4.5.2, du fournisseur LSI, des applications DL, d'OpenManage Server Administrator et Rapid Recovery Core sont installées dans le cadre de Recovery and Update Utility.
 - 7 Si la version qui figure dans l'utilitaire est identique à la version installée, Recovery and Update Utility vous invite à confirmer que vous souhaitez exécuter une installation de réparation. Vous pouvez sauter cette étape si vous n'avez pas besoin de réparer une installation de Rapid Recovery Core.
 - 8 Si la version qui figure dans l'utilitaire est plus récente que la version installée, Recovery and Update Utility vous invite à confirmer que vous souhaitez mettre à niveau le logiciel Rapid Recovery Core.
- ❗ **REMARQUE :** Les mises à niveau vers des versions plus anciennes de Rapid Recovery Core ne sont pas prises en charge.
- 9 Si le programme vous y invite, redémarrez votre système.
 - 10 Après avoir installé tous les services et applications, cliquez sur **Continuer**.

L'Assistant de configuration de l'appliance DL sera lancé si le système a besoin d'être à nouveau configuré après la réparation ; sinon, la console Core sera lancée.

Protection des stations de travail et des serveurs

Protection des machines

Cette section explique comment afficher, configurer et gérer les machines protégées de votre environnement Rapid Recovery.

À propos de la protection des machines avec Rapid Recovery

Pour protéger vos données à l'aide de Rapid Recovery, vous devez ajouter les stations de travail et les serveurs à protéger dans la console Core Rapid Recovery ; par exemple votre serveur Exchange, votre serveur SQL, votre serveur Linux, etc.

Vous devez installer le logiciel Agent Rapid Recovery sur toutes les machines physiques ou virtuelles à protéger sur le Core.

REMARQUE : exception à cette règle : pour protéger des machines virtuelles sur un hôte ESXi ou VMware, vous pouvez utiliser une protection sans agent. Pour en savoir plus, notamment sur les restrictions relatives à la protection sans agent, voir [Comprendre l'Instantané rapide pour Virtual](#).

Dans la console Core Rapid Recovery, à l'aide d'un Assistant Protéger une machine, vous pouvez identifier les machines à protéger. Vous pouvez effectuer les opérations suivantes :

- Vous pouvez protéger une seule machine à l'aide de l'Assistant Protéger une machine, qui se connecte à la machine correspondante à l'aide d'une adresse IP ou d'un nom d'hôte réseau. Pour en savoir plus sur la protection d'une seule machine, voir [Protéger une machine](#).
- Vous pouvez protéger un cluster réseau à l'aide de la fonction Protéger le cluster, qui se connecte au cluster et à ses nœuds à l'aide d'une adresse IP ou d'un nom d'hôte réseau.
- Vous pouvez protéger plusieurs machines simultanément à l'aide de l'Assistant Protéger plusieurs machines, qui se connecte aux machines correspondantes à l'aide de Microsoft Active Directory® ou d'un hôte ESXi ou vCenter ; ou vous pouvez spécifier les adresse IP ou le nom d'hôte réseau pour obtenir la liste des machines à saisir manuellement.

REMARQUE : Dell recommande de limiter à 50 le nombre de machines protégées simultanément, pour éviter les contraintes de ressources susceptibles de faire échouer l'opération de protection.

Lorsque vous identifiez vos exigences de protection pour une seule machine dans l'Assistant, vous pouvez spécifier les volumes à protéger. En cas de protection de plusieurs machines, tous les volumes sont protégés par défaut. (Vous pouvez modifier ce paramètre ultérieurement, machine par machine).

L'Assistant permet également de définir un programme de protection personnalisé (ou de réutiliser une planification existante).

À l'aide des options avancées, vous pouvez ajouter des mesures de sécurité supplémentaires en spécifiant ou en appliquant une clé de chiffrement pour les sauvegardes des machines à protéger.

Enfin, en l'absence de logithèque, vous pouvez en définir une à l'aide de l'Assistant.

Une fois le logiciel Agent installé, chaque machine doit être redémarrée.

Pour en savoir plus sur la protection des stations de travail et des serveurs, voir [Protéger une machine](#).

⚠ PRÉCAUTION : Rapid Recovery ne prend pas en charge les restaurations bare metal restore (BMR) des machines Linux comprenant des partitions d'amorçage ext2. Toute BMR effectuée sur une machine présentant ce type de partition va empêcher le démarrage de la machine. Si vous souhaitez effectuer une restauration BMR sur une machine Linux incluant une partition de démarrage ext2, vous devez convertir celle-ci en partition ext3 ou ext4 avant d'initier la protection et la sauvegarde de la machine.

À propos de la protection des machines Linux avec Rapid Recovery

Le logiciel agent Rapid Recovery est compatible avec plusieurs systèmes d'exploitation Linux (pour plus de détails, voir la configuration requise incluse dans *Rapid Recovery Guide d'installation et de mise à niveau* ou *Rapid Recovery Notes de mise à jour*). Le Core Rapid Recovery est compatible uniquement avec les machines Windows. Bien que vous puissiez gérer les machines Linux protégées depuis la console Core Rapid Recovery, plusieurs procédures ont des procédures qui diffèrent pour les machines Linux, comparées à leurs équivalents Windows. De plus, vous pouvez effectuer certaines opérations directement sur les machines Linux protégées à l'aide de l'utilitaire de ligne de commande `local_mount`.

📌 REMARQUE : L'utilitaire `local_mount` était auparavant appelé `aamount`.

À propos de la gestion des serveurs Exchange et SQL dans le Rapid Recovery Core

Les options spécifiques aux serveurs Exchange et SQL ne s'affichent dans la Rapid Recovery Core Console que lorsqu'une instance du logiciel et les fichiers associés sont détectés sur les serveurs protégés. Dans ce cas, des options additionnelles sont disponibles lorsque vous sélectionnez la machine protégée dans la Core Console.

Par exemple, si vous sélectionnez un serveur Exchange protégé dans le menu de navigation de gauche, l'option de menu déroulant **Exchange** s'affichera dans les options de menu de cette machine protégée.

Si vous sélectionnez un serveur SQL protégé dans le menu de navigation de gauche, le menu déroulant **SQL** s'affichera dans les options de menu de cette machine protégée.

Ces options peuvent fonctionner différemment, mais partagent des points communs. Vous pouvez accomplir les fonctions suivantes pour les serveurs Exchange et SQL protégés (exclusivement) :

- **Forçage de la troncature des journaux de serveur.** Les serveurs SQL et Exchange contiennent des journaux serveur. Le processus de troncature des journaux SQL identifie l'espace disponible sur le serveur. Lorsque vous tronquez les journaux d'un serveur Exchange, le processus identifie l'espace disponible, mais il libère également plus d'espace sur le serveur.
- **Définition des informations d'identification du serveur approprié.** Les serveurs Exchange vous permettent de définir les informations d'identification de la machine protégée sur la page Synthèse du serveur protégé. Les serveurs SQL permettent de définir des informations d'identification pour un serveur SQL protégé ou de définir des informations d'identification par défaut pour tous les serveurs SQL protégés.
- **Affichage de l'état des vérifications des points de restauration sur un serveur Exchange ou SQL.** Les points de restauration enregistrés sur un serveur SQL ou Exchange protégé disposent d'indicateurs d'état colorés qui signalent la réussite ou l'échec des différentes vérifications associées aux serveurs SQL ou Exchange.

Cette section porte sur les rubriques suivantes de gestion des machines protégées qui utilisent un serveur Exchange ou SQL :

- [Comprendre les indicateurs d'état des points de restauration](#)
- [Paramètres et fonctions des serveurs Exchange protégés](#)
- [Paramètres et fonctions des serveurs SQL protégés](#)

À propos de la protection des clusters de serveurs

Dans Rapid Recovery, la protection des clusters de serveur est associée aux machines protégées par Rapid Recovery installées sur des nœuds de cluster individuels (c'est-à-dire des machines individuelles dans le cluster) et au Core Rapid Recovery protégeant ces machines, comme s'il s'agissait d'une seule machine composite.

Vous pouvez configurer facilement un Core Rapid Recovery de sorte qu'il protège et gère un cluster. Dans Core Console, un cluster est organisé en tant qu'entité séparée qui fait office de conteneur contenant les nœuds associés. Par exemple, dans le menu **Machines protégées** de la zone de navigation de gauche, les clusters protégés sont répertoriés. Directement, sous chaque cluster, figurent les machines agent et les nœuds associés. Chacun d'entre eux est une machine protégée sur laquelle le logiciel Agent Rapid Recovery est installé. Si vous cliquez sur le cluster, la page **Synthèse** de ce cluster s'affiche dans la console Core.

Au niveau du Core et du cluster, vous pouvez afficher les informations concernant le cluster, telles que la liste des nœuds associés et les volumes partagés. Lorsque vous consultez les informations d'un cluster dans la console Core, vous pouvez cliquer sur **Nœuds protégés** dans le menu de navigation principal pour afficher un tableau récapitulatif des nœuds individuels du cluster. À partir de ce tableau récapitulatif, pour chaque nœud, vous pouvez exécuter différentes fonctions : forcer un instantané, effectuer une exportation ponctuelle ou configurer un disque de secours virtuel, monter ou afficher des points de restauration, lancer une restauration à partir d'un point de restauration, convertir le nœud de cluster sur sa machine protégée ou encore retirer la protection du nœud. S'il s'agit d'un nœud Exchange ou SQL Server, l'option de troncature des journaux s'affiche également.

Au niveau du cluster, vous pouvez également afficher les métadonnées de cluster Exchange et SQL correspondant aux nœuds dans le cluster. Vous pouvez spécifier des paramètres pour l'ensemble du cluster et pour les volumes partagés qu'il contient.

Si vous cliquez sur n'importe quel nœud du cluster dans le menu de navigation de gauche, les informations affichées dans la console Core concernent spécifiquement ce nœud du cluster. Vous pouvez afficher des informations relatives à ce nœud, ou configurer les paramètres de ce nœud en particulier.

Prise en charge des volumes partagés au sein d'un cluster

Dans la version 6.x de la Rapid Recovery, la prise en charge des volumes partagés au sein d'un cluster (CSV) est limitée à une sauvegarde native des CSV fonctionnant sous Windows Server 2008 R2. Vous pouvez également restaurer ces CSV depuis un point de récupération, ou effectuer une exportation virtuelle vers un CSV Hyper-V fonctionnant sous Windows Server 2008 R2. Il est impossible d'effectuer une exportation virtuelle d'un volume partagé au sein d'un cluster. Une des nouveautés de la version 6.0.1 et ultérieure de la Rapid Recovery est la capacité à effectuer des exportations virtuelles vers un CSV Hyper-V fonctionnant sous Windows Server 2012 ou Windows Server 2012 R2.

❗ REMARQUE : la fonctionnalité sans agent d'Hyper-V est uniquement compatible avec Windows Server 2012 R2 ou ultérieur.

Pour les autres systèmes d'exploitation, le service d'Agent de la Rapid Recovery peut être exécuté sur n'importe quel nœud d'un cluster et ce dernier peut être protégé en tant que tel depuis le Noyau de la Rapid Recovery. Cependant, les CSV ne s'affichent pas dans la console du Noyau et ne sont pas disponibles pour protection. Au contraire, tous les disques locaux (tel que le volume hébergeant le système d'exploitation) le sont.

Le tableau suivant présente la prise en charge actuelle du Noyau de la Rapid Recovery pour les volumes partagés au sein d'un cluster.

Tableau 57. Prise en charge de la Rapid Recovery pour les volumes partagés au sein d'un cluster

Prise en charge de la Rapid Recovery pour les volumes partagés au sein d'un cluster	Protection, réplication, cumul, montage, archivage	Restauration des CSV	Exportation virtuelle vers un CSV Hyper-V
Rapid Recovery	6.0	6.0	6.0.x
Windows Server 2008 R2	Oui	Oui	Oui
Windows Server 2012	Non	Non	Oui

Prise en charge de la Rapid Recovery pour les volumes partagés au sein d'un cluster	Protection, réplication, cumul, montage, archivage	Restauration des CSV	Exportation virtuelle vers un CSV Hyper-V
Windows Server 2012 R2	Non	Non	Oui

¹ Exclut la fonctionnalité sans agent d'Hyper-V, uniquement compatible avec Windows Server 2012 R2 et ultérieur.

Bien que la Rapid Recovery vous permette de protéger d'autres systèmes d'exploitation présents sur les volumes partagés au sein d'un cluster, cette opération s'effectue à vos risques et périls. Seules les configurations présentées dans le tableau ci-dessus sont prises en charge par Dell.

Prise en charge des volumes dynamiques et des volumes de base

Rapid Recovery permet de créer des snapshots de tous les volumes dynamiques et de base. Rapid Recovery permet également d'exporter les volumes dynamiques simples qui se trouvent sur un seul disque physique. Comme leur nom l'indique, les volumes dynamiques simples ne sont pas agrégés par bandes, mis en miroir, fractionnés, ni montés en RAID.

Le comportement lors de l'exportation virtuelle de disques dynamiques diffère selon que le volume à exporter est protégé par le logiciel Agent Rapid Recovery ou est une machine virtuelle (VM) utilisant la protection sans agent. En effet, les volumes dynamiques complexes comportent des géométries de disque arbitraires que l'Agent Rapid Recovery ne peut interpréter entièrement.

Lorsque vous tentez d'exporter un disque dynamique complexe sur une machine à l'aide du logiciel Agent Rapid Recovery, l'interface utilisateur affiche un message d'alerte indiquant que les exportations sont limitées aux volumes dynamiques simples. Si vous tentez d'exporter autre chose qu'un volume dynamique simple avec l'Agent Rapid Recovery, la tâche d'exportation échoue.

En revanche, les volumes dynamiques de machines virtuelles protégées sans agent prennent en charge la protection, l'exportation virtuelle, la restauration des données, la récupération complète et le stockage de logithèque (avec des restrictions importantes). Par exemple :

- **Protection :** si un volume dynamique est fractionné sur plusieurs disques, vous devez protéger l'ensemble de ces disques pour préserver l'intégrité du volume.
- **Exportation virtuelle :** vous pouvez exporter des volumes dynamiques complexes agrégés par bandes, mis en miroir, fractionnés ou montés en RAID sur un hôte ESXi protégé sans agent.
Cependant, les volumes sont exportés à partir du disque et ne sont pas analysés. Par exemple, si vous exportez un volume dynamique fractionné sur deux disques, l'exportation comportera deux volumes de disques distincts.

 **PRÉCAUTION :** Lorsque vous exportez un volume dynamique fractionné sur plusieurs disques, vous devez exporter les disques dynamiques et les volumes système d'origine afin de préserver les types de disques.

- **Restauration des données :** lorsque vous restaurez les données d'un volume dynamique fractionné sur plusieurs disques, vous devez restaurer les disques dynamiques et les volumes système d'origine afin de préserver les types de disques. Si vous ne restaurez qu'un seul disque, la configuration des disques sera effacée.

Stockage de logithèque : en outre, Rapid Recovery prend en charge la création de logithèques sur des volumes dynamiques complexes (agrégés par bandes, mis en miroir, fractionnés ou montés en RAID). Le système de fichiers de la machine qui héberge la logithèque doit être formaté en NTFS ou en ReFS.

Compréhension du programme d'installation du logiciel Agent Rapid Recovery

Rapid Recovery permet de télécharger des programmes d'installation depuis le Core Rapid Recovery. Sur la page **Téléchargements**, vous pouvez choisir de télécharger le programme d'installation du logiciel Agent, l'utilitaire de montage local (Local Mount Utility) ou un fichier MIB SNMP. Pour en savoir plus sur l'utilitaire LMU, voir [Utilitaire Local Mount Utility \(LMU\)](#). Pour en savoir plus sur le protocole SNMP, voir [Compréhension des paramètres SNMP](#).

❶ **REMARQUE :** pour accéder au programme d'installation de l'agent, voir [Téléchargement du programme d'installation du logiciel agent de Rapid Recovery](#). Pour en savoir plus sur le déploiement du programme d'installation de l'agent, voir le guide d'installation et de mise à niveau *Dell Data Protection | Rapid Recovery*.

Le programme d'installation de l'agent permet d'installer l'application Agent Rapid Recovery sur les machines devant être protégées par le Core Rapid Recovery. Si vous estimez que l'une de vos machines nécessite le programme d'installation de l'agent, vous pouvez télécharger le programme d'installation Web sur la page Téléchargements de la console Core Rapid Recovery.

❶ **REMARQUE :** le téléchargement du Core s'effectue sur le Portail des licences Dell Data Protection | Rapid Recovery. Pour télécharger le programme d'installation du Core Rapid Recovery, visitez la page <https://licenseportal.com>. Pour en savoir plus, voir le guide d'utilisation du *Portail des licences Dell Data Protection | Rapid Recovery*.

Téléchargement du programme d'installation du logiciel agent de Rapid Recovery

Téléchargez le programme d'installation du logiciel agent de Rapid Recovery et déployez-le sur les machines que vous souhaitez protéger sur le Core de Rapid Recovery. Effectuez cette procédure pour télécharger le programme d'installation Web.

- 1 Pour télécharger le programme d'installation web de l'agent directement à partir de la machine que vous souhaitez protéger, effectuez les opérations suivantes :
 - a Dans un navigateur web, ouvrez le Portail des licences Dell Data Protection | Rapid Recovery sur <https://licenseportal.com>.
 - b Dans le menu de navigation de gauche, cliquez sur **Téléchargements**.
 - c Dans le volet **Applications Windows**, faites défiler jusqu'à la ligne **Agent Windows**, puis cliquez sur **Télécharger** sur le programme d'installation adapté (systèmes 32 bits ou 64 bits).
Le fichier du programme d'installation, par exemple `Agent-X64-6.0.1.xxxx.exe`, est enregistré dans le dossier de destination des téléchargements.
- 2 Pour télécharger le programme d'installation web depuis le Core, dans la barre des icônes de la console Core, cliquez sur l'icône **Plus** et sélectionnez **Téléchargements**. 
- 3 Sur la page **Téléchargements**, dans le volet **Agent**, cliquez sur **Télécharger le programme d'installation web**.
- 4 Dans la boîte de dialogue **Ouverture de l'Agent-Web.exe**, cliquez sur **Enregistrer le fichier**.
Le fichier du programme d'installation, par exemple `Agent-X64-6.0.1.xxxx.exe`, est enregistré dans le dossier de destination des téléchargements.
- 5 Déplacez le programme d'installation sur la machine appropriée et installez le logiciel agent Rapid Recovery.
Pour obtenir plus d'informations sur l'installation du logiciel agent de Rapid Recovery, reportez-vous au *Guide d'installation et de mise à niveau de Rapid Recovery*.

Déploiement simultané d'Agent sur plusieurs machines depuis la console Core

Vous pouvez déployer le logiciel Rapid Recovery Agent simultanément sur plusieurs machines Windows. Les machines peuvent faire partie d'un domaine Active Directory, de vCenter ou d'un hôte virtuel ESX(i). Elles peuvent également être déjà protégées par le core Rapid Recovery local (cas d'une mise à niveau du logiciel Rapid Recovery Agent. Vous avez également la possibilité de déployer manuellement le logiciel vers des machines qui ne sont pas nécessairement associées à un domaine ou à un hôte spécifique.

Vous pouvez également déployer manuellement le logiciel Rapid Recovery Agent vers une ou plusieurs machines Linux à partir de la console Core.

⚠ **PRÉCAUTION :** Si AppAssure Agent avait été précédemment installé sur une machine Linux, avant d'installer Rapid Recovery Agent, retirez AppAssure Agent de la machine à l'aide d'un script de shell. Pour plus d'informations sur le retrait de l'agent à partir d'une machine Linux, reportez-vous à la rubrique [Désinstallation du logiciel AppAssure Agent d'une machine Linux](#). Pour parvenir à déployer le logiciel Agent sur des machines Linux, reportez-vous à la rubrique [À propos de l'installation du logiciel Agent sur des machines Linux](#). Ces rubriques se trouvent dans le manuel *Dell Data Protection | Rapid Recovery – Guide d'installation et de mise à niveau*.

Déployer le logiciel Rapid Recovery Agent ne suffit pas à protéger les machines automatiquement. Après le déploiement, vous devrez sélectionner l'option **Protéger plusieurs machines** dans la barre de boutons de la console Core.

REMARQUE : La fonctionnalité de déploiement simultané vers plusieurs machines était précédemment désignée sous le nom de “déploiement en masse”. La fonctionnalité de protection simultanée de plusieurs machines était précédemment désignée sous le nom de “protection en masse”.

Pour déployer et protéger simultanément plusieurs machines, vous devez effectuer les tâches suivantes :

- Déployer Rapid Recovery Agent sur plusieurs machines. Voir [Déploiement du logiciel Agent Rapid Recovery sur une ou plusieurs machines](#).
- Surveiller le déploiement. Voir [Vérifier le déploiement sur plusieurs machines](#).
- Protéger plusieurs machines. Voir [À propos de la protection de plusieurs machines](#).

REMARQUE : Si, au cours du déploiement, vous avez sélectionné l'option Protéger l'ordinateur après l'installation, ignorez cette tâche.

- Surveiller l'activité de protection en masse. Voir [Surveiller la protection de plusieurs machines](#).

Déploiement du logiciel Agent Rapid Recovery sur une ou plusieurs machines

Vous pouvez simplifier la tâche de déploiement du logiciel Agent Rapid Recovery grâce à l'Assistant de déploiement du logiciel Agent.

REMARQUE : cette fonction était autrefois désignée en tant que « déploiement de masse ».

Lorsque vous utilisez l'Assistant de déploiement du logiciel Agent, Rapid Recovery peut détecter automatiquement les machines d'un hôte et vous permet de sélectionner les machines sur lesquelles vous souhaitez effectuer un déploiement. Pour les machines se trouvant sur des domaines ou des hôtes autres qu'Active Directory, vCenter ou ESX(i), vous pouvez vous connecter manuellement à des machines individuelles à l'aide de leurs adresses IP et des informations d'identification appropriées. Vous pouvez également diffuser des mises à niveau du logiciel sur des machines déjà protégées par le Core Rapid Recovery.

Dans la console Core, vous pouvez effectuer l'une des tâches suivantes :

- Déployer sur des machines d'un domaine Active Directory
- Déployer sur des machines d'un hôte virtuel VMware vCenter/ESX(i)
- Déploiement d'une mise à niveau du logiciel agent Rapid Recovery sur des machines protégées
- Déploiement manuel sur des machines

REMARQUE : Dell recommande de limiter à 50 le nombre de machines déployées simultanément, pour éviter les contraintes de ressources susceptibles de faire échouer l'opération de déploiement.

REMARQUE : les machines cibles doivent disposer d'un accès Internet pour télécharger et installer des bits, car Rapid Recovery utilise la version Web du programme d'installation de l'agent Rapid Recovery pour déployer les composants d'installation. Si aucun accès Internet n'est disponible, utilisez la console Core pour télécharger le programme d'installation sur un support, tel qu'un lecteur USB, puis installer physiquement le logiciel sur les machines à protéger. Pour plus d'informations, voir [Téléchargement du programme d'installation du logiciel agent de Rapid Recovery](#).

Déployer sur des machines d'un domaine Active Directory

Suivez cette procédure pour déployer simultanément le logiciel agent de Rapid Recovery sur une ou plusieurs machines d'un domaine Active Directory.

Avant de démarrer cette procédure, vous devez vous munir des informations du domaine et des informations d'identification du serveur Active Directory.

- 1 Sur la console Core de Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis cliquez sur **Déployer le logiciel agent**.

L'Assistant de déploiement du logiciel agent s'ouvre.

- 2 Sur la page **Connexion** de l'Assistant, dans la liste déroulante **Source**, sélectionnez **Active Directory**.
- 3 Entrez les informations de domaine et d'identification, tel que décrit dans le tableau suivant.

Tableau 58. Informations et identifiants du domaine

Zone de texte	Description
Hôte	Nom d'hôte ou l'adresse IP du domaine Active Directory.
Nom d'utilisateur	Nom d'utilisateur utilisé pour se connecter à ce domaine, par exemple « Administrateur » (ou, si la machine est dans un domaine, [nom du domaine]\Administrateur).
Mot de passe	Mot de passe sécurisé utilisé pour se connecter au domaine.

- 4 Cliquez sur **Suivant**.
- 5 Sur la page **Machines**, sélectionnez les machines sur lesquelles vous souhaitez déployer le logiciel agent Rapid Recovery.
- 6 Si vous le souhaitez, pour redémarrer automatiquement les machines protégées après l'installation de l'agent, sélectionnez **Après l'installation, redémarrer la machine automatiquement (conseillé)**.
- 7 Cliquez sur **Terminer**.
Le système vérifie automatiquement chaque machine sélectionnée.
Si Rapid Recovery détecte des problèmes au cours de la vérification automatique, l'Assistant vous redirige vers une page Avertissements, sur laquelle vous pouvez supprimer des machines de la sélection et vérifier manuellement les machines sélectionnées.
Si les machines que vous avez ajoutées passent la vérification automatique, elles apparaissent dans le volet Déployer l'agent sur les machines.
- 8 Si la page Avertissement s'affiche et que vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel agent de Rapid Recovery est déployé sur les machines spécifiées. Les machines ne sont pas encore protégées. La protection débute après avoir terminé l'étape [Protéger plusieurs machines sur un domaine Active Directory](#).

Déployer sur des machines d'un hôte virtuel VMware vCenter/ESX(i)

Suivez cette procédure pour déployer simultanément le logiciel agent de Rapid Recovery sur une ou plusieurs machines d'un hôte virtuel VMware vCenter/ESX(i).

Avant de démarrer cette procédure, vous devez disposer des informations suivantes :

- Les informations d'identification de connexion de l'hôte virtuel VMware vCenter/ESX(i).
- L'emplacement de l'hôte.
- Les informations d'identification de connexion de chaque machine que vous souhaitez protéger.

REMARQUE : Les outils VMware doivent être installés sur toutes les machines virtuelles. Dans le cas contraire, Rapid Recovery ne peut pas détecter le nom de l'hôte de la machine virtuelle sur laquelle le déploiement doit être effectué. Au lieu du nom de l'hôte, Rapid Recovery utilise le nom de la machine virtuelle, ce qui peut causer des problèmes si le nom de l'hôte est différent du nom de la machine virtuelle.

- 1 Sur la console Core de Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis cliquez sur **Déployer le logiciel agent**.
L'**Assistant de déploiement du logiciel agent** s'ouvre.
- 2 Sur la page **Connexion** de l'Assistant, dans la liste déroulante **Source**, sélectionnez **vCenter / ESX(i)**.
- 3 Entrez les informations de l'hôte et les informations d'identification de connexion, tel que décrit dans le tableau suivant.

Tableau 59. Paramètres de connexion vCenter/ESX(i)

Zone de texte	Description
Hôte	Nom ou adresse IP de l'hôte virtuel VMware vCenter/ESX(i).
Port	Numéro de port utilisé pour la connexion à l'hôte virtuel.

Zone de texte	Description
	Le paramètre par défaut est 443.
Nom d'utilisateur	Nom d'utilisateur utilisé pour se connecter à l'hôte virtuel, par exemple « Administrateur » (ou, si la machine est dans un domaine, [nom du domaine]\Administrateur).
Mot de passe	Mot de passe utilisé pour se connecter à cet hôte virtuel.

- 4 Cliquez sur **Suivant**.
- 5 Sur la page **Machines** de l'Assistant, sélectionnez l'une des options suivantes dans le menu déroulant :
 - Hôtes et clusters
 - Machines virtuelles et modèles
- 6 Développez la liste de machines, puis sélectionnez les machines virtuelles sur lesquelles vous souhaitez déployer le logiciel. Une notification s'affiche si Rapid Recovery détecte qu'une machine est hors-ligne ou que les outils VMware ne sont pas installés.
- 7 Si vous souhaitez redémarrer les machines automatiquement après le déploiement, sélectionnez **Après l'installation, redémarrer la machine automatiquement (conseillé)**.
- 8 Cliquez sur **Suivant**.
Rapid Recovery vérifie automatiquement chaque machine que vous avez sélectionnée.
- 9 Sur la page **Réglages** de l'Assistant, entrez les informations d'identification pour chaque machine selon le format suivant :hostname::username::password.
- ① **REMARQUE : Saisissez une machine par ligne.**
- 10 Cliquez sur **Terminer**.
Le système vérifie automatiquement chaque machine sélectionnée.
Si Rapid Recovery détecte des problèmes au cours de la vérification automatique, l'Assistant vous redirige vers une page Avertissements, sur laquelle vous pouvez supprimer des machines de la sélection et vérifier manuellement les machines sélectionnées. Si les machines que vous avez ajoutées passent la vérification automatique, elles apparaissent dans le volet Déployer l'agent sur les machines.
- 11 Si la page Avertissement s'affiche et que vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel agent de Rapid Recovery est déployé sur les machines spécifiées. Les machines ne sont pas encore protégées. La protection débute après avoir terminé l'étape [Protection de plusieurs machines sur un hôte virtuel ESX\(i\)/ VMware vCenter](#).

Déploiement d'une mise à niveau du logiciel agent Rapid Recovery sur des machines protégées

Vous pouvez utiliser l'Assistant de déploiement du logiciel agent pour placer une mise à niveau du logiciel agent Rapid Recovery sur des machines qui sont déjà protégées par le Core local de Rapid Recovery.

- 1 Sur la console Core de Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis cliquez sur **Déployer le logiciel agent**.
L'**Assistant de déploiement du logiciel agent** s'ouvre.
- 2 Sur la page **Connexion** de l'Assistant, dans la liste déroulante **Source**, sélectionnez **Core local**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Machines** de l'Assistant, sélectionnez les machines protégées sur lesquelles vous souhaitez déployer une mise à niveau du logiciel agent Rapid Recovery.
- 5 Cliquez sur **Terminer**.
Le système vérifie automatiquement chaque machine sélectionnée.
Si Rapid Recovery détecte des problèmes au cours de la vérification automatique, l'Assistant vous redirige vers une page **Avertissements**, sur laquelle vous pouvez supprimer des machines de la sélection et vérifier manuellement les machines sélectionnées. Si les machines que vous avez ajoutées passent la vérification automatique, elles apparaissent dans le volet **Déployer l'agent sur les machines**.
- 6 Si la page **Avertissement** apparaît et que vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Déploiement manuel sur des machines

Utilisez la procédure suivante pour déployer l'agent Rapid Recovery sur plusieurs machines de tout type d'hôte, autre que le Core local, Active Directory ou vCenter/ESXi.

- 1 Sur la console Core de Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis sélectionnez **Déployer le logiciel agent**.
L'**Assistant de déploiement du logiciel agent** s'ouvre.
- 2 Sur la page **Connexion** de l'Assistant, sélectionnez **Manuellement** dans la liste déroulante **Source**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Machines** de l'Assistant, saisissez les détails de la machine dans la boîte de dialogue, au format `hostname::username::password::port`. Voici des exemples :
`10.255.255.255::administrator::&11@yYz90z::8006`
`abc-host-00-1::administrator::99!zU$083r::168`
- 5 Si vous souhaitez redémarrer les machines automatiquement après le déploiement, sélectionnez **Après l'installation, redémarrer la machine automatiquement (conseillé)**.
- 6 Cliquez sur **Terminer**.
Le système vérifie automatiquement chaque machine sélectionnée.
Si Rapid Recovery détecte des problèmes au cours de la vérification automatique, l'Assistant vous redirige vers une page **Avertissements**, sur laquelle vous pouvez supprimer des machines de la sélection et vérifier manuellement les machines sélectionnées.
Si les machines que vous avez ajoutées passent la vérification automatique, elles apparaissent dans le volet **Déployer l'agent sur les machines**.
- 7 Si la page **Avertissement** apparaît et que vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel agent de Rapid Recovery est déployé sur les machines spécifiées. Les machines ne sont pas encore protégées. La protection débute après avoir terminé l'étape [Protection manuelle de plusieurs machines](#).

Vérifier le déploiement sur plusieurs machines

Après avoir déployé le logiciel Agent Rapid Recovery sur deux machines ou plus, vous pouvez déterminer si l'opération a réussi en affichant chaque machine répertoriée dans le menu Machines protégées.

Vous pouvez également afficher des informations concernant le processus de déploiement en masse sur la page Événements. Suivez la procédure ci-dessous pour vérifier le déploiement.

- 1 Accédez à la console Core Rapid Recovery, cliquez sur  (Événements), puis sur **Alertes**.
Des événements d'alertes apparaissent dans la liste, indiquant l'heure à laquelle l'événement a été initié, accompagnée d'un message.
Pour chaque déploiement réussi du logiciel Agent, vous voyez une alerte indiquant que la machine protégée a été ajoutée.
- 2 Vous pouvez cliquer sur n'importe lequel des liens d'une machine protégée.
La page **Synthèse** de la machine sélectionnée s'affiche, en fournissant des informations pertinentes, telles que :
 - Le nom de l'hôte de la machine protégée.
 - Le dernier instantané, le cas échéant.
 - L'heure du prochain instantané planifié, selon la planification de protection de la machine sélectionnée
 - La clé de chiffrement éventuellement utilisée pour cette machine protégée.
 - La version du logiciel Agent.

Modifier les paramètres de déploiement

Effectuez cette procédure pour modifier les paramètres de déploiement.

- 1 À partir de la console Core de Rapid Recovery, cliquez sur  (Paramètres).
- 2 Sur la page **Paramètres**, dans la colonne de gauche, cliquez sur **Déployer** pour accéder à la section Déployer.
- 3 Modifiez l'une des options suivantes en cliquant sur le paramètre que vous souhaitez modifier afin de le rendre modifiable sous forme de zone de texte ou liste déroulante, puis cliquez sur  pour enregistrer le paramètre.

Tableau 60. Options de déploiement

Option	Description
Nom du programme d'installation de l'agent	Entrez le nom du fichier exécutable de l'agent. La valeur par défaut est Agent-web.exe.
Adresse du Core	Entrez l'adresse du Core.
Réception impossible, expiration du délai	Entrez le nombre de minutes d'inactivité qui doivent s'écouler avant l'expiration.
Nombre maximal d'installations parallèles	Entrez le nombre maximal d'installations que vous souhaitez installer simultanément. La valeur par défaut et limite est 100.
Redémarrage automatique après installation	Cochez la case pour Oui, effacez-la pour Non.
Protéger après le déploiement	Cochez la case pour Oui, effacez-la pour Non.

Comprendre la planification de la protection

Une planification de protection définit le moment où les sauvegardes sont transférées des machines agent protégées vers le Core Rapid Recovery.

Le premier transfert de sauvegarde enregistré sur le Core s'appelle l'instantané d'image de base. Toutes les données de tous les volumes spécifiés (notamment sur le système d'exploitation, les applications et les paramètres), sont enregistrées sur le Core, ce qui peut prendre beaucoup de temps en fonction de la quantité de données transférée. Ensuite, des instantanés incrémentiels (des sauvegardes plus petites, comprenant uniquement les données ayant été modifiées sur la machine protégée depuis la dernière sauvegarde) sont régulièrement enregistrés sur le Core, en fonction de l'intervalle défini (par exemple, toutes les 60 minutes). Cette sauvegarde contient moins de données qu'une image de base, et peut donc être transférée plus rapidement.

Les planifications de protection sont initialement définies à l'aide de l'assistant Protéger une machine ou de l'assistant Protéger plusieurs machines. À l'aide d'un Assistant, vous pouvez personnaliser les planifications de protection (en choisissant soit des périodes, soit une heure de protection quotidienne), en fonction des besoins de votre entreprise. Vous pouvez ensuite modifier la planification existante ou créer une nouvelle planification à tout moment dans la boîte de dialogue Planification de protection de la page récapitulative d'une machine protégée spécifique.

Rapid Recovery fournit une planification de protection par défaut qui comprend une période unique englobant tous les jours de la semaine, avec une seule plage d'horaires définie (de minuit à 23 h 59). L'intervalle par défaut (la durée écoulée entre deux instantanés) est de 60 minutes. En activant la protection pour la première fois, vous activez également la planification. Ainsi, en utilisant les paramètres par défaut, quelle que soit l'heure de la journée, la première sauvegarde se produit toutes les heures, au début de chaque heure (minuit, 1 h 00, 2 h 00, etc.).

Le fait de choisir des périodes permet d'afficher la planification de protection par défaut et d'effectuer des réglages en conséquence. Si vous sélectionnez une heure de protection quotidienne, le Core Rapid Recovery sauvegarde les machines protégées désignées une fois par jour à l'heure spécifié.

Vous pouvez personnaliser la planification pour définir des heures pleines et des heures creuses, à partir des périodes de jours ouvrables et de week-ends disponibles. Par exemple, si vos machines protégées sont principalement utilisées les jours ouvrables, vous pouvez réduire à 20 minutes l'intervalle de la période des jours ouvrables. Dans ce cas, trois instantanés sont créés toutes les heures. Inversement, vous pouvez décider de faire passer l'intervalle des week-ends de 60 minutes à 180 minutes pour créer des instantanés toutes les trois heures lorsque le trafic est faible.

Sinon, vous pouvez modifier la planification par défaut pour définir des horaires quotidiens de trafic élevé ou faible. Pour ce faire, modifiez les heures de début et de fin par défaut pour réduire la plage horaire (par exemple, de minuit à 16 h 59), puis définissez un intervalle approprié (par exemple, toutes les 20 minutes). Cela correspond à des sauvegardes fréquentes pendant les heures de fort trafic. Vous pouvez ensuite ajouter une plage horaire de jours ouvrables supplémentaire pour la période restante (de 17 h 00 à 23 h 59) et définir l'intervalle approprié (a priori plus long), par exemple de 180 minutes. Ces paramètres définissent une période creuse entre 17 h 00 à minuit tous les jours. Cette personnalisation entraîne la création d'instantanés toutes les trois heures de 17 h 00 à 23 h 59, et toutes les 20 minutes de minuit à 16 h 59.

Lorsque vous modifiez ou créez une planification de protection à l'aide de la boîte de dialogue Planification de protection, Rapid Recovery vous donne la possibilité d'enregistrer cette planification en tant que modèle réutilisable, que vous pouvez ensuite appliquer à d'autres machines protégées.

Les autres options des Assistants de protection permettent de définir une heure de protection quotidienne. Dans ce cas, une seule sauvegarde est créée à l'heure définie (le paramètre par défaut est 12 h 00).

Lorsque vous protégez une ou plusieurs machines à l'aide d'un Assistant, vous pouvez suspendre initialement la protection, ce qui permet de définir la planification de protection sans protéger les machines. Lorsque vous êtes prêt à protéger les machines selon les planifications de protection établies, vous devrez reprendre la protection explicitement. Pour en savoir plus sur la reprise de la protection, voir [Suspendre et reprendre la protection](#). Éventuellement, si vous voulez protéger une machine immédiatement, vous pouvez forcer un instantané. Pour plus d'informations, voir [Forcer un instantané](#).

Protéger une machine

Si vous avez déjà installé le logiciel Rapid Recovery Agent sur la machine à protéger, mais que vous n'avez pas encore redémarré cette dernière, c'est le moment de le faire.

Cette rubrique explique comment, à l'aide de l'Assistant de protection de machines, démarrer la protection des données sur la machine que vous spécifiez.

REMARQUE : Sauf dans les cas où vous utilisez une protection sans agent sur un hôte VMware ou ESXi, le logiciel Rapid Recovery Agent doit être installé sur la machine à protéger. Vous pouvez choisir d'installer Agent avant cette procédure ou d'attendre de procéder à la protection de la machine cible à l'aide de l'Assistant pour y déployer le logiciel.

Pour plus d'informations sur la protection sans agent et sur ses restrictions, voir [Comprendre l'Instantané rapide pour Virtual](#).

Pour plus d'informations sur l'installation du logiciel Agent, reportez-vous à la section « Installation de Rapid Recovery Agent » du *Portail des licences Dell Data Protection | Rapid Recovery – Guide d'installation et de mise à niveau*. Si Agent n'est pas installé avant que vous procédiez à la protection de la machine, vous ne serez pas en mesure de sélectionner dans l'assistant les volumes spécifiques à protéger. Dans ce cas, par défaut, tous les volumes de la machine Agent seront inclus comme devant être protégés. Rapid Recovery prend en charge la protection et la récupération des machines configurées avec des partitions EISA. Sont également prises en charge les machines Windows 8 et 8.1 ainsi que les machines Windows 2012 et 2012 R2 qui utilisent Windows RE (Windows Recovery Environment).

Pour protéger simultanément plusieurs machines dans le même processus, voir [À propos de la protection de plusieurs machines](#).

Lorsque vous ajoutez une protection, vous devez définir des informations de connexion (adresse IP et port). Vous devez également fournir les informations d'identification permettant de se connecter à la machine à protéger. Si vous le souhaitez, vous pouvez aussi indiquer le nom d'affichage à utiliser sur la console Core à la place de l'adresse IP de la machine. Dans ce cas, vous ne verrez plus l'adresse IP de la machine protégée lorsque vous afficherez les détails sur la console Core. Vous devrez enfin définir un calendrier de planification pour la protection de la machine.

Le processus de protection inclut des étapes facultatives qui vous seront proposées si vous sélectionnez une configuration avancée : fonctions et chiffrement du référentiel. Par exemple, vous pourrez spécifier un référentiel Rapid Recovery existant pour enregistrer des instantanés ou vous pourrez créer un nouveau référentiel. Vous pourrez également spécifier une clé de chiffrement existante (ou en ajouter une nouvelle) à appliquer aux données enregistrées sur le core pour cette machine. Pour plus d'informations sur les clés de chiffrement, voir [Comprendre les clés de chiffrement](#).

Le workflow de l'assistant de protection peut varier légèrement en fonction de votre environnement. Par exemple, si le logiciel Rapid Recovery Agent est installé sur la machine à protéger, vous ne serez pas invité à l'installer à partir de l'assistant. De même, si un référentiel existe déjà sur le core, vous ne serez pas invité à en créer un.

PRÉCAUTION : Rapid Recovery ne prend pas en charge les restaurations sans système d'exploitation (BMR) de machines Linux à partitions d'amorçage ext2. Toute restauration BMR effectuée sur une machine disposant de ce type de partition produit une machine qui ne démarre pas. Si vous voulez être en mesure d'effectuer à l'avenir une restauration BMR sur cette machine, vous devez convertir les partitions ext2 en ext3 ou ext4 avant de commencer à protéger et sauvegarder la machine.

1 Effectuez l'une des opérations suivantes :

- Si vous procédez à partir de l'Assistant de protection de machines, passez à l'[étape 2](#).
- Si vous procédez à partir de la console Core Rapid Recovery, dans la barre de boutons, cliquez sur **Protéger**.

L'**Assistant de protection de machines** s'affiche.

2 Dans la page **Accueil**, sélectionnez les options d'installation appropriée :

- Si vous n'avez pas besoin de définir un référentiel ni d'établir un chiffrement, sélectionnez **Normal**.
- Si vous avez besoin de créer un référentiel ou de définir un référentiel différent pour les sauvegardes de la machine sélectionnée, ou si vous souhaitez établir un chiffrement à l'aide de l'assistant, sélectionnez **Avancé (afficher les étapes facultatives)**.
- Le cas échéant, si vous ne souhaitez plus voir la page **Accueil** de l'Assistant de protection de machines à l'avenir, cochez l'option **Ignorer cette page d'accueil à la prochaine ouverture de l'Assistant**.

3 Lorsque vous êtes satisfait de vos choix dans la page d'accueil, cliquez sur **Suivant**.

La page **de connexion** s'affiche.

4 Dans la page **Connexion**, entrez les informations concernant la machine à laquelle vous souhaitez vous connecter (voir le tableau suivant), puis cliquez sur **Suivant**.

Tableau 61. Paramètres de connexion machine

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
Port	Le numéro du port sur lequel le core Rapid Recovery communique avec Agent sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Le nom d'utilisateur servant à se connecter à cette machine ; par exemple, Administrateur (ou, si la machine se trouve dans un domaine, [nom de domaine]\Administrateur).
Mot de passe	Le mot de passe utilisé pour se connecter à cette machine

Si la page **Installer l'agent** s'affiche ensuite dans l'Assistant de protection de machines, cela veut dire que Rapid Recovery ne détecte pas Rapid Recovery Agent sur la machine et qu'il va installer la version actuelle du logiciel. Allez à l'[étape 7](#).

Si la page **Mettre à niveau Agent** s'affiche ensuite dans l'assistant, cela veut dire qu'il existe une ancienne version du logiciel Agent sur la machine à protéger.

REMARQUE : Le logiciel Agent doit être installé sur la machine à protéger, et la machine doit être redémarrée avant de pouvoir être sauvegardée vers le core. Pour que le programme d'installation redémarre la machine protégée, sélectionnez l'option **Après l'installation, redémarrer automatiquement la machine (recommandé)** avant de cliquer sur **Suivant**.

- 5 Dans la page **Mettre à niveau Agent**, effectuez l'une des actions suivantes :
 - Pour déployer la nouvelle version du logiciel Agent (correspondant à la version du core Rapid Recovery), sélectionnez **Mettre à niveau Agent vers la dernière version du logiciel**.
 - Pour continuer la protection de la machine sans mise à jour de la version du logiciel Agent, désélectionnez l'option **Mettre à niveau Agent vers la dernière version du logiciel**.
- 6 Cliquez sur **Suivant**.
- 7 Si vous le désirez, dans la page **Protection**, si vous voulez que, pour la machine protégée, dans la console Core Rapid Recovery s'affiche un nom plus parlant que son adresse IP, dans le champ **Nom d'affichage**, entrez ce nom dans la boîte de dialogue. Vous pouvez entrer un maximum de 64 caractères. N'utilisez pas les caractères spéciaux décrits dans la rubrique [caractères interdits](#). En outre, ne faites pas commencer le nom d'affichage par l'une des combinaisons de caractères décrites dans la rubrique [expressions interdites](#).
- 8 Sélectionnez la planification de protection appropriée expliquée ci-dessous :
 - Pour utiliser la planification de protection par défaut, accédez à l'option Paramètres de planification, sélectionnez **Protection par défaut**.

Avec la planification de protection par défaut, le Core prend une fois par heure des instantanés de tous les volumes sur la machine protégée. Pour modifier les paramètres de protection à tout moment après avoir fermé l'Assistant, y compris pour le choix des volumes à protéger, accédez à la page **Résumé de la machine protégée**.

- Pour définir une planification de protection différente dans l'option Paramètres de planification, sélectionnez **Protection personnalisée**.
- 9 Effectuez la configuration comme suit :
 - Si vous avez sélectionné une configuration standard dans l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine spécifiée.
Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.
 - Si vous avez sélectionné une configuration standard pour l'Assistant de protection de machines et défini une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à [Créer des planifications de protection personnalisées](#).
 - Si vous avez sélectionné la configuration Avancée pour l'Assistant de protection d'une machine et choisi la protection par défaut, cliquez sur **Suivant** et passez à l'[étape 14](#) pour afficher les options de référentiel et de chiffrement.
 - Si vous avez sélectionné la configuration Avancée pour l'Assistant de protection de machines et spécifié la protection personnalisée, cliquez sur **Suivant** et passez à l'[étape 11](#) pour choisir les volumes à protéger.

- 10 Dans la page **Volumes de protection**, sélectionnez les volumes que vous souhaitez protéger. Si la liste contient des volumes que vous ne voulez pas inclure dans la protection, cliquez dans la colonne de cases à cocher pour effacer la sélection. Cliquez ensuite sur **Suivant**.

REMARQUE : En règle générale, il est recommandé de protéger, au minimum, le volume réservé au système et le volume contenant le système d'exploitation (généralement le lecteur C).

- 11 Dans la page **Planification de la protection**, définissez une planification de protection personnalisée et cliquez sur **Suivant**. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à [Créer des planifications de protection personnalisées](#).

Si le référentiel est déjà configuré, et que vous avez sélectionné l'option Avancé à l'étape 1, la page Chiffrement s'affiche. Passez à l'étape 13.

- 12 Dans la page **Référentiel**, les éléments suivants :

- Si vous disposez déjà d'un référentiel et que vous souhaitez y stocker les données de cette machine pour sa protection, procédez de la façon suivante :
 - 1 Sélectionnez **Utiliser un référentiel existant**.
 - 2 Sélectionnez un référentiel existant dans la liste.
 - 3 Cliquez sur **Suivant**.

La page **Chiffrement** s'affiche. Passez à l'étape 13 pour définir le chiffrement, si vous le souhaitez.

- Si vous souhaitez créer un référentiel, sélectionnez **Créer un référentiel**, puis effectuez les opérations décrites ci-après.
 - 1 Dans la page **Référentiel**, entrez les informations décrites dans le tableau suivant.

Tableau 62. Ajouter les paramètres du nouveau référentiel

Zone de texte	Description
Nom de référentiel	Entrez le nom d'affichage du référentiel. Par défaut, cette zone de texte contient le mot Repository et un numéro, qui correspond au nombre de référentiels de ce core. Par exemple, s'il s'agit du premier référentiel, son nom par défaut est Repository 1. Modifiez le nom si nécessaire. Les noms de référentiels doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas caractères interdits ni expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que votre référentiel devra prendre en charge. La valeur par défaut est 64.
Commentaires	(Optionnel) Entrez une note décrivant ce référentiel. Vous pouvez entrer jusqu'à 254 caractères. Par exemple, tapez Référentiel DVM 2 .

- 2 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.

PRÉCAUTION : Définissez un dossier dédié au sein de la racine de l'emplacement de stockage de votre référentiel. Ne spécifiez pas l'emplacement racine. Par exemple, utilisez E:\Repository\ et non E:\. Si le référentiel que vous créez à cette étape est supprimé ultérieurement, tous les fichiers de son emplacement de stockage seront supprimés. Si vous définissez votre emplacement de stockage à la racine, tous les autres fichiers dans le volume (par ex., E:\) seront également supprimés, ce qui pourrait entraîner une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.

- 3 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.
- 4 Dans la zone **Emplacement de stockage**, spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage connecté localement (par exemple en tant que stockage à connexion directe, un réseau de zone de stockage, ou un stockage connecté par réseau). Vous pouvez également spécifier un volume de stockage sur un emplacement partagé CIFS (Common Internet File System).
- Sélectionnez **Ajouter un fichier sur disque local** pour spécifier une machine locale, puis entrez les informations décrites dans le tableau suivant.

Tableau 63. Paramètres du disque local

Zone de texte	Description
Chemin de données	Entrez l'emplacement de stockage des données protégées. Par exemple, entrez X:\Repository\Data. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées. Par exemple, entrez X:\Repository\Metadata. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

- Vous pouvez également cliquer sur **Ajouter le fichier sur un partage CIFS** pour spécifier un emplacement de partage réseau, puis entrez les informations décrites dans le tableau suivant.

Tableau 64. Identifiants pour le partage CIFS

Zone de texte	Description
Chemin UNC	Entrez le chemin de l'emplacement du partage réseau. Si cet emplacement se trouve à la racine, définissez un nom de dossier dédié (par exemple, Repository). L'extension de fichier doit commencer par \\. Lorsque vous spécifiez ce chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Les lettres a à z peuvent être en majuscules ou en minuscules. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe pour accéder à l'emplacement du partage réseau.

- Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails** et entrez les détails de l'emplacement de stockage décrits dans le tableau suivant.

Tableau 65. Détails de la configuration du stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille minimale est de 1 Go. La valeur par défaut est de 250 Go. Vous pouvez choisir parmi les options suivantes : - Go - To ① REMARQUE : La taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) sous Windows XP ou Windows 7, la taille de fichier est limitée à 16 To. Si l'emplacement de stockage est un volume NTFS sous Windows 8, 8.1, Windows 10, ou Windows Server 2012, 2012 R2, la taille de fichier est limitée à 256 To.

Zone de texte	Description
	REMARQUE : Pour que Rapid Recovery puisse valider le système d'exploitation, WMI (Windows Management Instrumentation) doit être installé sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle l'utilisation du Windows Cache Manager dans le référentiel et facilite le réglage du référentiel pour des performance optimales sur différentes configurations. Définissez l'option sur une des valeurs suivantes : • Activé • Éteint • Synchroniser Si la fonction est définie comme activée (valeur par défaut), Windows contrôle la mise en cache. Cette option est appropriée pour Windows 10, et pour les versions de Windows Server 2012 et ultérieur. REMARQUE : L'activation de la stratégie de mise en cache d'écriture peut améliorer la vitesse des performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, il est recommandé de désactiver cette stratégie. Si la fonction est désactivée, c'est Rapid Recovery qui contrôle la mise en cache. Si la fonction est définie sur Synchroniser, Windows contrôle la mise en cache et les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets que devrait comprendre chaque secteur. La valeur par défaut est 512.
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

6 Cliquez sur **Suivant**.

Si vous avez choisi l'option **Avancé** à l'étape 1, la page **Chiffrement** s'affiche.

- 13 Si vous le souhaitez, dans la page **Chiffrement**, pour activer le chiffrement, sélectionnez **Activer le chiffrement**.
Les champs Clé de chiffrement apparaissent dans la page **Chiffrement**.

REMARQUE : Si vous l'activez, le chiffrement sera appliqué aux données de tous les volumes protégés de cette machine. Vous pouvez modifier ultérieurement les paramètres de chiffrement à partir de la console Core Rapid Recovery. Pour plus d'informations sur le chiffrement, reportez-vous à la rubrique [Comprendre les clés de clés de chiffrement](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining, chaînage des blocs de chiffrement) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous recommande vivement de créer une clé de clé de chiffrement et de protéger la phrase de passe que vous définissez. Stockez cette phrase de passe dans un endroit sûr, car elle est d'une importance capitale pour la restauration des données. Sans la phrase de passe, la restauration des données est impossible.

- 14 Dans la page **Chiffrement**, sélectionnez l'une des options suivantes :
- Si vous souhaitez chiffrer cette machine protégée à l'aide d'une clé de chiffrement qui est déjà définie dans ce core Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement**, puis sélectionnez la clé appropriée dans le menu déroulant. Passez à l'étape suivante.
 - Si vous souhaitez ajouter au core une nouvelle clé de chiffrement et appliquer cette clé à cette machine protégée, entrez les informations décrites dans le tableau suivant.

Tableau 66. Paramètres de clé de chiffrement

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement.

Zone de texte	Description
	Les noms de clés de chiffrement doivent contenir entre 1 et 130 caractères alphanumériques. Vous ne pouvez pas inclure de caractères spéciaux (barre oblique inverse, barre oblique normale, barre verticale, deux-points, astérisque, guillemets, point d'interrogation, parenthèse ouvrante ou fermante, et commercial, dièse).
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lors de l'affichage des clés de chiffrement dans la console Core.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès. La bonne pratique consiste à éviter d'utiliser les caractères spéciaux mentionnés ci-dessus. Notez la phrase de passe dans un endroit sûr. Le support Dell ne peut pas récupérer de phrase de passe. Une fois que vous avez créé une clé de chiffrement et que vous l'avez appliquée à une ou plusieurs machines protégées, vous ne pourrez pas restaurer les données si vous perdez la phrase de passe.
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.

- 15 Cliquez sur **Terminer** pour enregistrer et appliquer vos paramètres.

Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.

Protection d'un cluster

Cette rubrique explique comment ajouter un cluster à protéger dans Rapid Recovery. Lorsque vous ajoutez un cluster à protéger, vous devez spécifier le nom d'hôte ou l'adresse IP du cluster, l'application de cluster ou l'un des nœuds de cluster ou l'une des machines incluant le logiciel agent Rapid Recovery.

REMARQUE : une logithèque sert à stocker les instantanés capturés à partir des nœuds protégés. Avant de démarrer la protection des données dans le cluster, vous devez associer au moins une logithèque à votre Core Rapid Recovery.

Pour en savoir plus sur la configuration des logithèques, voir [Comprendre les référentiels](#).

- 1 Dans la Rapid Recovery Core Console, cliquez sur le menu déroulant **Protéger**, puis sur **Protéger le cluster**.
- 2 Dans la boîte de dialogue Connexion au cluster, saisissez les informations suivantes.

Tableau 67. Paramètres de connexion au cluster

Zone de texte	Description
Hôte	Nom d'hôte ou adresse IP du cluster, de l'application de cluster ou de l'un des nœuds de cluster.
Port	Numéro du port de la machine sur laquelle le Core Rapid Recovery communique avec l'agent. Le port par défaut est 8006.
Nom d'utilisateur	Nom d'utilisateur de l'administrateur du domaine utilisé pour se connecter à la machine (ex. : nom_de_domaine\administrateur).
	REMARQUE : le nom de domaine est obligatoire. Vous ne pouvez pas vous connecter au cluster avec le nom d'utilisateur de l'administrateur local.
Mot de passe	Mot de passe utilisé pour se connecter à cette machine.

- 3 Cliquez sur **Connexion**.
- 4 Dans la boîte de dialogue Protéger un cluster, sélectionnez une logithèque pour ce cluster.
- 5 Si vous souhaitez que les points de restauration de ce cluster soient chiffrés par le Core, sélectionnez une clé de chiffrement.

- 6 Si vous ne souhaitez pas que la protection commence immédiatement après la fin de cette procédure, sélectionnez **Suspendre initialement la protection**.
- 7 Pour protéger le cluster en fonction des paramètres par défaut, sélectionnez les nœuds de la protection par défaut, puis passez à l'étape 10.

REMARQUE : par défaut, un instantané de l'ensemble des volumes est capturé toutes les 60 minutes.

- 8 Pour entrer des paramètres personnalisés pour ce cluster (par exemple, pour personnaliser l'horaire de protection des volumes protégés), effectuez l'une des tâches suivantes, puis consultez la page [Créer des planifications de protection personnalisées](#).
 - Pour personnaliser les paramètres d'un nœud unique, cliquez sur **Paramètres** en regard du nœud à personnaliser, puis sur **Fonction** en regard du volume adéquat.
 - Pour personnaliser les paramètres du cluster, cliquez sur le bouton Paramètres au bas de la boîte de dialogue, puis sur **Fonction** en regard du volume adéquat.

Pour en savoir plus sur la personnalisation des nœuds, voir [Pour protéger les nœuds dans un cluster](#).

- 9 Lorsque vous avez effectué toutes les modifications nécessaires, cliquez sur **Enregistrer**.
- 10 Dans la boîte de dialogue Protéger un cluster, cliquez sur **Protéger**.

Modifier les paramètres de nœuds de cluster

Une fois que vous avez ajouté de la protection pour des nœuds de cluster, vous pouvez facilement modifier les paramètres de configuration de base pour ces machines/nœuds (par exemple, nom d'affichage, nom d'hôte, etc.), les paramètres de protection (par exemple, en modifiant les horaires de protection des volumes locaux sur la machine, en ajoutant ou en supprimant des volumes, et en suspendant la protection), etc.

Pour modifier les paramètres de nœuds de cluster, vous devez effectuer les tâches suivantes :

- Dans la console Core Rapid Recovery, allez au cluster qui contient le nœud que vous souhaitez modifier, puis sélectionnez la machine ou le nœud à modifier.
- Pour modifier et afficher les paramètres de configuration, voir [Configurer les groupes de notification](#).
- Pour configurer des groupes de notification pour les événements système, voir [Paramètres d'affichage et de modification des machines protégées](#).
- Pour personnaliser les paramètres de stratégie de conservation, voir [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).
- Pour modifier l'horaire de protection, voir [Modifier les planifications de protection](#).
- Pour modifier les paramètres de transfert, voir [À propos de la modification des paramètres de transfert](#).

Pour protéger les nœuds dans un cluster

Pour accomplir cette tâche, vous devez commencer par protéger un cluster. Pour plus d'informations, voir [Protection d'un cluster](#).

Cette rubrique explique comment protéger les données d'une machine ou d'un nœud de cluster sur lesquels un agent Rapid Recovery est installé. Cette procédure permet d'ajouter individuellement des nœuds pour la protection que vous auriez peut-être omis lorsque vous avez protégé un cluster.

- 1 Dans la console Core Rapid Recovery, sous Machine protégée, cliquez sur le cluster pour lequel vous souhaitez protéger les nœuds.
- 2 Sur la page Récapitulatif du cluster, cliquez sur **Nœuds protégés**.
- 3 Sur la page Nœuds protégés, cliquez sur **Protéger le nœud de cluster**.
- 4 Dans la boîte de dialogue Protéger le nœud de cluster, sélectionnez ou entrez les informations suivantes.

Tableau 68. Paramètres de la protection des nœuds de cluster

Zone de texte	Description
Hôte	Liste déroulante des nœuds du cluster disponibles à la protection.
Port	Le numéro du port sur lequel le Core Rapid Recovery communique avec l'agent sur le nœud.
Nom d'utilisateur	Nom d'utilisateur de l'administrateur de domaine utilisé pour se connecter à ce nœud, par exemple, exemple_domaine \administrateur ou administrateur@exemple_domaine.com
Mot de passe	Mot de passe utilisé pour se connecter à cette machine.

5 Pour ajouter le nœud, cliquez sur **Connexion**.

6 Pour commencer à protéger ce nœud avec les paramètres de protection par défaut, passez à l'étape 13.

REMARQUE : Les paramètres personnalisés protègent tous les volumes de la machine avec une planification ayant une fréquence 60 minutes.

7 Dans la boîte de dialogue Protéger [nom du nœud], si vous souhaitez utiliser une logithèque autre que celui par défaut, utilisez la liste déroulante.

8 Si vous voulez sécuriser les points de restauration pour ce cluster avec le chiffrement basé sur un Core, utilisez la liste déroulante pour sélectionner une clé de chiffrement.

9 Si vous ne voulez pas que la protection commence immédiatement après la fin de cette procédure, sélectionnez **Suspendre initialement la protection**.

10 Pour entrer les paramètres personnalisés (par exemple, pour personnaliser l'horaire de protection des volumes protégés), effectuez les tâches suivantes :

- Pour personnaliser les paramètres d'un seul volume, cliquez sur **Fonction** en regard du volume que vous souhaitez personnaliser.
- Voir [Créer des planifications de protection personnalisées](#).

11 Cliquez sur **Protéger**.

Créer des planifications de protection personnalisées

Exécutez la procédure ci-dessous pour créer des planifications personnalisées pour protéger les données sur les machines protégées lorsque vous définissez la protection en utilisant un assistant.

1 Sur la page **Protection** de l'Assistant (Protéger la machine, Protéger plusieurs machines, Protéger un cluster), sélectionnez Protection personnalisée.

2 Cliquez sur **Suivant**.

3 Sur la page **Volumes de protection**, sélectionnez les volumes que vous voulez protéger, puis cliquez sur **Suivant**.

4 Sur la page **Planification de protection**, pour modifier l'intervalle de planification, procédez comme suit :

a Sélectionnez **Périodes**.

Les périodes existantes s'affichent et peuvent être modifiées. Vous pouvez modifier les champs de d'heure de début, d'heure de fin et d'intervalle (en minutes) de chaque période.

b Pour chaque période, cliquez dans la zone de texte de l'intervalle et saisissez l'intervalle adapté en minutes.

Par exemple, sélectionnez l'intervalle par défaut de 60 et remplacez-le par la valeur 20 pour effectuer des instantanés toutes les 20 minutes pendant cette période.

5 Pour créer une période creuse et une période de fort trafic pendant les jours de la semaine, modifiez la plage horaire de la période de la semaine afin qu'elle ne couvre pas une période de 24 heures, définissez un intervalle optimal pour la période de fort trafic, sélectionnez **Créer des instantanés pendant les heures restantes** et définissez un intervalle pour la période creuse, en procédant comme suit :

a Sélectionnez **Périodes**.

Les périodes existantes s'affichent et peuvent être modifiées.

b Cliquez sur **De** ou utilisez l'icône de l'horloge pour modifier l'heure de début de la période.

c Cliquez sur **À** ou utilisez l'icône de l'horloge pour modifier l'heure de fin de la période.

d Cliquez dans la zone de texte de l'intervalle et saisissez l'intervalle adapté en minutes.

Par exemple, sélectionnez l'intervalle par défaut de 60 et remplacez-le par la valeur 20 pour effectuer des instantanés toutes les 20 minutes pendant l'intervalle de temps que vous avez sélectionné pour cette période.

- e Sélectionnez **Prendre des instantanés pour le reste du temps**, puis saisissez un intervalle en minutes.
- 6 Pour définir un horaire quotidien unique pour une seule sauvegarde tous les jours, cliquez sur **Horaire de protection quotidien**, puis entrez une heure dans le format HH:MM AM ou PM. Par exemple, pour effectuer une sauvegarde quotidienne à 21 h 00, entrez 09:00 PM.
- 7 Pour définir la planification sans commencer les sauvegardes, cliquez sur **Suspendre initialement la protection**.
Après avoir suspendu la protection depuis l'assistant, celle-ci reste suspendue jusqu'à ce que vous la repreniez de manière explicite. Après avoir repris la protection, les sauvegardes se produisent sur la base de la planification que vous avez définie. Pour plus d'informations sur la reprise de la protection, voir [Suspension et reprise de la protection](#).
- 8 Après avoir modifié la planification de protection, cliquez sur **Terminer** ou **Suivant**, selon le cas. Retournez à la procédure de l'assistant approprié pour terminer les étapes nécessaires.

Modifier les planifications de protection

Une planification de protection définit le moment où les sauvegardes sont transférées des machines agent protégées vers le Core Rapid Recovery. Les planifications de protection sont initialement définies à l'aide de l'assistant Protéger une machine ou de l'assistant Protéger plusieurs machines.

Vous pouvez modifier une planification de protection existante à tout moment dans l'onglet Synthèse d'une machine agent.

REMARQUE : pour obtenir des informations conceptuelles sur les planifications de protection, voir [Comprendre la planification de la protection](#). Pour en savoir plus sur la protection d'une seule machine, voir [Protéger une machine](#). Pour en savoir plus sur la protection en masse (protection de plusieurs machines), voir [À propos de la protection de plusieurs machines](#). Pour en savoir plus sur la personnalisation des périodes de protection d'un agent à l'aide de l'un de ces Assistants, voir [Créer des planifications de protection personnalisées](#). Pour en savoir plus sur la modification d'une planification de protection existante, voir [Modifier les planifications de protection](#).

Pour modifier une protection de planification existante pour les volumes d'une machine protégée, procédez comme suit.

- 1 Dans la liste des machines protégées de la console Core, cliquez sur la machine protégée incluant la planification de protection à modifier.
- 2 Sur la page de la machine choisie, sélectionnez les volumes correspondants, puis cliquez sur **Configurer la planification**.
Pour sélectionner tous les volumes simultanément, cochez la case dans la ligne d'en-tête. Initialement, tous les volumes partagent la même planification de protection.

REMARQUE : en règle générale, il est recommandé de protéger, au minimum, le volume réservé au système et le volume comportant le système d'exploitation (normalement le disque C:).

La boîte de dialogue Planification de protection s'ouvre.

- 3 Dans la boîte de dialogue Planification de protection, effectuez l'une des opérations suivantes :
 - Si vous avez déjà créé un modèle de planification de protection et que vous souhaitez l'appliquer à cette machine protégée, sélectionnez le modèle dans la liste déroulante, puis passez à l'[étape 7](#).
 - Si vous voulez supprimer une période existante de la planification, décochez les cases en regard de chacune des périodes, puis passez à l'[étape 7](#). Vous avez le choix entre :
 - Lundi-vendredi : cette période correspond à une semaine de travail standard de cinq jours.
 - Samedi-dimanche : cette période correspond à un week-end standard.
 - Si vous souhaitez enregistrer une nouvelle planification de protection en tant que modèle, passez à l'[étape 4](#).
- 4 Si les heures de début et de fin des jours de semaine sont de minuit à 23 h 59, il n'existe qu'une période. Pour modifier les heures de début et de fin d'une période, procédez comme suit :
 - a Sélectionnez la période appropriée.
 - b Pour modifier l'heure de début de cette période, utilisez l'icône en forme d'horloge, sous **Heure de début**.
Par exemple, utilisez les flèches pour afficher l'heure 8 h 00.
 - c Pour modifier l'heure de fin de cette période, utilisez l'icône en forme d'horloge, sous **Heure de fin**.

Par exemple, utilisez les flèches pour afficher l'heure 6 h 00.

- d Modifiez l'intervalle en fonction des besoins. Par exemple, pour définir une période de forte activité, faites passer l'intervalle de 60 à 20 minutes pour créer des instantanés trois fois par heure.
- 5 Si vous avez défini une période autre que minuit à 23 h 59 à l'étape 7, et que vous souhaitez que des sauvegardes soient effectuées dans les plages de temps restantes, vous devez ajouter d'autres périodes pour définir la protection, en procédant comme suit :
 - a Dans la catégorie appropriée, cliquez sur **Ajouter période**.
 - b Cliquez sur l'icône en forme d'horloge, puis sélectionnez les heures de début et de fin désirées.
Par exemple, définissez l'heure de début minuit et l'heure de fin 19 h 59.
 - c Modifiez l'intervalle en fonction des besoins. Par exemple, pour définir une période de faible activité, faites passer l'intervalle de 60 à 120 minutes pour créer des instantanés toutes les deux heures.
- 6 Si nécessaire, continuez à créer des périodes en définissant des heures de début et de fin et des intervalles de manière appropriée.

REMARQUE : si vous souhaitez supprimer une période que vous avez ajoutée, cliquez sur l'icône en forme de corbeille à l'extrémité droite de cette période, puis cliquez sur **Oui** pour confirmer.

- 7 Pour créer un modèle à partir de la planification que vous définissez, cliquez sur **Enregistrer comme modèle**.
- 8 Dans la boîte de dialogue Enregistrer le modèle, attribuez un nom au modèle, puis cliquez sur **Enregistrer**.
- 9 Lorsque l'horaire de protection vous convient, cliquez sur **Appliquer**.
La boîte de dialogue Planification de protection se ferme.

Suspendre et reprendre la protection

Lorsque vous suspendez la protection, vous arrêtez temporairement tous les transferts de données depuis la machine sélectionnée vers le Core de Rapid Recovery. Lorsque vous reprenez la protection, le Core de Rapid Recovery applique les planifications de protection et sauvegarde les données régulièrement en fonction de la planification.

Vous pouvez suspendre la protection de toute machine protégée de Rapid Recovery :

- lorsque vous établissez la protection à l'aide de l'assistant Protéger une machine ou de l'assistant Protéger plusieurs machines.
- Depuis le menu déroulant Machines protégées dans la zone de navigation gauche du Core de Rapid Recovery (suspension de la protection pour toutes les machines protégées).
- Depuis la page Machines protégées (accessible lorsque vous cliquez sur le menu Machines protégées).
- Depuis une machine protégée dans le menu déroulant Machines protégées.
- Depuis le haut de chaque page pour une machine protégée spécifique.

Si vous suspendez la protection à l'aide de l'assistant Protéger une machine ou de l'assistant Protéger plusieurs machines, la protection est suspendue jusqu'à ce qu'elle soit explicitement reprise.

Si vous suspendez la protection en dehors d'un assistant, vous pouvez choisir soit de suspendre la protection jusqu'à sa reprise explicite, soit de la suspendre pendant une durée donnée (spécifiée dans une combinaison de jours, d'heures et de minutes). Si vous suspendez la protection pendant une durée donnée, à la fin du délai, le système reprend automatiquement la protection en fonction de la planification de protection.

Vous pouvez reprendre la protection de toute machine protégée suspendue de Rapid Recovery :

- Depuis le menu déroulant Machines protégées dans la zone de navigation gauche du Core de Rapid Recovery (reprise de la protection pour toutes les machines protégées).
- Depuis une machine protégée dans le menu déroulant Machines protégées.
- Depuis la page Machines protégées (accessible lorsque vous cliquez sur le menu Machines protégées).
- Depuis le haut de chaque page pour une machine protégée spécifique.

Utilisez la procédure décrite ci-dessous pour suspendre ou reprendre la protection, selon les besoins.

- 1 Dans la console Core de Rapid Recovery, pour suspendre la protection pour toutes les machines, cliquez sur le menu déroulant Machines protégées dans la zone de navigation de gauche, puis effectuez les opérations suivantes :
 - a cliquez sur **Suspendre la protection**.

La boîte de dialogue Suspendre la protection apparaît.

- b Sélectionnez le paramètre approprié en utilisant l'une des options décrites ci-dessous, puis cliquez sur **OK**.
 - Si vous voulez suspendre la protection jusqu'à ce vous stipuliez explicitement que vous voulez la reprendre, sélectionnez **Suspendre jusqu'à la reprise**.
 - Si vous voulez suspendre la protection pendant une durée donnée, sélectionnez **Suspendre pendant**, puis dans les champs Jours, Heures et Minutes, entrez ou sélectionnez la durée de la suspension selon les besoins.
- 2 Pour reprendre la protection pour toutes les machines, effectuez les opérations suivantes :
 - a Cliquez sur **Reprendre la protection**.
La boîte de dialogue Reprendre la protection apparaît.
 - b Dans la boîte de dialogue Reprendre la protection, cliquez sur **Oui**.
La boîte de dialogue Reprendre la protection se ferme, et la protection reprend pour toutes les machines.
- 3 Pour suspendre la protection d'une seule machine, cliquez sur le menu déroulant dans la zone de navigation à gauche, à droite de la machine concernée, puis effectuez l'une des actions suivantes :
 - a cliquez sur **Suspendre la protection**.
La boîte de dialogue Suspendre la protection apparaît.
 - b Sélectionnez le paramètre approprié en utilisant l'une des options décrites ci-dessous, puis cliquez sur **OK**.
 - Si vous voulez suspendre la protection jusqu'à ce vous stipuliez explicitement que vous voulez la reprendre, sélectionnez **Suspendre jusqu'à la reprise**.
 - Si vous voulez suspendre la protection pendant une durée donnée, sélectionnez **Suspendre pendant**, puis dans les champs Jours, Heures et Minutes, entrez ou sélectionnez la durée de la suspension selon les besoins.
- 4 Pour reprendre la protection d'une seule machine, effectuez les opérations suivantes :
 - a Cliquez sur **Reprendre la protection**.
La boîte de dialogue Reprendre la protection apparaît.
 - b Dans la boîte de dialogue Reprendre la protection, cliquez sur **Oui**.
La boîte de dialogue Reprendre la protection se ferme, et la protection reprend pour la machine sélectionnée.
- 5 Pour suspendre la protection d'une seule machine depuis les pages des machines, accédez à la machine concernée. La page Résumé affiche la machine sélectionnée.
 - a En haut de la page, cliquez sur **Suspendre**.
La boîte de dialogue Suspendre la protection apparaît.
 - b Sélectionnez le paramètre approprié en utilisant l'une des options décrites ci-dessous, puis cliquez sur **OK**.
 - Si vous voulez suspendre la protection jusqu'à ce vous stipuliez explicitement que vous voulez la reprendre, sélectionnez **Suspendre jusqu'à la reprise**.
 - Si vous voulez suspendre la protection pendant une durée donnée, sélectionnez **Suspendre pendant**, puis dans les champs Jours, Heures et Minutes, entrez ou sélectionnez la durée de la suspension selon les besoins.
- 6 Si vous souhaitez reprendre la protection, procédez comme suit :
 - a En haut de la page, cliquez sur **Reprendre**.
 - b Dans la boîte de dialogue Reprendre la protection, cliquez sur **Oui**.
La boîte de dialogue Reprendre la protection se ferme et la protection reprend pour la machine sélectionnée.

Gérer les machines protégées

Cette section explique comment afficher, configurer et gérer les machines protégées de votre environnement Rapid Recovery.

À propos de la gestion des machines protégées

Les tâches que vous pouvez accomplir pour gérer les machines protégées sont découpées en quelques catégories.

- Vous pouvez afficher les machines protégées sur le Core Rapid Recovery à l'aide des options présentées dans la rubrique [Affichage des machines protégées](#).

- Vous pouvez configurer les paramètres de la machine, accéder aux informations système ou configurer la notification des événements concernant une machine donnée. Pour plus d'informations, voir [Configurer les paramètres d'une machine](#).
- Vous pouvez accéder à des diagnostics sur une machine protégée. Pour plus d'informations, voir [Téléchargement et affichage du fichier journal d'une machine protégée](#).
- Vous pouvez supprimer une machine de la protection, annuler les opérations en cours ou afficher des informations sur les licences d'une machine protégée. Pour plus d'informations, voir [Gérer les machines](#).
- Vous pouvez voir et gérer les données enregistrées dans le Core. Pour plus d'informations, voir [Gérer les instantanés et les points de restauration](#).

Affichage des machines protégées

Sur la page **Accueil** de la console Core Rapid Recovery, dans la vue des tableaux récapitulatifs, vous pouvez afficher des informations récapitulatives concernant les machines protégées par le Core, dans le volet Machines protégées.

REMARQUE : un agent logiciel agit à la place de l'utilisateur pour prendre des mesures spécifiques. Les machines protégées sont parfois qualifiées d'agents, puisqu'elles exécutent le logiciel Agent Rapid Recovery pour permettre la sauvegarde et la réplication des données sur le Core Rapid Recovery.

Vous pouvez afficher l'état et le nom d'affichage de chaque machine, quelle logithèque elle utilise, la date et l'heure du dernier instantané, le nombre de points de restauration présents dans la logithèque pour la machine, et la quantité totale d'espace de stockage que les instantanés occupent dans la logithèque.

Pour gérer les aspects de n'importe quelle machine protégée, commencez par naviguer jusqu'à la machine que vous voulez voir, configurer ou gérer. Depuis la page Accueil, trois méthodes distinctes permettent d'accéder à une machine protégée :

- Dans le volet Machines Protégées, vous pouvez cliquer sur l'adresse IP ou le nom d'affichage d'une machine protégée. Cette opération vous conduit à la page Synthèse de la machine protégée sélectionnée.
- Dans la zone de navigation de gauche, vous pouvez cliquer sur le titre du menu **Machines protégées**. La page Machines protégées s'affiche. La page Machines protégées affiche des informations récapitulatives sur chacune des machines. Pour obtenir une description détaillée de cette page, voir [Affichage des informations récapitulatives d'une machine protégée](#).
- Dans la zone de navigation de gauche, sous Machines protégées, vous pouvez cliquer sur l'adresse IP ou le nom d'affichage de n'importe quelle machine protégée. Cette opération vous conduit à la page Synthèse de la machine protégée sélectionnée. Pour une description détaillée de cette page, voir [Affichage des informations récapitulatives d'une machine protégée](#).

Affichage des informations récapitulatives d'un cluster

Effectuez cette procédure pour visualiser les informations synthétiques d'un cluster, notamment les informations de quorum du cluster.

- 1 Dans la Rapid Recovery Core Console, accédez au menu Machines protégées et cliquez sur le cluster à afficher.
La page Synthèse de la machine s'affiche.
- 2 La page Synthèse vous permet de consulter diverses informations (nom du cluster, type de cluster, type de quorum (le cas échéant), chemin du quorum (le cas échéant), etc.) Cette page affiche aussi des informations d'ensemble sur les volumes du cluster, y compris la taille et la planification de protection. Le cas échéant, vous pouvez également voir des informations relatives au serveur SQL ou au serveur Exchange d'un cluster différent.
- 3 Pour afficher les informations les plus récentes, cliquez sur **Actualiser**.

Pour en savoir plus sur l'affichage d'informations synthétiques et d'informations sur l'état d'une machine ou d'un nœud particulier du cluster, voir [Affichage des machines protégées](#).

Configurer les paramètres d'une machine

Une fois que vous avez ajouté une machine à protéger dans Rapid Recovery, vous pouvez facilement afficher et modifier les paramètres qui régissent le comportement de cette machine protégée. Lorsque vous modifiez les paramètres d'une machine spécifique, ces paramètres remplacent le comportement défini au niveau du core.

Vous pouvez afficher et configurer les paramètres de machine suivants dans la console core Rapid Recovery :

- **Général.** Paramètres généraux de configuration de la machine : nom d'affichage, nom d'hôte, port, clé de chiffrement et référentiel. Pour plus d'informations concernant la configuration des paramètres généraux d'une machine, voir [Paramètres d'affichage et de modification des machines protégées](#).
- **Travaux nocturnes.** Le sous-ensemble des paramètres de travaux nocturnes du core qui apparaissent pour une machine protégée spécifique vous permet de remplacer ceux définis au niveau du core. Cela inclut notamment le cumul, qui vous permet de gérer la stratégie de conservation. Certains paramètres peuvent différer en fonction du type de la machine qui est protégée.
- **Paramètres de transfert.** Paramètres spécifiques à la gestion des transferts de données pour la machine protégée sélectionnée. Pour plus d'informations sur les types de transfert de données affectées par ces paramètres, voir [À propos de la modification des paramètres de transfert](#).
- **Writers exclus.** Ces paramètres vous permettent d'exclure des writers. Ils sont spécifiques à la machine. Un writer est une API spécifique publiée par Microsoft pour permettre à d'autres composants logiciels d'utiliser Microsoft Volume Shadow Services (VSS). Chacun des writers dans Rapid Recovery qui participent à des instantanés de volume sont répertoriés dans les paramètres d'exclusion de writers. Dans le cas où un writer interfère ou entrave l'exécution d'un transfert, il est possible de le désactiver individuellement. Dell recommande de ne pas toucher à ces paramètres, sauf à agir sous les directives d'un représentant du support technique de Dell.
- **Détails de la licence.** Ce sont des détails sur la licence de la machine protégée spécifique. Ces paramètres reprennent des informations fournies par le core et le Portail des licences Dell Data Protection | Rapid Recovery. Ces paramètres sont en lecture seule. Pour les modifier, vous devez mettre à jour vos les informations de votre licence entre le core et le portail de licences. Consultez votre administrateur de licences pour plus de détails. Pour plus d'informations, reportez-vous au manuel *Portail des licences Dell Data Protection | Rapid Recovery – Guide d'utilisation*.

L'affichage ou la modification des paramètres au niveau d'une machine s'effectuent de la même manière pour les paramètres généraux, les exclusions de writers et les détails de licence. Pour plus d'informations, reportez-vous à [Paramètres d'affichage et de modification des machines protégées](#).

La modification des travaux nocturnes pour une machine donnée est différente. Pour plus d'informations concernant la configuration des paramètres de travaux nocturnes d'une machine, voir [Personnalisation des tâches nocturnes pour une machine protégée](#).

Dans certains cas, vous souhaitez peut-être ajuster le débit de transfert des données d'une machine protégée. Pour plus d'informations, reportez-vous à [À propos de la modification des paramètres de transfert](#).

Paramètres d'affichage et de modification des machines protégées

Les paramètres des machines permettent de déterminer le fonctionnement d'une machine protégée par le Core. Lorsque vous modifiez les paramètres d'une machine spécifique, ces paramètres remplacent le fonctionnement défini au niveau du Core.

Suivez les étapes de cette procédure pour afficher et modifier les paramètres généraux, les paramètres de transfert, les paramètres relatifs aux processus d'écriture exclus et les paramètres d'octroi de licences d'une machine protégée.

REMARQUE : pour afficher et modifier les paramètres des tâches nocturnes, voir [Personnalisation des tâches nocturnes pour une machine protégée](#).

Cette tâche constitue également une étape de la rubrique [Modifier les paramètres de nœuds de cluster](#).

- 1 Dans la console Core Rapid Recovery, sous Machines protégées, cliquez sur l'adresse IP ou le nom de la machine dont vous souhaitez afficher ou modifier les paramètres de configuration.

La page **Synthèse** de la machine sélectionnée s'affiche.

- 2 Cliquez sur le menu **Paramètres**.

La page **Paramètres**, qui présente les paramètres de la machine sélectionnée, s'affiche. Éventuellement, pour afficher les catégories de paramètres n'importe où sur la page, vous pouvez cliquer sur le lien hypertexte approprié, sur la gauche de la page.

Lorsque vous cliquez sur un paramètre à modifier, celui-ci peut être modifié en tant que champ de texte ou menu déroulant.

Pour chaque paramètre, lorsque vous êtes satisfait de vos modifications, cliquez sur  pour enregistrer les modifications et quitter le mode d'édition, ou cliquez sur  pour quitter le mode d'édition sans enregistrer.

- 3 Pour modifier les paramètres généraux d'une machine protégée, cliquez sur le paramètre approprié, puis saisissez les informations de configuration comme indiqué dans le tableau suivant.

Tableau 69. Paramètres généraux d'une machine protégée

Zone de texte	Description
Nom d'affichage	Entrez le nom d'affichage de la machine. Il s'agit du nom s'affichant pour une machine protégée dans la console Core Rapid Recovery. Vous pouvez entrer jusqu'à 64 caractères. Par défaut, il s'agit du nom d'hôte de la machine. Le cas échéant, vous pouvez rendre ce nom plus convivial en le modifiant. N'utilisez pas de caractères interdits ou de expressions interdites .
Nom de l'hôte	Entrez le nom d'hôte de la machine.
Port	Entrez le numéro de port de la machine. Ce port est utilisé par le service Core Rapid Recovery pour communiquer avec cette machine. Le port par défaut est 8006.
Clé de chiffrement	Si vous souhaitez que la clé de chiffrement définie pour ce Core Rapid Recovery soit appliquée aux données de tous les volumes de cette machine protégée, vous pouvez spécifier la clé de chiffrement dans ce champ. La clé doit être déverrouillée. Si aucune clé de chiffrement n'existe, vous pouvez en ajouter une. Pour en savoir plus sur la gestion des clés de chiffrement, voir Gérer les clés de chiffrement. Si les volumes de cette machine protégée sont chiffrés, vous pouvez passer à une clé de chiffrement différente. Sinon, vous pouvez dissocier une clé de chiffrement en sélectionnant aucune dans le menu déroulant Clé de chiffrement. REMARQUE : après avoir appliqué, modifié ou dissocié une clé de chiffrement pour une machine protégée, Rapid Recovery crée une nouvelle image de base lors du prochain instantané planifié ou forcé.
Logithèque	Sélectionnez la logithèque des points de restauration. Affiche la logithèque configurée sur le Core Rapid Recovery dans laquelle les données de cette machine doivent être stockées. Le volume d'espace de stockage peut être local (sur un stockage attaché au serveur Core) ou se trouver sur un volume d'un emplacement partagé CIFS. REMARQUE : le paramètre de la logithèque de cette page peut uniquement être modifié s'il n'existe aucun point de restauration ou si la logithèque précédente est absente.

- 4 Pour modifier les paramètres des tâches nocturnes d'une machine protégée, voir [Personnalisation des tâches nocturnes pour une machine protégée](#).
- 5 Pour modifier les paramètres Exchange d'un serveur Exchange protégé, dans la section Paramètres de serveur Exchange, cliquez sur **Activer la vérification automatique de montabilité**, puis procédez comme suit :

- Pour activer la vérification automatique de montabilité, cochez la case correspondante, puis cliquez sur .
- Pour désactiver la vérification automatique de montabilité, décochez la case correspondante, puis cliquez sur .

Pour en savoir plus sur la vérification automatique de montabilité, voir [À propos des vérifications de la montabilité de la base de données Exchange](#).

- 6 Pour modifier les paramètres de transfert d'une machine protégée, cliquez sur le paramètre approprié, puis saisissez les informations de configuration comme indiqué dans le tableau suivant.

REMARQUE : pour obtenir des informations conceptuelles sur les paramètres de transfert, voir [À propos de la modification des paramètres de transfert](#).

Tableau 70. Paramètres de transfert d'une machine protégée

Zone de texte	Description
 Restaurer les valeurs par défaut	Cette commande restaure tous les paramètres de transfert par défaut du système.
Priorité	Définit la priorité de transfert entre les machines protégées. Permet d'affecter une priorité par rapport à d'autres machines protégées. Sélectionnez un nombre entre 1 et 10, 1 correspondant à la priorité la plus élevée. Le paramètre par défaut établit la priorité 5.
REMARQUE : la priorité s'applique aux transferts se trouvant dans la file d'attente.	
Nombre maximal de flux simultanés	Définit le nombre maximal de liens TCP envoyés au Core pour y être traités en parallèle par une machine protégée, pour les machines protégées dans une logithèque DVM.
REMARQUE : Dell conseille d'affecter la valeur 8 au paramètre. Si vous constatez des pertes de paquets, essayez d'augmenter cette valeur.	
Nombre maximal d'écritures simultanées	Définit le nombre maximal d'écritures simultanées sur disque par connexion de machine protégée.
REMARQUE : Dell conseille d'affecter au paramètre la même valeur que celle sélectionnée pour le nombre de flux simultanés. Si vous constatez des pertes de paquets, essayez d'abaisser ce nombre, par exemple, si le nombre maximal de flux simultanés est 8, réglez cette valeur sur 7.	
Utiliser le nombre maximal de nouvelles tentatives par défaut du Core	Sélectionnez cette option pour définir le nombre maximal de nouvelles tentatives pour chaque machine protégée en cas d'échec de certaines opérations.
Taille maximale de segment	Définit le volume maximal de données, en octets, qu'une machine peut recevoir dans un même segment TCP. Le paramètre par défaut est 419 4304. Ne remplacez pas les valeurs par défaut de ce paramètre, à moins d'y être invité par un représentant du support technique de Dell.
Longueur maximale de la file d'attente de transfert	Spécifie le nombre de commandes qui peuvent être envoyées simultanément. Le paramètre par défaut est 64. Vous pouvez définir une valeur plus élevée si le système a un nombre d'opérations d'E/S simultanées plus élevé.
Lectures en attente par flux de données	Spécifie le nombre d'opérations de lecture en attente seront stockées sur le back-end. Ce paramètre permet de mieux contrôler les files d'attente des machines protégées. Le paramètre par défaut est 0.
Transfer Data Server Port (Port de serveur de transfert de données)	Définit le port à utiliser pour les transferts. Le paramètre par défaut est 8009.
Transfer Timeout (Expiration du délai d'attente de transfert)	Spécifie en minutes et en secondes la durée pendant laquelle un paquet peut être statique avant l'expiration du transfert.
Snapshot Timeout (Expiration du délai d'attente d'instantané)	Spécifie en minutes et en secondes le temps d'attente maximal d'une prise d'instantané.

Zone de texte	Description
Délai d'attente de nettoyage d'instantané	Spécifie (en minutes et en secondes) la durée maximale du processus de suppression d'un instantané VSS sur une machine protégée.
Network Read Timeout (Expiration du délai d'attente de lecture réseau)	Spécifie en minutes et en secondes le temps d'attente maximal d'une connexion de lecture. Si la lecture réseau ne peut pas être exécutée pendant cette durée, l'opération est relancée.
Network Write Timeout (Expiration du délai d'attente d'écriture réseau)	Spécifie en secondes le temps d'attente maximal d'une connexion d'écriture. Si l'écriture réseau ne peut pas être exécutée pendant cette durée, l'opération est relancée.

- 7 Pour modifier les paramètres relatifs aux processus d'écriture exclus, cliquez sur le paramètre approprié, puis saisissez les informations de configuration comme indiqué dans le tableau suivant.

Tableau 71. Paramètres relatifs aux processus d'écriture exclus d'une machine protégée

Zone de texte	Description
Programmes d'écriture exclus	Sélectionnez un programme d'écriture si vous souhaitez l'exclure. Comme les programmes d'écriture qui apparaissent dans la liste sont spécifiques à la machine que vous configurez, vous n'allez pas voir tous les programmes d'écriture dans cette liste. Par exemple, voici certains des programmes d'écriture que vous pouvez voir : • ASR Writer (Enregistreur ASR) • COM+ REGDB Writer (Enregistreur COM+ REGDB) • Performance Counters Writer (Enregistreur de compteurs de performance) • Registry Writer (Enregistreur de registre) • Shadow Copy Optimization Writer (Enregistreur d'optimisation de copie en double) • SQLServerWriter • System Writer (Enregistreur système) • Task Scheduler Writer (Enregistreur de planificateur de tâche) • VSS Metadata Store Writer (Enregistreur de magasin de métadonnées VSS) • WMI Writer (Rédacteur WMI)

- 8 Les détails de la licence d'une machine protégée sont en lecture seule. Les informations détaillées de la licence sont fournies dans le tableau suivant.

Tableau 72. Détails de la licence d'une machine protégée

Zone de texte	Description
Date d'expiration	Indique la date d'expiration de la licence de la machine protégée sélectionnée.
État de la licence	Indique l'état actuel de la licence de la machine protégée sélectionnée.
Type de licence	Indique le type de licence de la machine protégée sélectionnée.
Type d'agent	Indique si la machine actuellement protégée est une machine physique ou un agent virtuel.

Modifier les paramètres d'un hôte ou d'un hôte Hyper-V

Cette procédure s'applique aux hôtes ou aux nœuds Hyper-V qui utilisent Rapid Recovery Rapid Snap for Virtual (protection sans agent) pour protéger des machines virtuelles (VM) .

Un hôte Hyper-V qui utilise Rapid Snap for Virtual (protection sans agent) pour protéger des machines virtuelles est signalé dans la zone de navigation de gauche par une icône d'hôte.  Les paramètres d'un hôte Hyper-V avec machines virtuelles protégées sans agent ne

sont pas les mêmes que ceux d'une machine protégée classique. Toutes les modifications apportées aux paramètres d'un hôte s'appliquent aux VM qu'héberge cet hôte.

- 1 Dans la console Core, sous Machines protégées dans la zone de navigation de gauche, cliquez sur l'hôte Hyper-V dont vous voulez modifier les paramètres.
La page **Résumé** de l'hôte s'ouvre.
- 2 Dans la barre de menus de l'hôte, cliquez sur **Paramètres**.
La page **Paramètres** s'ouvre.
- 3 Sous **Général**, cliquez sur le paramètre que vous souhaitez modifier.
L'option sélectionnée devient modifiable, sous forme de champ de texte ou de menu déroulant.
- 4 Entrez les informations de configuration décrites dans le tableau suivant.

Tableau 73. Informations de paramètres généraux

Zone de texte	Description
Nom d'affichage	Le nom qui s'affiche pour une machine protégée dans la console Core Rapid Recovery. Vous pouvez entrer jusqu'à 64 caractères. Par défaut, il s'agit du nom d'hôte de la machine. Vous pouvez modifier le nom d'affichage pour le rendre plus convivial, si nécessaire. N'utilisez pas caractères interdits ni expressions interdites .
Nom d'hôte	Le nom de la machine protégée tel qu'il apparaît dans les métadonnées de la machine.

 **REMARQUE : Ne changez pas ce paramètre, car cela risquerait de rompre la connexion entre la machine protégée et le core.**

- 5 Sous **File d'attente de transferts**, pour modifier le nombre de travaux de transfert pouvant s'afficher sur l'hôte à un moment donné, cliquez sur le paramètre de **Nombre maximum de transferts simultanés**.
 **REMARQUE : Pour des performances optimales, il est recommandé que le nombre maximum de transferts simultanés pour l'hôte ou le nœud Hyper-V soit de 1, qui est le paramètre par défaut.**
- 6 Sous **Travaux nocturnes**, pour modifier les paramètres des travaux nocturnes disponibles, cliquez sur **Modifier**.
La fenêtre **Travaux nocturnes** s'affiche.
- 7 Entrez les informations de configuration décrites dans le tableau suivant.

Tableau 74. Informations sur les travaux nocturnes

Zone de texte	Description
Effacer les clés de registre orphelines sur l'hôte Hyper-V protégé	Supprime du registre les fichiers inutiles résultant de connexions et de déconnexions de disques virtuels lors de transferts de données.
Vérifier l'intégrité des points de restauration	Effectue la vérification de l'intégrité de chaque point de restauration créé pour les machines virtuelles sur l'hôte Hyper-V.

- 8 Cliquez sur **OK**.
- 9 Sous **Protection automatique**, pour déterminer s'il y a lieu de protéger automatiquement les nouvelles machines virtuelles lors de leur ajout à l'hôte Hyper-V, cliquez sur le paramètre de **protection automatique des nouvelles machines virtuelles**.

Modification des paramètres pour une machine virtuelle protégée Hyper-V

Cette procédure s'applique aux machines virtuelles Hyper-V qui sont protégées sans agent à l'aide de Rapid Recovery Rapid Snap for Virtual.

Un hôte Hyper-V qui utilise Rapid Snap for Virtuel (protection sans agent) est indiqué dans la zone de navigation gauche par l'icône de

. Les paramètres pour une machine virtuelle sans agent Hyper-V sont identiques à ceux d'une machine virtuelle protégée typique, à l'exception de la section Hyper-V au bas de la page **Paramètres**. La tâche suivante fournit des instructions concernant uniquement les

paramètres de la section **Hyper-V**. Pour tous les autres paramètres de machine protégée, voir [Paramètres d'affichage et de modification des machines protégées](#).

- 1 Dans la zone de navigation gauche de la Core Console, sous **Machines protégées**, cliquez sur la machine virtuelle Hyper-V dont vous souhaitez modifier les paramètres.
La page **Récapitulatif** de la machine virtuelle s'affiche.
- 2 Sur la barre de menus de l'hôte, cliquez sur **Paramètres**.
La page **Paramètres** s'affiche.
- 3 Dans la liste de gauche, cliquez sur **Hyper-V**.
Le paramètre sélectionné devient modifiable, comme un champ de texte ou un menu déroulant.
- 4 Sous **Hyper-V**, cliquez sur **Configuration d'instantané**.
Le paramètre sélectionné devient un menu déroulant modifiable.
- 5 Dans le menu déroulant, sélectionnez l'une des options décrites dans le tableau suivant.

Tableau 75. Informations sur les paramètres Hyper-V

Zone de texte	Description
Essayer d'abord de créer un instantané VSS pendant le transfert. Si cela échoue, créer un point de vérification.	Si l'instantané VSS réussit, le point de restauration sera dans un état cohérent avec l'application. Si l'instantané VSS échoue et qu'un point de restauration est créé, le point de restauration sera dans un état cohérent avec le plantage.
Ne pas créer d'instantané VSS pendant le transfert	Génère un point de restauration dans un état avec le plantage.
Utiliser uniquement des instantanés VSS pendant les transferts. Si la création d'instantané VSS échoue, le transfert entier échoue.	Génère uniquement des points de restauration cohérents avec l'application. Si l'instantané VSS échoue, aucun point de restauration n'est généré.

Modification des paramètres vSphere pour une machine virtuelle protégée VMware

Cette procédure s'applique aux machines virtuelles VMware ESXi ou Workstation qui sont protégées sans agent à l'aide de Rapid Recovery Snap for Virtual.

Les paramètres d'une machine virtuelle VMware protégée sans agent incluent les mêmes paramètres utilisés pour une machine protégée typique, à une exception près. La section **vSphere** de la page **Paramètres** inclut des paramètres qui s'appliquent uniquement aux machines virtuelles VMware protégées sans agent. La tâche suivante fournit des instructions concernant uniquement la section **vSphere** de la page **Paramètres**. Pour tous les autres paramètres de machine protégée, voir [Paramètres d'affichage et de modification des machines protégées](#).

- 1 Dans la Core Console, sous Machines protégées dans la zone de navigation gauche, cliquez sur l'hôte Hyper-V dont vous souhaitez modifier les paramètres.
La page **Récapitulatif** de l'hôte s'affiche.
- 2 Sur la barre de menus de l'hôte, cliquez sur **Paramètres**.
La page **Paramètres** s'affiche.
- 3 Dans la liste de gauche, cliquez sur **vSphere**.
Le paramètre sélectionné devient modifiable, comme un champ de texte ou un menu déroulant.
- 4 Sous **vSphere**, cliquez sur le paramètre à modifier.
Le paramètre sélectionné devient modifiable, comme un champ de texte ou un menu déroulant.
- 5 Entrez les informations de configuration, tel que décrit dans le tableau suivant.

Tableau 76. Informations sur les paramètres vSphere

Zone de texte	Description
Autoriser Rapid Recovery à supprimer des VMware créées par un utilisateur	Le paramètre par défaut est Non.
Autoriser le transfert de volumes ayant une capacité utilisée non valide	Le paramètre par défaut est Oui.
Autoriser les instantanés suspendus	Le paramètre par défaut est Oui.

À propos de la modification des paramètres de transfert

Dans la Rapid Recovery, vous pouvez modifier les paramètres afin de gérer les processus de transfert de données d'une machine protégée. Les paramètres de transfert décrits dans cette section sont définis sur le niveau de la machine protégée. Pour modifier les transferts au niveau du Noyau, veuillez consulter [Modifier les paramètres de la file d'attente de transfert](#).

La Rapid Recovery est prise en charge par Windows 8 et Windows Server 2012 pour les transferts normaux (de base et par incréments), ainsi que pour la restauration, la restauration complète et l'exportation de machines virtuelles.

Il existe trois types de transferts au sein de la Rapid Recovery :

- **Instantané.** Les données présentes sur la machine protégée sont sauvegardées. Deux types d'instantanés sont possibles : une image de base de toutes les données protégées et un instantané par incréments pour les données modifiées depuis le dernier instantané. Ce type de transfert crée des points de récupération qui sont stockés dans la logithèque associée au Noyau. Pour plus d'informations, veuillez consulter [Gérer les instantanés et les points de restauration](#).
- **Exportation de machines virtuelles.** Une machine virtuelle (MV) est créée depuis un point de récupération. Elle contient toutes les données enregistrées lors de la sauvegarde de la machine protégée, ainsi que le système d'exploitation, les pilotes et les données associées, dans le but de garantir le démarrage de la MV. Pour plus d'informations, veuillez consulter [VM export \(Exportation NFS\)](#).
- **Restauration.** Les informations sauvegardées sont restaurées sur une machine virtuelle. Pour plus d'informations, veuillez consulter [À propos de la restauration de volumes à partir d'un point de restauration](#).

REMARQUE : l'ensemble du volume est réécrit lors d'une restauration d'un système Windows utilisant des partitions EFI.

Le transfert de données dans la Rapid Recovery implique la transmission d'un volume de données le long d'un réseau, depuis les machines protégées vers le Noyau. Dans le cas d'une réplication, un transfert survient également depuis le point d'origine, ou Noyau source, vers le Noyau cible.

Le transfert de données au sein de votre système peut être optimisé par le biais de certains paramètres de performances. Ces paramètres commandent l'utilisation de la bande passante lors du processus de sauvegarde des machines protégées, d'exportation des MV ou de restauration. Voici quelques uns des facteurs qui ont un impact sur les performances lors du transfert de données :

- Nombre de transferts de données d'agent simultanés
- Nombre de flux de données simultanés
- Quantité de données modifiées sur le disque
- Bande passante réseau disponible
- Performances du sous-système de disques de la logithèque
- Quantité de mémoire disponible pour la mise en tampon des données

Vous pouvez modifier les options de performances pour qu'elles répondent aux besoins de votre entreprise et les ajuster en fonction de votre environnement. Pour plus d'informations, veuillez consulter [Limitation de la vitesse de transfert](#).

Limitation de la vitesse de transfert

Lorsque vous transférez des données de sauvegarde ou des points de restauration répliqués entre des machines protégées et des Cores sur le réseau, vous pouvez délibérément réduire la vitesse de transfert. Ce processus est connu sous le nom de limitation.

En limitant la vitesse de transfert, vous réduisez la quantité de bande passante allouée aux transferts de fichiers à partir de Rapid Recovery. Lorsque vous configurez la réplication, par exemple, la limitation peut réduire le risque que le transfert de points de restauration antérieurs vers le Core répliqué utilise toute la bande passante de votre réseau.

⚠ PRÉCAUTION : la limitation de la vitesse de transfert n'est pas toujours imposée ni préconisée. Ces informations sont fournies pour permettre d'identifier une solution à d'éventuels problèmes de performances dans votre environnement Rapid Recovery. Par exemple, la limitation résout parfois les problèmes associés aux échecs de transfert répétés ou aux ralentissements dus au transfert d'une grande quantité de données pour vos Cores protégés ou répliqués.

Plusieurs facteurs permettent d'identifier la meilleure approche de la limitation. Le type de la machine protégée est un facteur clé. Par exemple, un serveur Microsoft Exchange occupé présente un taux de changement nettement plus élevé qu'un serveur Web hérité rarement utilisé.

Les fonctionnalités d'entrée et de sortie des volumes de stockage de vos machines protégées peuvent également intervenir dans le niveau d'efficacité.

La vitesse de votre réseau est un autre facteur critique, incluant de nombreuses variables. Le segment principal du réseau en place (par exemple, 1GbE ou 10GbE), l'architecture, la configuration, l'utilisation intentionnelle d'une association de cartes réseau et même le type de câbles utilisé peuvent affecter la vitesse de transfert du réseau. Si le réseau étendu de votre environnement est plus lent, et que la sauvegarde ou la réplication des tâches de transfert échoue, il peut être avisé de limiter la vitesse de transfert en définissant certains de ces paramètres.

Enfin, le processus de limitation du réseau implique un certain nombre de tentatives et d'erreurs. Dell vous recommande d'ajuster et tester vos paramètres de transfert, et de revenir régulièrement sur ces paramètres pour vous assurer qu'ils continuent de répondre à vos besoins.

Le réglage de la vitesse de transfert doit être effectué machine par machine. Dans la Core Console, accédez à une machine spécifique, sélectionnez Paramètres, puis réglez la vitesse de transfert. Pour obtenir des informations spécifiques sur l'affichage et la modification de ces paramètres, voir [Paramètres d'affichage et de modification des machines protégées](#). Cette rubrique contient également des descriptions de tous les paramètres utilisés pour la limitation du transfert. Ces descriptions peuvent aider à identifier les paramètres à ajuster en premier lieu.

Les quatre paramètres principaux impliqués dans la limitation de la vitesse de transfert sont présentés dans le tableau suivant :

Tableau 77. Paramètres applicables aux machines protégées utilisés pour limiter la vitesse de transfert

Paramètres Machine-Level	Paramètre par défaut	Paramètre de limitation suggéré
Nombre maximal de flux simultanés	8	4
Nombre maximal d'écritures simultanées	8	4
Taille maximale de segment	4194304	2097152
Lectures en attente par flux de données	0	Commencer à 24

Dell recommande d'ajuster et tester les autres paramètres avant de modifier le paramètre par défaut relatif aux lectures en attente par flux de données, sauf indication contraire d'un représentant du support technique de Dell. Pour faire des essais avec ce paramètre, commencez par la valeur 24.

Lorsque vous définissez des limitations dans les paramètres de transfert des machines protégées, ces limitations s'appliquent à chaque tâche. Si deux tâches de transfert sont exécutées simultanément ou se chevauchent, l'utilisation de la bande passante est multipliée par deux. Si quatre tâches de transfert se chevauchent sur le réseau, l'utilisation de la bande passante est multipliée par quatre, et ainsi de suite.

Personnalisation des tâches nocturnes pour une machine protégée

Les tâches nocturnes peuvent être configurées au niveau du Noyau et à celui de la machine à partir de l'onglet Configuration correspondant. Lorsque les paramètres des tâches nocturnes sont configurés au niveau du Noyau, les modifications sont appliquées à

toutes les machines concernées protégées par ce Noyau. Les modifications apportées aux tâches nocturnes au niveau de la machine remplacent les modifications apportées au niveau du Noyau (pour les machines précisées uniquement).

Pour obtenir la liste de toutes les tâches nocturnes, ainsi que leur description et leur portée particulières, veuillez consulter [Comprendre les travaux nocturnes](#).

Suivez les étapes décrites dans la procédure suivante pour modifier les tâches nocturnes d'une unique machine protégée.

- 1 Dans la console du Noyau de la Rapid Recovery, dans le menu Machines protégées, cliquez sur l'adresse IP ou le nom de la machine dont vous souhaitez personnaliser les tâches nocturnes.

La page **Récapitulatif** de la machine sélectionnée apparaît.

- 2 Cliquez sur le menu **Paramètres**.

La page **Paramètres** apparaît, affichant les paramètres de configuration pour la machine sélectionnée.

- 3 Il est également possible de cliquer sur le lien **Tâches nocturnes** et de faire défiler la page Paramètres vers le bas pour visualiser les paramètres des tâches nocturnes.

- 4 Sous le titre Tâches nocturnes, cliquez sur  **Modification**.

La boîte de dialogue **Tâches nocturnes** s'affiche.

REMARQUE : pour plus d'informations sur le paramètre de Cumul, dont la façon de configurer une stratégie de conservation personnalisée, veuillez consulter [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).

- 5 Dans la boîte de dialogue **Tâches nocturnes**, sélectionnez les tâches que vous voulez exécuter la nuit ou supprimez les options que vous voulez omettre pour cette machine.

REMARQUE : les options varient en fonction des machines. Par exemple, une machine protégée fonctionnant sous Exchange Server peut inclure Vérification de la somme de contrôle des bases de données Exchange et Troncature des journaux Exchange.

- 6 Cliquez sur **OK**.

REMARQUE : les résultats de cette procédure s'appliquent uniquement à la machine protégée sélectionnée. Pour les appliquer autre part, répétez la procédure sur chaque machine que vous souhaitez personnaliser. Pour modifier les paramètres des tâches nocturnes pour toutes les machines protégées par un Noyau, veuillez consulter [Configuration des tâches nocturnes du Core](#).

Affichage des informations sur le système d'une machine protégée

La console Core Rapid Recovery permet d'accéder facilement aux informations système relatives aux machines protégées sur votre Core.

Le volet **Généralités** contient des informations générales sur l'environnement et la machine Core. Le volet **Volumes** répertorie les informations relatives aux volumes de stockage de la machine Core. Le volet **Connexions Replay Engine** affiche les volumes de toutes les machines actuellement protégées.

Suivez cette procédure pour afficher les informations système détaillées d'une machine protégée.

- 1 Accédez à la console Core Rapid Recovery, puis dans le menu Machines protégées de la zone de navigation de gauche, cliquez sur le nom d'une machine protégée.

La page **Synthèse** de la machine protégée sélectionnée s'affiche.

- 2 Sur la page **Synthèse**, dans la partie inférieure du volet **Synthèse**, cliquez sur  **Informations sur le système**.

- 3 Sur la page **Informations sur le système**, vous pouvez afficher les détails suivants concernant la machine protégée sélectionnée.

- **Informations sur le système.** Les détails Nom d'hôte, Version du SE, Architecture du SE, Mémoire (Physique), Nom d'affichage, Nom de domaine qualifié complet, Emplacement des métadonnées de cache, Emplacement du cache principal, Emplacement du cache secondaire et Type de machine virtuelle (le cas échéant) sont affichés.
- **Volumes.** Les détails Nom du volume, Identifiant du périphérique, Système de fichiers, Capacité formatée, Capacité utilisée et Points de montage s'affichent.

- **Processeurs.** Les détails Architecture et Nombre de Cores s'affichent.
- **Cartes réseau.** Les détails Type d'adaptateur et Vitesse s'affichent.
- **Adresses IP.** Les détails Adresse IP et Famille s'affichent.

Gérer les machines

Cette section décrit un ensemble de tâches que vous pouvez effectuer pour gérer les machines. Les sujets abordés sont les suivants :

- [Supprimer une machine](#)
- [Retirer la protection d'un cluster](#)
- [Afficher les informations sur la licence d'une machine](#)
- [Téléchargement et affichage du fichier journal d'une machine protégée](#)
- [Convertir un nœud de cluster protégé en machine protégée](#)

Supprimer une machine

Lorsque vous retirez la protection d'une machine sur le Core Rapid Recovery, vous avez le choix entre deux options : celle de conserver les points de restauration enregistrés jusqu'à présent sur le Core RR ou celle de supprimer les points de restauration. Si vous conservez les points de restauration, vous obtenez ce que l'on appelle une machine à « points de restauration uniquement ». En utilisant ces points de restauration pour la machine qui a été supprimée de la protection actuelle, vous pouvez continuer à restaurer la machine ultérieurement, mais seulement jusqu'à son état tel qu'il avait été capturé dans un des points de restauration sauvegardés.

Si vous supprimez les points de restauration, cette opération supprime du Core Rapid Recovery toutes les données d'instantané de cette machine anciennement protégée.

 **PRÉCAUTION :** si vous supprimez les points de restauration, vous ne serez plus en mesure de restaurer les données de cette machine.

Suivez les étapes de la procédure ci-après pour retirer la protection d'une machine de votre environnement Rapid Recovery.

- 1 Dans la console Core Rapid Recovery, dans le volet de navigation de gauche se trouvant sous Machines protégées, cliquez sur la machine à supprimer.
- 2 Sur la page Synthèse de la machine appropriée, cliquez sur **Supprimer la machine**.
- 3 Dans la boîte de dialogue, si vous souhaitez également supprimer de la logithèque tous les points de restauration de cette machine, sélectionnez **Supprimer avec des points de restauration**.
- 4 Pour confirmer votre choix de supprimer la machine, cliquez sur **Oui**.
Rapid Recovery retire la protection de la machine et annule toutes les tâches actives de cette machine.

Retirer la protection d'un cluster

Suivez cette procédure pour retirer la protection d'un cluster.

- 1 Dans la console Core Rapid Recovery, sous Machines protégées, cliquez sur le cluster que vous souhaitez retirer.
- 2 Sur la page Résumé du cluster, cliquez sur **Supprimer le cluster**.
- 3 (Facultatif) Pour supprimer tous les points de restauration actuellement enregistrés pour ce cluster dans la logithèque, sélectionnez **Supprimer avec des points de restauration** dans la boîte de dialogue.
- 4 Dans la boîte de dialogue, cliquez sur **Oui** pour confirmer.

Retrait de la protection des nœuds de cluster

Suivez cette procédure suivante pour retirer la protection des nœuds de cluster.

Si vous souhaitez simplement supprimer un nœud d'un cluster, voir [Convertir un nœud de cluster protégé en machine protégée](#).

- 1 Dans la console Core de Rapid Recovery, accédez au menu Machines protégées et cliquez sur le nœud de cluster à supprimer.
- 2 Sur la page Synthèse du nœud, cliquez sur **Supprimer la machine**.
La boîte de dialogue Supprimer le nœud apparaît.

- 3 (Facultatif) Pour supprimer tous les points de restauration actuellement enregistrés pour ce cluster dans la logithèque, sélectionnez **Supprimer avec des points de restauration** dans la boîte de dialogue.
- 4 Dans la boîte de dialogue, cliquez sur **Oui** pour confirmer.

Retrait de la protection de tous les nœuds d'un cluster

Suivez cette procédure pour retirer la protection de tous les nœuds d'un cluster.

⚠ PRÉCAUTION : si vous supprimez tous les nœuds d'un cluster, ce cluster sera également supprimé.

- 1 Dans la console Core de Rapid Recovery, accédez au menu Machines protégées et cliquez sur le cluster dont vous souhaitez supprimer les nœuds.
- 2 Sur la page Synthèse du cluster, cliquez sur **Nœuds protégés**.
- 3 Sur la page Nœuds protégés, sélectionnez tous les nœuds.
- 4 Cliquez sur le menu déroulant **Supprimer des machines**, puis sélectionnez l'une des options décrites dans le tableau suivant.

Tableau 78. Options de retrait des nœuds

Option	Description
Supprimer et conserver les points de restauration	Pour conserver les points de restauration actuellement stockés pour ce cluster.
Supprimer les points de restauration	Pour retirer de la logithèque tous les points de restauration de ce cluster actuellement stockés.

- 5 Dans la boîte de dialogue Supprimer les nœuds, cliquez sur **Oui** pour confirmer.

Afficher les informations sur la licence d'une machine

Vous pouvez afficher les informations sur l'état de la licence active pour le logiciel Agent Rapid Recovery installé sur une machine protégée.

- 1 Dans la Rapid Recovery Core Console, accédez au menu Machines protégées et cliquez sur la machine à modifier.
La page **Synthèse** de la machine sélectionnée s'affiche.
- 2 Cliquez sur le menu **Paramètres**.
La page **Paramètres**, qui présente les paramètres de configuration de la machine sélectionnée, s'affiche.
- 3 Cliquez sur le lien **Octroi de licences** pour faire défiler la page Paramètres vers le bas de sorte à afficher les paramètres d'octroi de licences relatifs à la machine.
L'écran État s'ouvre et affiche des détails concernant la gestion de licence du produit.

Téléchargement et affichage du fichier journal d'une machine protégée

Si vous rencontrez des erreurs ou des problèmes avec une machine protégée, vous pouvez télécharger les journaux de cette machine afin de les consulter ou de les transmettre à votre représentant du support technique de Dell.

- 1 Dans la zone de navigation de gauche de la Core Console, sous Machines protégées, cliquez sur la flèche pour développer le menu contextuel pour la machine protégée appropriée. Faites défiler vers le bas jusqu'à **Plus**, développez ce menu, puis sélectionnez **Journal de l'agent**.
La page **Télécharger le journal de l'agent** s'affiche.
- 2 Sur la page **Télécharger le journal de l'agent**, cliquez sur  **Cliquer ici pour lancer le téléchargement**.
- 3 Dans la boîte de dialogue **Ouverture d'AgentAppRecovery.log**, effectuez l'une des opérations suivantes :
 - Pour ouvrir le fichier journal, sélectionnez **Ouvrir avec**, choisissez une application (par exemple, Bloc-notes) permettant d'afficher le fichier journal texte, puis cliquez sur **OK**.
Le fichier AgentAppRecovery.log s'ouvre dans l'application sélectionnée.
 - Pour enregistrer le fichier localement, sélectionnez **Enregistrer le fichier**, puis cliquez sur **OK**.

Le fichier AgentAppRecovery.log est enregistré dans votre dossier Téléchargements. Il est possible de l'ouvrir à l'aide d'un éditeur de texte.

Liens connexes

[Téléchargement et affichage du fichier journal du Core](#)

Convertir un nœud de cluster protégé en machine protégée

Dans Rapid Recovery, vous pouvez convertir un nœud de cluster protégé en machine protégée de sorte qu'il continue d'être géré par le Core sans plus faire partie du cluster. Cela est très utile, par exemple, si vous devez supprimer le nœud du cluster tout en continuant de le protéger.

- 1 Dans la Rapid Recovery Core Console, accédez au cluster qui contient la machine à convertir, puis cliquez sur **Nœuds protégés**.
- 2 Sur la page **Nœuds protégés**, accédez au nœud spécifique à convertir, puis cliquez sur le menu déroulant Actions et sélectionnez **Convertir en agent**.
- 3 Pour rajouter la machine au cluster, sélectionnez-la, puis accédez à la page Récapitulatif dans le menu Actions, et cliquez sur **Convertir en nœud**. Cliquez ensuite sur **Oui** pour confirmer cette action.

Comprendre les groupes personnalisés

La console Core Rapid Recovery affiche le menu Machines protégées dans la zone de navigation de gauche. Cela inclut toutes les machines ou clusters de serveurs ajoutés pour protéger le Core Rapid Recovery. Dessous, d'autres menus peuvent apparaître, selon les objets que vous avez inclus dans votre Core. De la même façon, vous pouvez créer un groupe personnalisé, qui s'affiche alors en tant que dernier type de menu dans la zone de navigation de gauche.

Le principal avantage d'un groupe personnalisé est la possibilité de grouper des objets de Core ensemble dans un conteneur logique. Cela peut vous permettre d'organiser et de gérer les objets de Core pour un usage particulier (par exemple : par organisation, centre de coûts, service, région géographique, et ainsi de suite).

Créer un groupe ajoute toujours un membre de groupe (par exemple : une machine protégée ou un cluster de serveurs, une machine répliquée ou une machine comportant uniquement des points de restauration) sur le nouveau groupe personnalisé. L'objet ajouté est déterminé selon votre point d'origine lors de la création du groupe. Idéalement, vous allez ensuite ajouter des membres au groupe. Par la suite, vous pourrez effectuer des actions de groupe qui s'appliqueront à tous les membres de ce groupe personnalisé, comme décrit dans [Exécuter des actions de groupe](#).

Les groupes personnalisés peuvent inclure des machines protégées, des clusters de serveurs, des machines répliquées et des machines comportant uniquement des points de restauration. Les clusters de serveurs se comportent de la même façon que les machines protégées, à l'exception du fait qu'un cluster de serveurs et ses nœuds se comportent comme une même entité. Si vous tentez d'ajouter un nœud à un groupe à partir d'un cluster de serveurs, l'ensemble du cluster est ajouté.

Un groupe personnalisé peut comporter des membres similaires ou non. Pour les groupes comportant des membres semblables, les actions de groupe s'appliquent toutes à tous les membres des groupes. Par exemple, si vous forcez un instantané pour un groupe personnalisé de machines protégées, toutes les machines protégées du groupe seront sauvegardées. Pour les groupes comportant des membres non similaires (par exemple, les machines protégées et les machines répliquées), si vous appliquez une action groupée comme la réplication forcée, celle-ci ne s'applique qu'aux seules machines répliquées.

Vous pouvez créer un ou plusieurs groupes. Une seule machine protégée ou une seule machine répliquée peut être incluse dans un ou plusieurs groupes. De cette façon, vous pouvez grouper des machines sur le core comme vous le souhaitez, et vous pouvez effectuer des actions s'appliquant à ce groupe.

Chacun des groupes personnalisés est affiché dans la zone de navigation de gauche, avec le libellé que vous choisissez. Les groupes avec des machines protégées standard apparaissent en premier dans le groupe personnalisé ; les machines répliquées s'affichent sous les machines protégées, le cas échéant. S'il y a des machines comportant uniquement des points de restauration, elles sont répertoriées sous les machines répliquées.

Dans la zone de navigation à gauche, les objets qui sont protégés sur le Core s'affichent tous dans leur propre menu. De ces menus, celui des groupes personnalisés s'affiche en dernier.

L'inclusion d'une machine dans un groupe ne retire pas celle-ci de son emplacement d'origine. Par exemple, si vous disposez de trois machines protégées portant les noms Agent1, Agent2 et Agent3, et que vous ajoutez Agent1 à GroupPersonnalisé1, Agent1 apparaît alors dans les deux emplacements.

Pour en savoir plus, reportez-vous aux rubriques suivantes :

- [Modifier les noms des groupes personnalisés](#)
- [Supprimer des groupes personnalisés](#)
- [Exécuter des actions de groupe](#)
- [Afficher toutes les machines d'un groupe personnalisé sur une seule page](#)

Créer des groupes personnalisés

Lorsque vous passez le pointeur sur le nom d'une machine dans le menu Machines protégées ou Machines répliquées, une flèche s'affiche pour ouvrir un menu déroulant. Depuis ce menu, vous pouvez créer un libellé personnalisé.

Utilisez la procédure ci-dessous pour créer un groupe personnalisé.

- 1 Accédez à la console Core Rapid Recovery.
- 2 À partir des machines protégées, des machines répliquées ou du menu contenant uniquement des points de récupération, effectuez les opérations suivantes :
 - a Placez votre curseur sur une machine contenue dans le menu.
 - b Cliquez sur le menu déroulant de cette machine.
 - c Déroulez et sélectionnez **Choisir le libellé**, puis cliquez sur **Nouveau libellé**.

La boîte de dialogue **Créer un libellé** s'affiche.

- 3 Dans le champ **Nom**, entrez un libellé approprié pour votre groupe personnalisé.
Utilisez un nom descriptif qui indique la finalité du groupe. Par exemple, pour grouper les machines protégées, les machines répliquées et les machines contenant uniquement des points de restauration par service, entrez `Accounting Department`. Vous pourrez renommer le groupe ultérieurement.

REMARQUE : Les libellés ne doivent pas dépasser 50 caractères. Vous pouvez inclure un espace simple entre les mots. Vous devez fournir un libellé pour le groupe personnalisé.

- 4 Lorsque vous avez choisi le nom du libellé, cliquez sur **OK**.
La boîte de dialogue se ferme et le groupe personnalisé apparaît en tant que dernier élément de la zone de navigation de gauche.
- 5 Si vous le souhaitez, vous pouvez ajouter d'autres machines protégées, machines répliquées machine contenant uniquement des points de restauration dans ce groupe. Naviguez jusqu'au nom de la machine dans le menu approprié, cliquez sur son menu déroulant, descendez dans la liste et choisissez **Choisir le libellé**, puis cliquez sur le nom du groupe personnalisé.
Vous pouvez maintenant effectuer des actions sur ce groupe. Pour plus d'informations, voir [Exécuter des actions de groupe](#).

Modifier les noms des groupes personnalisés

Lorsque vous modifiez le nom d'un groupe personnalisé, seul son libellé change. La machine ne changera pas.

Utilisez la procédure ci-dessous pour modifier le nom d'un groupe personnalisé.

- 1 Accédez à la console Core Rapid Recovery.
- 2 Dans le menu Machines protégées, passez le pointeur sur le groupe personnalisé à modifier.
- 3 Cliquez sur le menu déroulant de ce groupe, puis sur **Modifier**.
La boîte de dialogue **Modifier un libellé** s'affiche, dans laquelle le nom du groupe personnalisé devient modifiable.
- 4 Dans le champ **Nom**, mettez à jour le texte, ou supprimez le texte du libellé existant et entrez un nouveau libellé ou votre groupe personnalisé.

Utilisez un nom descriptif qui indique la finalité du groupe. Par exemple, pour grouper les machines protégées, les machines répliquées et les machines contenant uniquement des points de restauration par région géographique, entrez **Tokyo**. Vous pourrez renommer le groupe ultérieurement.

REMARQUE : Les libellés ne doivent pas dépasser 50 caractères. Vous pouvez inclure un espace simple entre les mots. Vous devez fournir un libellé pour le groupe personnalisé.

- 5 Lorsque vous avez choisi le nom du libellé, cliquez sur **OK**.
La boîte de dialogue se ferme et le groupe personnalisé modifié apparaît en tant que dernier élément de la zone de navigation de gauche.
- 6 Si vous le souhaitez, vous pouvez ajouter d'autres machines protégées, machines répliquées ou machines contenant uniquement des points de restauration dans ce groupe. Naviguez jusqu'au nom de la machine dans le menu approprié, cliquez sur son menu déroulant, descendez dans la liste et choisissez **Choisir le libellé**, puis cliquez sur le nom du groupe personnalisé.

Supprimer des groupes personnalisés

Lorsque vous supprimez un groupe personnalisé, vous supprimez le groupe du menu Machines protégées. Les machines de ce groupe ne sont pas supprimées, et vous pourrez toujours les retrouver dans le menu standard approprié.

Utilisez la procédure ci-dessous pour supprimer un groupe personnalisé.

- 1 Accédez à la console Core Rapid Recovery.
- 2 Dans le menu Machines protégées, passez le pointeur sur le groupe personnalisé à supprimer.
- 3 Cliquez sur le menu déroulant de ce groupe, puis cliquez sur **Supprimer le libellé**.
Un message s'affiche demandant de confirmer la suppression du groupe.
- 4 Confirmez la suppression du groupe personnalisé.
La boîte de dialogue se ferme, et le groupe personnalisé est supprimé de la zone de navigation.

Exécuter des actions de groupe

Vous pouvez effectuer des actions de groupe sur n'importe quel groupe dans la zone de navigation de la console Core Rapid Recovery. Si le groupe comporte des membres dissemblables (par exemple, des machines répliquées ou des machines de points de restauration uniquement), les actions que vous demandez ne s'appliquent qu'aux membres du groupe pertinents.

Utilisez la procédure ci-dessous pour effectuer des actions de groupe sur un groupe personnalisé.

- 1 Naviguez jusqu'à la Core Console Rapid Recovery.
- 2 Dans le menu Machines protégées, passez le pointeur sur le groupe personnalisé pour lequel vous souhaitez effectuer une action de groupe.
- 3 Cliquez sur le menu déroulant du groupe, puis sélectionnez une action comme suit :
 - Pour forcer la création d'un instantané incrémentiel ou d'une image de base pour toutes les machines protégées, cliquez sur **Forcer l'instantané** ou **Forcer l'image de base**, le cas échéant. Pour plus d'informations, voir [Forcer un instantané](#).
 - Pour suspendre la protection de toutes les machines protégées, cliquez sur **Suspendre la protection**, puis spécifiez les paramètres de reprise de la protection. Pour plus d'informations, voir [Suspendre et reprendre la réplication](#).
 - Pour reprendre la protection de toutes les machines protégées du groupe dont la protection a été suspendue, cliquez sur **Reprendre la protection**, puis confirmez votre choix. Pour plus d'informations, voir [Suspendre et reprendre la réplication](#).
 - Pour actualiser les informations de tous les objets du groupe, cliquez sur **Actualiser les métadonnées**.
 - Pour suspendre la réplication de toutes les machines répliquées de ce groupe, sous Réplication, cliquez sur **Pause**. Pour plus d'informations, voir [Suspendre et reprendre la réplication](#).
 - Pour reprendre la réplication de toutes les machines répliquées de ce groupe dont la réplication a été suspendue, sous Réplication, cliquez sur **Reprendre**. Pour plus d'informations, voir [Suspendre et reprendre la réplication](#).
 - Pour forcer la réplication de toutes les machines protégées de ce groupe, sous Réplication, cliquez sur **Forcer**. Pour plus d'informations, voir [Forcer la réplication](#).
 - Pour retirer la réplication de toutes les machines protégées de ce groupe, sous Réplication, cliquez sur **Retirer**. Pour plus d'informations, voir [Retirer une réplication entrante du Core cible](#).
 - Pour supprimer les machines comprenant uniquement des points de restauration de ce Core et ignorer les points de restauration, sous Points de restauration uniquement, cliquez sur **Supprimer les points de restauration**.

- Pour les groupes personnalisés uniquement, pour modifier le libellé d'un groupe personnalisé, cliquez sur **Modifier**. Pour plus d'informations, voir [Modifier les noms des groupes personnalisés](#).
- Pour les groupes personnalisés uniquement, pour supprimer un groupe personnalisé du menu de navigation, cliquez sur **Supprimer le libellé**. Pour plus d'informations, voir [Supprimer des groupes personnalisés](#).

Afficher toutes les machines d'un groupe personnalisé sur une seule page

En cliquant sur le nom d'un groupe personnalisé, vous accédez à la page Machines qui répertorie toutes les machines du groupe personnalisé. Vous pouvez effectuer certaines fonctions sur toutes les machines à partir du menu Actions, ou vous pouvez effectuer des fonctions de manière individuelle en choisissant des commandes depuis chacune des machines individuelles.

À propos de la protection de plusieurs machines

Vous pouvez ajouter la protection simultanée de deux machines Windows ou plus sur le Core Rapid Recovery à l'aide de l'Assistant Protéger plusieurs machines. Pour protéger vos données à l'aide de Rapid Recovery, vous devez ajouter les stations de travail et les serveurs à protéger dans la console Core Rapid Recovery ; par exemple votre serveur Exchange, votre serveur SQL, votre serveur Linux, etc.

Comme pour la protection de machines individuelles, la protection simultanée de plusieurs machines vous oblige à installer le logiciel Agent Rapid Recovery sur chaque machine à protéger.

REMARQUE : exception à cette règle : pour protéger des machines virtuelles sur un hôte ESXi ou VMware, vous pouvez utiliser une protection sans agent. Pour en savoir plus, notamment sur les restrictions relatives à la protection sans agent, voir [Comprendre l'Instantané rapide pour Virtual](#).

Les machines protégées doivent être configurées avec une règle de sécurité permettant l'installation à distance.

La connexion aux machines exige que celles-ci soient sous tension et accessibles.

Il existe plusieurs méthodes pour déployer le logiciel Agent sur plusieurs machines simultanément. Par exemple :

- Vous pouvez installer le logiciel Agent Rapid Recovery sur plusieurs machines à l'aide de l'Assistant de déploiement du logiciel Agent. Pour plus d'informations, voir [Déploiement du logiciel Agent Rapid Recovery sur une ou plusieurs machines](#).
- Vous pouvez déployer le logiciel Agent Rapid Recovery à l'aide de l'Assistant Protéger plusieurs machines.

Le processus de protection de plusieurs machines comprend des étapes facultatives auxquelles vous pouvez accéder si vous sélectionnez une configuration avancée. Les options avancées comprennent les fonctions de la logithèque et le chiffrement. Par exemple, vous pouvez spécifier une logithèque Rapid Recovery existante pour enregistrer les instantanés, ou en créer une nouvelle. Vous pouvez également spécifier une clé de chiffrement existante (ou en ajouter une nouvelle) afin de l'appliquer aux données enregistrées sur le Core pour les machines protégées.

Le flux de travail de l'assistant Protéger plusieurs machines peut varier légèrement selon votre environnement. Par exemple, si le logiciel Agent Rapid Recovery est déjà installé sur les machines à protéger, vous n'êtes pas invité à l'installer dans l'Assistant. De la même manière, si une logithèque existe déjà sur le Core, le système ne demande pas d'en créer une.

Pour protéger plusieurs machines, suivez la procédure appropriée, en fonction de votre configuration. Voir les options suivantes pour protéger plusieurs machines :

- [Protéger plusieurs machines sur un domaine Active Directory](#)
- [Protection de plusieurs machines sur un hôte virtuel ESX\(i\)/ VMware vCenter](#)
- [Protection manuelle de plusieurs machines](#)

Protéger plusieurs machines sur un domaine Active Directory

Cette procédure permet de protéger simultanément une ou plusieurs machines d'un même domaine Active Directory.

- 1 Dans la console Core Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis sur **Protéger plusieurs machines**.

L'Assistant de protection de plusieurs machines s'ouvre.

- 2 Dans la page **Bienvenue** de l'assistant, sélectionnez l'une des options suivantes :
 - Normal
 - Avancé (afficher des étapes facultatives)
- 3 Cliquez sur **Suivant**.
- 4 Dans la page **Connexion** de l'assistant, dans la liste déroulante **Source**, sélectionnez **Active Directory**.
- 5 Entrez les informations de domaine et les identifiants comme dans le tableau suivant.

Tableau 79. Informations de domaine et identifiants

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP du domaine Active Directory.
Nom d'utilisateur	Le nom d'utilisateur servant à se connecter au domaine ; par exemple, Administrateur (ou, si la machine se trouve dans un domaine, [nom de domaine]\Administrateur).
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à ce domaine.

- 6 Cliquez sur **Suivant**.
- 7 Dans la page **Sélectionner des machines** de l'assistant, sélectionnez les machines à protéger :
Le système vérifie automatiquement chacune des machines que vous avez sélectionnées.
- 8 Cliquez sur **Suivant**.
Si la page **Protection** s'affiche ensuite dans l'Assistant de protection de plusieurs machines, passez à l'étape 11.
Si le logiciel Agent n'est pas encore déployé sur les machines à protéger, ou si l'une des machines que vous avez spécifiées ne peut être protégée pour une autre raison, les machines sélectionnées apparaissent dans la page Avertissements.
- 9 Dans la page **Avertissements** de l'assistant, vous avez également la possibilité de vérifier une machine en la sélectionnant et en cliquant sur **Vérifier** dans la barre d'outils.
- 10 Si vous souhaitez, dans la page **Avertissements**, vous pouvez sélectionner **Après l'installation d'Agent, redémarrer automatiquement les machines**.
i REMARQUE : Dell recommande cette option. Vous devez redémarrer les machines d'agent pour qu'elles puissent être protégées.
- 11 Si l'état indique que la machine est accessible, cliquez sur **Suivant** pour installer Rapid Recovery.
La page **Protection** s'affiche.
- 12 Dans la page **Protection** de l'assistant, sélectionnez la planification de protection appropriée décrite ci-après.
 - Pour utiliser la planification de protection par défaut, dans l'option Paramètres de planification, sélectionnez **Protection par défaut (instantanés toutes les heures de tous les volumes)**.
 - Si vous souhaitez définir un planning de protection différent, dans l'option Paramètres de planification, sélectionnez **Protection personnalisée**.
- 13 Effectuez la configuration comme suit :
 - Si vous avez sélectionné une configuration standard dans l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine spécifiée.
Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.
 - Si vous avez sélectionné une configuration normale pour l'Assistant de protection de machines et défini une protection personnalisée, cliquez sur **Suivant**. Voir [Créer des planifications de protection personnalisées](#).
 - Si vous avez sélectionné la configuration avancée pour l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Suivant** et passez à l'[étape 15](#) pour afficher les options de référentiel et de chiffrement.
 - Si vous avez sélectionné une configuration standard pour l'Assistant de protection de machines et défini une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à [Créer des planifications de protection personnalisées](#).
- 14 Cliquez sur **Suivant**.
- 15 Dans la page **Référentiel** de l'assistant, effectuez l'une des opérations suivantes :

- Si vous disposez déjà d'un référentiel et que vous souhaitez y stocker les données de cette machine pour sa protection, procédez de la façon suivante :
 - 1 Sélectionnez **Utiliser un référentiel existant**.
 - 2 Sélectionnez un référentiel existant dans la liste.
 - 3 Cliquez sur **Suivant**.

La page **Chiffrement** s'affiche. Passez à l'étape 19 pour éventuellement définir le chiffrement.

- Si vous souhaitez créer un référentiel, sélectionnez **Créer un référentiel**, puis effectuez les opérations décrites ci-après.
 - 1 Dans la page **Référentiel**, entrez les informations décrites dans le tableau suivant.

Tableau 80. Ajouter les paramètres du nouveau référentiel

Zone de texte	Description
Nom de référentiel	Entrez le nom d'affichage du référentiel. Par défaut, cette zone de texte contient le mot Repository et un numéro, qui correspond au nombre de référentiels de ce core. Par exemple, s'il s'agit du premier référentiel, son nom par défaut est Repository 1. Modifiez le nom si nécessaire. Les noms de référentiels doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas caractères interdits ni expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que votre référentiel devra prendre en charge. La valeur par défaut est 64.
Commentaires	(Optionnel) Entrez une note décrivant ce référentiel. Vous pouvez entrer jusqu'à 254 caractères. Par exemple, tapez Référentiel DVM 2 .

- 2 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.

⚠ PRÉCAUTION : Définissez un dossier dédié au sein de la racine de l'emplacement de stockage de votre référentiel. Ne spécifiez pas l'emplacement racine. Par exemple, utilisez E:\Repository\ et non E:\. Si le référentiel que vous créez à cette étape est supprimé ultérieurement, tous les fichiers de son emplacement de stockage seront supprimés. Si vous définissez votre emplacement de stockage à la racine, tous les autres fichiers dans le volume (par ex., E:\) seront également supprimés, ce qui pourrait entraîner une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.

- 3 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.
- 4 Dans la zone **Emplacement de stockage**, spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage connecté localement (par exemple en tant que stockage à connexion directe, un réseau de zone de stockage, ou un stockage connecté par réseau). Vous pouvez également spécifier un volume de stockage sur un emplacement partagé CIFS (Common Internet File System).
 - Sélectionnez **Ajouter un fichier sur disque local** pour spécifier une machine locale, puis entrez les informations décrites dans le tableau suivant.

Tableau 81. Paramètres du disque local

Zone de texte	Description
Chemin de données	Entrez l'emplacement de stockage des données protégées. Par exemple, entrez X:\Repository\Data. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées.

Zone de texte	Description
	Par exemple, entrez X:\Repository\Metadata.
	Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

- Vous pouvez également cliquer sur **Ajouter le fichier sur un partage CIFS** pour spécifier un emplacement de partage réseau, puis entrez les informations décrites dans le tableau suivant.

Tableau 82. Identifiants pour le partage CIFS

Zone de texte	Description
Chemin UNC	Entrez le chemin de l'emplacement du partage réseau. Si cet emplacement se trouve à la racine, définissez un nom de dossier dédié (par exemple, Repository). L'extension de fichier doit commencer par \\. Lorsque vous spécifiez ce chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Les lettres a à z peuvent être en majuscules ou en minuscules. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe pour accéder à l'emplacement du partage réseau.

- Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails** et entrez les détails de l'emplacement de stockage décrits dans le tableau suivant.

Tableau 83. Détails de la configuration du stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille minimale est de 1 Go. La valeur par défaut est de 250 Go. Vous pouvez choisir parmi les options suivantes : - Go - To ① REMARQUE : La taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) sous Windows XP ou Windows 7, la taille de fichier est limitée à 16 To. Si l'emplacement de stockage est un volume NTFS sous Windows 8, 8.1, Windows 10, ou Windows Server 2012, 2012 R2, la taille de fichier est limitée à 256 To. ① REMARQUE : Pour que Rapid Recovery puisse valider le système d'exploitation, WMI (Windows Management Instrumentation) doit être installé sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle l'utilisation du Windows Cache Manager dans le référentiel et facilite le réglage du référentiel pour des performances optimales sur différentes configurations. Définissez l'option sur une des valeurs suivantes : - Activé - Éteint - Synchroniser Si la fonction est définie comme activée (valeur par défaut), Windows contrôle la mise en cache. Cette option est appropriée pour Windows 10, et pour les versions de Windows Server 2012 et ultérieur.

Zone de texte	Description
	REMARQUE : L'activation de la stratégie de mise en cache d'écriture peut améliorer la vitesse des performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, il est recommandé de désactiver cette stratégie. Si la fonction est désactivée, c'est Rapid Recovery qui contrôle la mise en cache. Si la fonction est définie sur Synchroniser, Windows contrôle la mise en cache et les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets que devrait comprendre chaque secteur. La valeur par défaut est 512.
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

6 Cliquez sur **Suivant**.

Si vous avez choisi l'option **Avancé** à l'étape 1, la page **Chiffrement** s'affiche.

- 16 Si vous le souhaitez, dans la page **Chiffrement** de l'assistant, pour activer le chiffrement, sélectionnez **Activer le chiffrement**.
Les champs Clé de chiffrement apparaissent dans la page Chiffrement.

REMARQUE : Si vous l'activez, le chiffrement sera appliqué aux données de tous les volumes protégés de cette machine. Vous pouvez modifier ultérieurement les paramètres à partir de la console Core Rapid Recovery. Pour plus d'informations sur le chiffrement, reportez-vous à la rubrique [Comprendre les clés de clés de chiffrement](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining, chaînage des blocs de chiffrement) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous recommande vivement de créer une clé de clé de chiffrement et de protéger la phrase de passe que vous définissez. Stockez cette phrase de passe dans un endroit sûr, car elle est d'une importance capitale pour la restauration des données. Sans la phrase de passe, la restauration des données est impossible.

- 17 Si vous souhaitez chiffrer ces machines protégées à l'aide d'une clé de chiffrement qui est déjà définie dans ce core Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement**, puis sélectionnez la clé appropriée dans le menu déroulant. Passez à l'étape 19.
- 18 Si vous souhaitez ajouter au core une nouvelle clé de chiffrement et appliquer cette clé à ces machines protégées, entrez les informations décrites dans le tableau suivant.

Tableau 84. Paramètres de clé de chiffrement

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement. Les noms de clés de chiffrement doivent contenir entre 1 et 130 caractères alphanumériques. Vous ne pouvez pas inclure de caractères spéciaux (barre oblique inverse, barre oblique normale, barre verticale, deux-points, astérisque, guillemets, point d'interrogation, parenthèse ouvrante ou fermante, et commercial, dièse).
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lors de l'affichage des clés de chiffrement dans la console Core.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès. La bonne pratique consiste à éviter d'utiliser les caractères spéciaux mentionnés ci-dessus. Notez la phrase de passe dans un endroit sûr. Le support Dell ne peut pas récupérer de phrase de passe. Une fois que vous avez créé une clé de chiffrement et que vous l'avez appliquée à une ou plusieurs machines protégées, vous ne pourrez pas restaurer les données si vous perdez la phrase de passe.

Zone de texte	Description
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.
19	Cliquez sur Terminer pour enregistrer et appliquer vos paramètres. L'assistant se ferme.
20	Si, malgré la page Avertissements , vous êtes satisfait de vos sélections, cliquez à nouveau sur Terminer .

Le logiciel Rapid Recovery Agent se déploie si nécessaire vers les machines spécifiées, qui tombent sous la protection du core.

Protection de plusieurs machines sur un hôte virtuel ESX(i)/ VMware vCenter

Suivez cette procédure pour protéger simultanément une ou plusieurs machines sur un hôte virtuel ESX(i)/ VMware vCenter.

PRÉCAUTION : si vous optez pour la protection sans agent, Dell recommande de la limiter à 200 MV à la fois au maximum. Par exemple, ne sélectionnez pas plus de 200 MV dans l'assistant Protection de plusieurs machines. Dans le cas contraire, les performances s'en trouvent ralenties. Il n'y a aucune limite au nombre de MV qu'un Noyau peut protéger sans agent au cours du temps. Par exemple, vous pourriez protéger 200 MV aujourd'hui et 200 autres demain.

- 1 Dans la console du Noyau de la Rapid Recovery, cliquez sur le menu déroulant **Protection**, puis sur **Protection de plusieurs machines**.
L'assistant Protection de plusieurs machines s'ouvre.
- 2 Sur la page d'accueil, sélectionnez l'une des options suivantes :
 - Par défaut
 - Avancée (afficher les étapes facultatives)
- 3 Cliquez sur **Suivant**.
- 4 Sur la page Connexion de l'assistant, depuis la liste déroulante intitulée **Source**, sélectionnez **vCenter/ ESX(i)**.
- 5 Saisissez les identifiants de connexion et les informations de l'hôte, comme il est décrit dans le tableau suivant.

Tableau 85. Paramètres de connexion vCenter/ ESX(i)

Zone de texte	Description
Hôte	Le nom ou l'adresse IP de l'hôte virtuel ESX(i)/ VMware vCenter.
Port	Le port utilisé pour se connecter à l'hôte virtuel. La valeur par défaut est 443.
Nom d'utilisateur	Le nom utilisé pour se connecter à l'hôte virtuel. Par exemple, Administrateur ou, si la machine se trouve dans un domaine, [nom du domaine]\Administrateur.
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à cet hôte virtuel.

- Pour choisir la protection sans agent, sélectionnez **Protection sans agent des MV sélectionnées**, puis consultez [Protéger des machines virtuelles vCenter/ESXi sans Rapid Recovery Agent](#).
- 6 Sur la page Machines à sélectionner, sélectionnez l'une des options suivantes, à partir du menu déroulant :
 - Hôtes et clusters
 - MV et modèles
 - 7 Développez la liste des machines, puis sélectionnez les MV que vous souhaitez protéger.
Une notification apparaît si la Rapid Recovery détecte une machine hors ligne ou ne disposant pas de VMware Tools.
 - 8 Cliquez sur **Suivant**.
 - 9 Sur la page Ajustements, saisissez les identifiants de connexion pour chaque machine, selon le format suivant :
hostname::username::password.

REMARQUE : saisissez une machine par ligne.

- 10 Cliquez sur **Suivant**.
Si la page Protection apparaît ensuite dans l'assistant Protection de plusieurs machines, passez à l'étape 14.

Si le logiciel Agent n'est pas encore déployé sur les machines que vous souhaitez protéger, ou si l'une des machines que vous avez déterminées ne peut être protégée pour toute autre raison, alors les machines sélectionnées apparaissent sur la page Avertissements.

- 11 Il est également possible, sur la page Avertissements, de vérifier n'importe quelle machine en la sélectionnant et en cliquant sur **Vérifier** dans la barre d'outils.
- 12 Vous pouvez également sélectionner **Après l'installation de l'Agent, redémarrer les machines automatiquement** sur la page Avertissements.

REMARQUE : Dell recommande cette option, puisqu'il vous faut redémarrer les machines agents avant que la protection ne prenne effet.

- 13 Si l'état indique que la machine est joignable, cliquez sur **Suivant** pour installer le logiciel agent.
La page Protection s'affiche.
 - 14 Sur la page Protection, sélectionnez la planification appropriée pour la protection, comme il est décrit ci-dessous.
 - Si vous souhaitez utiliser la planification de protection par défaut, sélectionnez **Protection par défaut (instantanés horaires de tous les volumes)** dans l'option Paramètres de la planification.
 - Si vous souhaitez définir une planification de protection différente, sélectionnez **Protection personnalisée** dans l'option Paramètres de la planification.
 - 15 Configurez comme suit :
 - Si vous avez sélectionné une configuration Par défaut dans l'assistant Protection de machines et avez spécifié une protection par défaut, cliquez alors sur **Terminer** pour confirmer vos choix, fermer l'assistant et protéger la machine que vous avez indiquée.
La première fois qu'une protection est appliquée à une machine, une image de base (c'est-à-dire un instantané de toutes les données présentes dans les volumes protégés) sera transférée à la logithèque du Noyau de la Rapid Recovery en fonction de la planification que vous avez définie, à moins que vous n'ayez initialement spécifié la suspension de la protection.
 - Si vous avez sélectionné une configuration Par défaut dans l'assistant Protection de machines et avez spécifié une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la configuration d'une planification de protection personnalisée, veuillez consulter [Créer des planifications de protection personnalisées](#).
 - Si vous avez sélectionné une configuration Avancée dans l'assistant Protection de machines et avez spécifié une protection par défaut, cliquez sur **Suivant** et passez à l'[étape 17](#) pour connaître les options de chiffrement et de logithèques.
 - Si vous avez sélectionné une configuration Avancée dans l'assistant Protection de machines et avez spécifié une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la configuration d'une planification de protection personnalisée, veuillez consulter [Créer des planifications de protection personnalisées](#).
 - 16 Cliquez sur **Suivant**.
 - 17 Sur la page **Logithèque**, effectuez l'une des actions suivantes :
 - Si vous disposez déjà d'une logithèque et souhaitez stocker les données de cette machine dans une logithèque existante pour les protéger, procédez comme suit :
 - 1 Sélectionnez **Utiliser une logithèque existante**.
 - 2 Sélectionnez une logithèque existante dans la liste.
 - 3 Cliquez sur **Suivant**.
- La page **Chiffrement** s'affiche. Passez à l'[étape 18](#) pour configurer le chiffrement au moyen des options.
- Si vous souhaitez créer une logithèque, sélectionnez **Créer une logithèque**, puis procédez comme suit.
 - 1 Sur la page **Logithèque**, saisissez les informations comme il est décrit dans le tableau suivant.

Tableau 86. Paramètres de la page Ajouter une nouvelle logithèque

Zone de texte	Description
Nom de la logithèque	Saisissez le nom d'affichage de la logithèque. Par défaut, cette zone de texte est constituée du mot Logithèque et d'un chiffre, qui correspond au nombre de logithèques qui existent pour ce Noyau. Par exemple, pour la première logithèque, le nom par défaut est Logithèque 1. Modifiez le nom selon vos besoins.

Zone de texte	Description
	Les noms des logithèques doivent comprendre entre 1 et 40 caractères alphanumériques, incluant les espaces. N'utilisez pas caractères interdits , ni expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que la logithèque peut prendre en charge. La valeur par défaut est 64.
Commentaires	Vous avez la possibilité de saisir une note descriptive concernant la logithèque. Vous pouvez saisir jusqu'à 254 caractères. Par exemple, saisissez Logithèque DVM 2 .

- 2 Cliquez sur **Ajouter un emplacement de stockage** pour préciser le volume ou l'emplacement de stockage spécifique pour la logithèque. Ce volume doit être un emplacement de stockage principal.

⚠ PRÉCAUTION : définissez un dossier dédié présent dans la racine pour être l'emplacement de stockage de votre logithèque. Ne spécifiez pas l'emplacement de la racine directement. Par exemple, utilisez E:\Repository\ et non simplement E:\. Si la logithèque que vous créez lors de cette étape est par la suite supprimée, tous les fichiers se trouvant dans l'emplacement de stockage de votre logithèque le seront également. Si vous avez défini la racine comme emplacement de stockage, tous les autres fichiers du volume (par exemple, E:\) seront supprimés, ce qui peut représenter une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.

- 3 Cliquez sur **Ajouter un emplacement de stockage** pour préciser le volume ou l'emplacement de stockage spécifique pour la logithèque. Ce volume doit être un emplacement de stockage principal.
- 4 Dans la zone **Emplacement de stockage**, spécifiez comment ajouter le fichier à l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage attaché localement (comme un stockage à connexion directe, un SAN ou un NAS). Vous pouvez également spécifier un volume de stockage sur un emplacement partagé CIFS.
 - Sélectionnez **Ajouter un fichier sur un disque local** pour spécifier une machine locale, puis saisissez les informations nécessaires, comme il est décrit dans le tableau suivant.

Tableau 87. Paramètres du disque local

Zone de texte	Description
Chemin d'accès aux données	Saisissez l'emplacement de destination pour le stockage des données protégées. Par exemple, saisissez X:\Repository\Data. Lorsque vous spécifiez le chemin d'accès, utilisez des caractères alphanumériques, le trait d'union et le point (seulement pour séparer les noms d'hôtes et les domaines). La barre oblique inverse est utilisée uniquement pour définir les niveaux du chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
Chemin d'accès aux métadonnées	Saisissez l'emplacement de destination pour le stockage des métadonnées protégées. Par exemple, saisissez X:\Repository\Metadata. Lorsque vous spécifiez le chemin d'accès, utilisez des caractères alphanumériques, le trait d'union et le point (seulement pour séparer les noms d'hôtes et les domaines). La barre oblique inverse est utilisée uniquement pour définir les niveaux du chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
• Ou encore, sélectionnez Ajouter un fichier sur un partage CIFS pour spécifier un emplacement de partage réseau, puis saisissez les informations nécessaires, comme il est décrit dans le tableau suivant.	

Tableau 88. Identifiants du partage CIFS

Zone de texte	Description
Chemin UNC	Saisissez le chemin de l'emplacement du partage réseau. Si cet emplacement se trouve à la racine, précisez un nom de dossier dédié (par exemple, Repository). Le chemin doit commencer par \\. Lorsque vous spécifiez le chemin d'accès, utilisez des caractères alphanumériques, le trait d'union et le point (seulement pour séparer les noms d'hôtes et

Zone de texte	Description
	les domaines). Les lettres de a à z sont sensibles à la casse. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe pour accéder à l'emplacement du partage réseau.

- 5 Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails**, puis saisissez les informations détaillées relatives à l'emplacement de stockage, comme il est décrit dans le tableau suivant.

Tableau 89. Informations détaillées de la configuration du stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille minimale est 1 Go. La taille par défaut est de 250 Go. Vous avez le choix entre : - Go - To REMARQUE : la taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) sur lequel se trouve Windows XP ou Windows 7, la limite de taille est 16 To. Si l'emplacement de stockage est un volume NTFS sur lequel se trouve Windows 8, Windows 8.1, Windows 10, Windows Server 2012 ou Windows Server 2012 R2, la limite de taille est de 256 To. REMARQUE : pour que la Rapid Recovery valide le système d'exploitation, l'infrastructure de gestion Windows (WMI) doit être installée sur l'emplacement de stockage prévu.
Stratégie de mise en cache de l'écriture	La stratégie de mise en cache de l'écriture contrôle l'utilisation du Gestionnaire de cache de Windows dans la logithèque et facilite son réglage pour des performances optimales sur différentes configurations. Paramétrez l'option sur une des valeurs suivantes : - Activer - Désactiver - Synchroniser Si l'option est paramétrée sur Activer (valeur par défaut), Windows contrôle la mise en cache. Ceci est particulièrement indiqué pour Windows 10 et pour Windows Server 2012 et versions ultérieures. REMARQUE : définir la stratégie de mise en cache de l'écriture sur Activer peut accélérer les performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, la valeur recommandée est Désactiver. Si l'option est paramétrée sur Désactiver, la Rapid Recovery contrôle la mise en cache. Si la fonction est définie sur Synchroniser, Windows contrôle la mise en cache et les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets que devrait comprendre chaque secteur. La valeur par défaut est 512.
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8 192.

- 6 Cliquez sur **Suivant**.

Si vous avez choisi l'option **Avancé** lors de l'étape 1, la page **Chiffrement** s'affiche.

- 18 Vous avez aussi la possibilité d'activer le chiffrement sur la page Chiffrement. Pour cela, sélectionnez **Activer le chiffrement**. Les champs des clés de chiffrement apparaissent sur la page Chiffrement.

❶ **REMARQUE** : si vous activez le chiffrement, celui-ci sera appliqué à toutes les données contenues dans les volumes protégés de cette machine agent. Vous pouvez modifier les paramètres ultérieurement depuis l'onglet Configuration situé dans la console du Noyau de la Rapid Recovery. Pour plus d'informations sur le chiffrement, veuillez consulter la section [Comprendre les clés de clés de chiffrement](#).

⚠ **PRÉCAUTION** : la Rapid Recovery utilise une méthode de chiffrement AES sur 256 bits en mode CBC (chaînage de chiffrement de blocs) avec des clés de 256 bits. Bien que le chiffrement soit facultatif, Dell vous recommande de créer une clé de chiffrement et de protéger la phrase de sécurité que vous avez définie. Conservez la phrase de sécurité dans un emplacement sûr, puisqu'elle est essentielle à la récupération des données. Sans cette phrase de sécurité, la récupération des données est impossible.

- 19 Si vous souhaitez chiffrer ces machines protégées à l'aide d'une clé de chiffrement déjà définie sur ce Noyau de la Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement existante**, puis sélectionnez la clé appropriée dans le menu déroulant.
Passez à l'étape 21.
- 20 Si vous souhaitez ajouter une nouvelle clé de chiffrement au Noyau et appliquer cette clé aux machines protégées, saisissez alors les informations nécessaires, comme il est décrit dans le tableau suivant.

Tableau 90. Paramètres des clés de chiffrement

Zone de texte	Description
Nom	Saisissez un nom pour la clé de chiffrement. Les noms des clés de chiffrement doivent comprendre entre 1 et 130 caractères alphanumériques. Cependant, aucun caractère spécial ne peut être saisi, dont l'oblique, l'oblique inverse, la barre verticale, les deux-points, l'astérisque, les guillemets, le point d'interrogation, les parenthèses (ouvrante et fermante), l'esperluette ou le croisillon.
Description	Saisissez un commentaire pour la clé de chiffrement. Ces informations apparaissent dans le champ Description lorsque vous visualisez des clés de chiffrement depuis la console du Noyau.
Phrase de sécurité	Saisissez la phrase de sécurité utilisée pour contrôler l'accès. Il est recommandé de ne pas utiliser les caractères spéciaux listés ci-dessus. Notez et enregistrez la phrase de sécurité dans un emplacement sûr. Le service d'assistance Dell ne peut pas récupérer une phrase de sécurité. Une fois que vous avez créé une clé de chiffrement et l'avez appliquée à une ou plusieurs machines, il vous sera impossible de récupérer les données si vous ne disposez plus de cette phrase de sécurité.
Confirmer la phrase de sécurité	Saisissez de nouveau la phrase de sécurité.

- 21 Cliquez sur **Terminer** pour enregistrer et appliquer vos paramètres.
- 22 Si la page Avertissements apparaît et que vous êtes satisfait de vos choix, cliquez à nouveau sur **Terminer**.

Le logiciel Agent de la Rapid Recovery est déployé sur les machines spécifiées, si nécessaire, et les machines sont ajoutées à la protection sur le Noyau.

Protection manuelle de plusieurs machines

Procédez comme suit pour saisir manuellement chaque machine à protéger. Cela est utilisé, par exemple, dans le cadre de la protection de machines Linux.

- 1 Dans la Rapid Recovery Core Console, cliquez sur le menu déroulant **Protéger**, puis sur **Protéger plusieurs machines**.
L'Assistant Protéger plusieurs machines s'ouvre.
- 2 Sur la page **Bienvenue**, sélectionnez l'une des options suivantes :
 - Par défaut

- Avancé (afficher les étapes facultatives)
- 3 Cliquez sur **Suivant**.
 - 4 Sur la page **Connexion** de l'Assistant, sélectionnez **Manuellement** dans la liste déroulante **Source**.
 - 5 Cliquez sur **Suivant**.
 - 6 Sur la page **Sélectionner les machines**, entrez les détails de la machine dans la boîte de dialogue au format suivant :
`hostname::username::password::port`. Le paramètre Port est facultatif. Voici des exemples :
`10.255.255.255::administrator::&11@yYz90z::8006`
`abc-host-00-1::administrator::99!zU$o83r::168`
 - 7 Cliquez sur **Suivant**.
 Si la page **Protection** s'affiche ensuite dans l'Assistant Protéger plusieurs machines, passez à l'[étape 11](#).
 Si le logiciel Agent n'est pas encore déployé sur les machines à protéger ou que l'une des machines spécifiées ne peut pas être protégée pour une raison quelconque, les machines sélectionnées s'affichent sur la page **Avertissements**.
 - 8 Sur la page **Avertissements sur les machines**, vous pouvez vérifier toutes les machines en les sélectionnant puis en cliquant sur **Vérifier** dans la barre d'outils.
 - 9 Sur la page **Avertissements sur les machines**, vous pouvez sélectionner **Après installation d'Agent, redémarrer les machines automatiquement**.

REMARQUE : Dell recommande cette option. Vous devez redémarrer les machines agents pour qu'elles puissent être protégées. En effet, ce redémarrage garantit l'exécution du service Agent et, le cas échéant, l'utilisation du module de noyau adéquat pour protéger la machine.
 - 10 Si l'état indique que la machine est accessible, cliquez sur **Suivant** pour installer le logiciel Agent.
 La page **Protection** s'affiche.
 - 11 Sur la page **Protection**, sélectionnez les planifications de protection appropriées, tel que décrit ci-dessous.
 - Pour utiliser la planification de protection par défaut, dans l'option Paramètres de planification, cliquez sur **Protection par défaut (instantanés de tous les volumes toutes les heures)**.
 - Pour définir une planification de protection différente, dans l'option Paramètres de planification, sélectionnez **Protection personnalisée**.
 - 12 Poursuivez la configuration comme suit :
 - si vous avez sélectionné une configuration standard dans l'assistant Protéger une machine et que vous avez spécifié la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'assistant et protéger la machine que vous avez spécifiée.
 Lorsque vous ajoutez pour la première fois la protection d'une machine, une image de base (instantané de toutes les données des volumes protégés) sera transférée vers la logithèque du Core Rapid Recovery conformément à la planification définie, sauf si vous avez demandé la suspension initiale de la protection.
 - Si vous avez sélectionné une configuration standard pour l'Assistant Protéger une machine et spécifié une protection personnalisée, cliquez sur **Suivant**. Voir [Créer des planifications de protection personnalisées](#).
 - Si vous avez sélectionné une configuration avancée pour l'Assistant Protéger une machine et spécifié la protection par défaut, cliquez sur **Suivant** et passez à l'[étape 14](#) pour afficher les options de logithèque et de chiffrement.
 - Si vous avez sélectionné une configuration avancée pour l'Assistant Protéger une machine et spécifié une protection personnalisée, cliquez sur **Suivant** pour définir une planification de protection personnalisée. Pour obtenir de plus amples informations sur la définition d'une planification de protection personnalisée, voir [Créer des planifications de protection personnalisées](#).
 - 13 Sur la page **Logithèque**, ce qui suit s'applique :
 - Si vous disposez déjà d'une logithèque et souhaitez stocker les données de cette machine dans la logithèque existante à des fins de protection, procédez comme suit :
 - 1 Sélectionnez **Utiliser une logithèque existante**.
 - 2 Sélectionnez une logithèque existante dans la liste.
 - 3 Cliquez sur **Suivant**.

La page **Cryptage** s'affiche. Passez à l'[étape 19](#) pour définir un chiffrement facultatif.
 - Si vous souhaitez créer une logithèque, sélectionnez **Créer une logithèque**, puis procédez comme suit.
 - 1 Sur la page **Logithèque**, saisissez les informations présentées dans le tableau suivant.

Tableau 91. Paramètres Ajouter une nouvelle logithèque

Zone de texte	Description
Nom de la logithèque	Entrez le nom d'affichage de la logithèque. Par défaut, cette zone de texte contient le mot Logithèque et un numéro, qui correspond au numéro des logithèques de ce Core. Par exemple, s'il s'agit de la première logithèque, le nom par défaut est Logithèque 1. Modifiez les noms selon vos besoins. Les noms de logithèques doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas de caractères interdits ou de expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que doit prendre en charge la logithèque. Par défaut, la valeur est 64.
Commentaires	(Facultatif) Entrez une note descriptive concernant cette logithèque. Vous pouvez entrer jusqu'à 254 caractères. Par exemple, saisissez Logithèque DVM 2 .

- 2 Cliquez sur **Ajouter un emplacement de stockage** pour définir le volume ou l'emplacement de stockage spécifique de cette logithèque. Ce volume doit être un emplacement de stockage principal.

⚠ PRÉCAUTION : définissez un dossier dédié à la racine de l'emplacement de stockage de votre logithèque. Ne spécifiez pas l'emplacement racine. Par exemple, utilisez E:\Repository\, et non E:\. Si la logithèque créée lors de cette étape est supprimée ultérieurement, tous les fichiers présents dans l'emplacement de stockage de la logithèque sont supprimés. Si vous définissez votre emplacement de stockage à la racine, tous les autres fichiers du volume (par exemple, E:\) sont supprimés, ce qui pourrait entraîner une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** s'affiche.

- 3 Cliquez sur **Ajouter un emplacement de stockage** pour définir le volume ou l'emplacement de stockage spécifique de cette logithèque. Ce volume doit être un emplacement de stockage principal.
- 4 Dans la zone **Emplacement de stockage**, indiquez comment vous souhaitez ajouter le fichier de l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage à connexion locale (par exemple un périphérique de stockage DAS [Direct Attached Storage], SAN [Storage Area Network] ou NAS [Network Attached Storage]). Vous pouvez également spécifier un volume de stockage dans un emplacement partagé CIFS (Common Internet File System).
 - Cliquez sur **Ajouter le fichier sur le disque local** pour indiquer une machine locale, puis entrez les informations, tel que décrit dans le tableau suivant.

Tableau 92. Paramètres du disque local

Zone de texte	Description
Chemin de données	Indiquez l'emplacement de stockage des données protégées. Par exemple, saisissez X:\Repository\Data. Lorsque vous spécifiez le chemin, n'utilisez que des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôte et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées. Par exemple, saisissez X:\Repository\Metadata. Lorsque vous spécifiez le chemin, n'utilisez que des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôte et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.

- Ou bien, cliquez sur **Ajouter le fichier sur le partage CIFS** pour indiquer un emplacement de partage réseau, puis entrez les informations, tel que décrit dans le tableau suivant.

Tableau 93. Identifiants du partage CIFS

Zone de texte	Description
chemin UNC	Entrez le chemin du partage réseau. Si cet emplacement est à la racine, définissez un nom de dossier dédié (par exemple, Repository). Le chemin doit commencer par \\. Lorsque vous spécifiez le chemin, n'utilisez que des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôte et les domaines). Les lettres a à z sont sensibles à la casse. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe permettant d'accéder à l'emplacement du partage réseau.

- 5 Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails**, puis saisissez les informations de l'emplacement de stockage, comme indiqué dans le tableau suivant.

Tableau 94. Détails de la configuration de stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité pour l'emplacement de stockage. La taille minimale est de 1 To. La valeur par défaut est 250 Mo. Vous pouvez choisir parmi les options suivantes : • Go • To ❗ REMARQUE : la taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) qui utilise Windows XP ou Windows 7, la limite de taille du fichier est de 16 To. Si l'emplacement de stockage est un volume NTFS qui utilise Windows 8, 8.1, Windows 10 ou Windows Server 2012, 2012 R2, la limite de taille de fichier est de 256 To. ❗ REMARQUE : pour que Rapid Recovery valide le système d'exploitation, vous devez installer Windows Management Instrumentation (WMI) sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle la façon dont le gestionnaire de cache Windows est utilisé dans la logithèque. Elle vous aide également à paramétrer la logithèque pour optimiser les performances dans différentes configurations. Affectez à ce paramètre l'une des valeurs suivantes : • Activé • Désactivé • Synchroniser Si la valeur est Activé, la valeur par défaut, Windows contrôle la mise en cache. Cette option est utile pour Windows 10 et pour les versions de Windows Server 2012 et ultérieures. ❗ REMARQUE : la définition de la stratégie de mise en cache d'écriture sur la valeur Activé peut permettre d'améliorer les performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, le paramétrage recommandé est Désactivé. Si la fonction est définie sur Désactivé, Rapid Recovery contrôle la mise en cache. Si la valeur est Synchroniser, Windows contrôle la mise en cache, ainsi que les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets de chaque secteur. La valeur par défaut est 512.

Zone de texte	Description
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

6 Cliquez sur **Suivant**.

Si vous avez choisi l'option **Avancé** à l'étape 1, la page **Chiffrement** s'affiche.

- 14 Éventuellement, sur la page **Chiffrement**, vous pouvez activer le chiffrement en sélectionnant **Activer le chiffrement**.
Les champs de clé de chiffrement s'affichent sur la page **Chiffrement**.

REMARQUE : si vous activez le chiffrement, celui-ci sera appliqué aux données de tous les volumes protégés de cette machine. Vous pourrez modifier les paramètres ultérieurement sur la page Clés de chiffrement de la Rapid Recovery Core Console. Pour en savoir plus sur le chiffrement, voir la rubrique [Comprendre les clés de clés de chiffrement](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous conseille vivement d'établir une clé de chiffrement, et de protéger la phrase secrète que vous définissez. Conservez la phrase secrète dans un lieu sûr, car elle est indispensable à la restauration des données. Sans phrase secrète, la restauration des données est impossible.

- 15 Si vous souhaitez chiffrer ces machines protégées à l'aide d'une clé de chiffrement déjà définie dans ce Core Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement existante**, puis choisissez la clé appropriée dans le menu déroulant.
Passez à l'étape 17.
- 16 Si vous voulez ajouter une nouvelle clé de chiffrement au Core et l'appliquer à ces machines protégées, entrez les informations tel que décrit dans le tableau suivant.

Tableau 95. Paramètres de la clé de chiffrement

Zone de texte	Description
Nom	Entrez le nom de la clé de chiffrement. Les noms des clés de chiffrement doivent contenir entre 1 et 130 caractères alphanumériques. Vous ne devez pas inclure de caractères spéciaux comme une barre oblique penchée vers l'arrière ou vers l'avant, une barre verticale, un astérisque, un guillemet, un point d'interrogation, une parenthèse ouverte ou fermée, une esperluette ou un dièse.
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lorsque vous regardez les clés de chiffrement de Core Console.
Phrase secrète	Entrez la phrase secrète servant au contrôle des accès. Il est conseillé d'éviter d'une manière générale d'employer les caractères spéciaux cités ci-dessus. Conservez la phrase secrète à un emplacement sûr. Le support technique de Dell ne peut pas récupérer une phrase secrète. Après avoir créé une clé de chiffrement et après l'avoir appliquée à une ou plusieurs machines protégées, vous ne pourrez plus récupérer les données si vous perdez la phrase secrète.
Confirmez la phrase secrète	Entrez de nouveau la phrase secrète que vous venez d'entrer.

- 17 Cliquez sur **Terminer** pour enregistrer et appliquer vos paramètres.
L'assistant se ferme.
- 18 Si la page **Avertissement** s'affiche et que vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel Agent Rapid Recovery est déployé sur les machines spécifiées, si nécessaire, et la protection des machines est ajoutée sur le Core.

Surveiller la protection de plusieurs machines

Vous pouvez suivre l'avancement de l'application par Rapid Recovery des stratégies de protection et des planifications sur les machines.

Dans la console Core Rapid Recovery, accédez à la page Accueil de Rapid Recovery, puis cliquez sur  (Événements).

La page **Événements** s'affiche. Elle contient trois sections : Tâches, Alertes et Événements. Au cours du transfert des volumes, l'état et les heures de début et de fin s'affichent dans le volet Tâches.

Vous pouvez également filtrer les tâches par état (active, en attente, terminée, en file d'attente et échouée). Pour plus d'informations, voir [Affichage des tâches](#).

 **REMARQUE :** pour afficher uniquement les tâches en attente d'exécution, veillez à cliquer sur l'icône Tâches en attente.

Lors de l'ajout d'une nouvelle machine, une alerte est enregistrée pour indiquer si l'opération a réussi ou que des erreurs ont été enregistrées. Pour plus d'informations, voir [Afficher les alertes](#).

Pour en savoir plus sur l'affichage de tous les événements, voir [Afficher tous les événements](#).

Paramètres et fonctions des serveurs Exchange protégés

Si vous protégez un serveur Microsoft Exchange Server dans votre Core, vous pouvez configurer divers paramètres et fonctions supplémentaires utiles dans la Rapid Recovery Core Console.

La Core Console associée au serveur Exchange ne propose qu'un seul paramètre : **Activer la vérification automatique de montabilité**. Si cette option est activée, la vérification de la montabilité s'effectue automatiquement sur le serveur Exchange. Ce paramètre est disponible lorsque l'état de la machine protégée est vert (Actif) ou jaune (En pause).

Pour en savoir plus, voir [À propos des vérifications de la montabilité de la base de données Exchange](#).

Vous pouvez également vérifier la montabilité de façon ponctuelle en accédant au volet Points de restauration d'un serveur Exchange protégé. Pour en savoir plus, voir [Forcer une vérification de montabilité d'une base de données Exchange](#).

La liste suivante répertorie les fonctions pouvant être exécutées sur un serveur Exchange protégé par le Core.

- **Définition d'informations d'identification sur un serveur Exchange.** Le Core Rapid Recovery vous permet de définir des informations d'identification qui permettent au Core de s'authentifier auprès du serveur Exchange et d'obtenir des informations.
Pour en savoir plus sur la définition d'informations d'identification sur des serveurs Exchange, voir [Définition des références pour un serveur Exchange](#).
- **Troncature des journaux Exchange.** Lorsque vous forcez la troncature des journaux d'un serveur Exchange, ce processus identifie l'espace disponible et le récupère sur le serveur Exchange protégé.
Pour en savoir plus sur la troncature des journaux d'un serveur Exchange à la demande, voir [Forcer la troncature de journal pour une machine Exchange](#). Vous pouvez également exécuter ce processus dans le cadre d'une tâche nocturne.
- **Forcement d'une vérification de montabilité d'une base de données Exchange.** Cette fonction vérifie que les bases de données Exchange peuvent être montées, détecte la corruption et alerte les administrateurs afin de garantir la restauration de l'ensemble des données du serveur Exchange.
Pour en savoir plus sur la vérification forcée de la montabilité à la demande, voir [Forcer une vérification de montabilité d'une base de données Exchange](#).

Vous pouvez également forcer une vérification automatique de la montabilité après chaque instantané. Pour en savoir plus sur les vérifications de la montabilité, voir [À propos des vérifications de la montabilité de la base de données Exchange](#).

- **Forcement d'une vérification de somme de contrôle des points de restauration d'un serveur Exchange.** Cette fonction vérifie l'intégrité des points de restauration contenant les fichiers de la base de données Exchange.
Pour en savoir plus sur la vérification forcée de la somme de contrôle à la demande, voir [Forçage de la vérification de la somme de contrôle des fichiers de bases de données Exchange](#).

Vous pouvez tronquer les journaux Exchange et forcer une vérification de somme de contrôle dans le cadre d'une tâche nocturne. Pour en savoir plus sur les tâches pouvant être planifiées la nuit, voir [Comprendre les travaux nocturnes](#). Pour en savoir plus sur l'exécution de tâches nocturnes, voir [Configuration des tâches nocturnes du Core](#).

Définition des références pour un serveur Exchange

Afin de définir les références de connexion, un serveur Exchange doit être présent sur un volume protégé. Si Rapid Recovery ne détecte pas la présence d'un serveur Exchange la fonction Définir les références n'apparaît pas dans la console Core.

Lorsque vous protégez les données d'un serveur Microsoft Exchange, vous pouvez définir des références de connexion dans la console Core de Rapid Recovery.

Effectuez les étapes de cette procédure pour définir des identifiants pour chaque serveur Exchange.

- 1 Dans la zone de navigation de gauche de la console Core de Rapid Recovery, sélectionnez la machine protégée où se trouve le serveur Exchange pour lequel vous souhaitez définir les références.
La page **Récapitulatif** du serveur Exchange s'affiche.
- 2 Sur la page **Récapitulatif**, au niveau des liens en haut de la page, cliquez sur la flèche vers le bas ▼ à droite du menu Exchange puis, à partir du menu déroulant qui s'affiche, sélectionnez **Définir les références**.
La boîte de dialogue **Modifier les références Exchange** pour le serveur Exchange protégé s'affiche.
- 3 Dans la boîte de dialogue **Modifier les références d'Exchange**, entrez vos références comme suit :
 - a Dans le champs de texte du **Nom d'utilisateur**, entrez le nom d'un utilisateur disposant d'autorisations sur le serveur Exchange ; par exemple, Administrateur (ou si la machine se trouve dans un domaine, [nom du domaine]\Administrateur).
 - b Dans le champ de texte du **Mot de passe**, entrez le mot de passe du nom d'utilisateur que vous avez défini pour la connexion au serveur Exchange.
 - c Cliquez sur **OK** pour confirmer les paramètres et fermer la boîte de dialogue.

Forcer la troncature de journal pour une machine Exchange

Pour forcer une troncature de journal, une base de données Exchange doit être présente sur un volume protégé. Si Rapid Recovery ne détecte pas la présence d'une base de données, la fonction de troncature de journal n'apparaît pas dans la console Core.

Lorsque vous forcez la troncature de journal pour un serveur Exchange protégé, la taille des journaux est réduite. Suivez cette procédure pour forcer la troncature de journal à la demande.

- 1 Dans la zone de navigation gauche de la console Core de Rapid Recovery, sélectionnez le serveur Exchange protégé dont vous souhaitez forcer la troncature de journal.
La page **Résumé** de la machine protégée s'affiche.
- 2 Dans la partie supérieure de la page, cliquez sur le menu déroulant **Exchange** puis sélectionnez **Forcer la troncature de journal**.
- 3 Dans la boîte de dialogue qui s'affiche, cliquez pour confirmer que vous souhaitez forcer la troncature de journal.
La boîte de dialogue se ferme. Le système démarre la troncature des journaux du serveur Exchange. Si les alertes Toast sont activées pour ce type d'événement, un message indiquant que la troncature de journal démarre s'affiche.

À propos des vérifications de la montabilité de la base de données Exchange

Lorsque vous réalisez des sauvegardes de serveurs Microsoft Exchange à l'aide de Rapid Recovery, vous pouvez vérifier la montabilité de l'ensemble des bases de données Exchange après chaque instantané. Cette fonction de détection d'endommagement signale aux administrateurs les pannes potentielles et garantit que toutes les données des serveurs Exchange seront récupérées en cas de panne.

Pour activer ou désactiver cette fonction, accédez au menu **Paramètres** d'une machine protégée, puis réglez l'option **Activer la vérification automatique de montabilité** sur Oui ou Non respectivement. Pour en savoir plus sur la modification des paramètres d'une machine protégée, voir [Paramètres d'affichage et de modification des machines protégées](#).

Les vérifications de la montabilité ne sont pas incluses dans les paramètres des tâches nocturnes. Toutefois, si l'option Vérification automatique de montabilité et la tâche nocturne Tronquer les journaux Exchange sont activées, la vérification de montabilité se déclenche une fois la troncature des journaux terminée.

Vous pouvez également vérifier la montabilité de façon ponctuelle en accédant au volet **Points de restauration** d'un serveur Exchange protégé. Pour en savoir plus, voir [Forcer une vérification de montabilité d'une base de données Exchange](#).

REMARQUE : les vérifications de montabilité s'appliquent uniquement à Microsoft Exchange 2007, 2010 et 2013. De plus, vous devez attribuer le rôle d'administrateur organisationnel au compte du service de l'agent Rapid Recovery dans Exchange.

Forcer une vérification de montabilité d'une base de données Exchange

Pour forcer une vérification de montabilité, une base de données Exchange doit être présente sur un volume protégé. Si Rapid Recovery ne détecte pas la présence d'une base de données, la fonction de vérification de la montabilité n'apparaît pas dans la console Core.

Suivez cette procédure pour forcer le système à effectuer une vérification de montabilité pour un point de restauration de serveur Exchange à la demande.

- 1 Dans la zone de navigation gauche de la console Core de Rapid Recovery, sélectionnez la machine pour laquelle vous souhaitez forcer la vérification de montabilité, puis cliquez sur le menu **Points de restauration**.
- 2 Faites défiler l'écran vers le bas jusqu'au volet **Points de restauration**.
- 3 Naviguez dans les points de restauration pour trouver le point de restauration souhaité. Vous pouvez également cliquer sur la flèche ► (Développer) à droite d'un point de restauration dans la liste pour développer la vue.
Dans les informations développées du point de restauration, vous pouvez voir les volumes inclus dans le point de restauration.
- 4 Dans le volet **Points de restauration**, sur la ligne représentant le point de restauration souhaité, cliquez sur  puis, à partir du menu déroulant, sélectionnez **Forcer la vérification de montabilité**.
- 5 Dans la boîte de dialogue qui s'ouvre, cliquez pour confirmer que vous souhaitez forcer une vérification de montabilité.
La boîte de dialogue se ferme. Le système effectue une vérification de montabilité. Si les alertes Toast sont activées pour ce type d'événement, un message indiquant que la vérification de montabilité démarre s'affichera.

Pour savoir comment afficher le statut des vérifications de capacité d'attachement, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Forçage de la vérification de la somme de contrôle des fichiers de bases de données Exchange

Pour forcer une vérification de somme de contrôle, une base de données Exchange doit être présente sur un volume protégé. Si Rapid Recovery ne détecte pas la présence d'une base de données, la fonction de vérification de somme de contrôle n'apparaît pas dans la console Core.

Suivez cette procédure pour forcer le système à effectuer une vérification de somme de contrôle pour un point de restauration de serveur Exchange.

- 1 Dans la zone de navigation gauche de la console Core de Rapid Recovery, sélectionnez le serveur Exchange protégé pour lequel vous souhaitez forcer la vérification de somme de contrôle, puis cliquez sur le menu **Points de restauration**.
La page **Points de restauration** s'affiche pour le serveur Exchange protégé.
- 2 Faites défiler vers le bas jusqu'au volet **Points de restauration**.
- 3 Parcourez les points de restauration jusqu'à trouver le point de restauration souhaité. Vous pouvez également cliquer sur la flèche ► (Développer) à droite d'un point de restauration dans la liste pour développer la vue.
Les informations du point de restauration développé indiquent les volumes inclus dans le point de restauration.
- 4 Dans le volet **Recovery Points** (Points de restauration), sur la ligne représentant le point de restauration souhaité, cliquez sur  (Paramètres), puis sélectionnez **Forcer la vérification de somme de contrôle** dans le menu déroulant.
- 5 Dans la boîte de dialogue qui s'affiche, cliquez pour confirmer que vous souhaitez forcer la vérification de somme de contrôle.

La boîte de dialogue se ferme. Le système effectue une vérification de somme de contrôle. Si les alertes Toast sont activées pour ce type d'événement, un message indiquant que la vérification de somme de contrôle démarre s'affiche.

Pour savoir comment afficher le statut des vérifications de somme de contrôle, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Paramètres et fonctions des serveurs SQL protégés

Si vous protégez un serveur Microsoft SQL Server dans votre Core, vous pouvez configurer divers paramètres et fonctions supplémentaires utiles dans la Rapid Recovery Core Console.

La Core Console associée à SQL Server ne propose qu'un seul paramètre : **Capacité d'attachement**.

Le Core Rapid Recovery vous permet de vérifier la capacité d'attachement SQL et de contrôler l'intégrité des points de restauration contenant des bases de données SQL. Cette action vérifie la cohérence des bases de données SQL et garantit que les fichiers MDF (données) et LDF (journaux) associés sont bien disponibles dans l'instantané de sauvegarde.

Dans les anciennes versions, la vérification de la capacité d'attachement SQL nécessitait l'installation d'une version sous licence de SQL Server sur la machine Core. À présent, le Core Rapid Recovery vous permet de vérifier la capacité d'attachement en ouvrant une instance de SQL Server sur le Core ou en utilisant une version sous licence de SQL Server sur une machine SQL Server protégée.

Les paramètres de la capacité d'attachement vous permettent d'indiquer la version sous licence de SQL Server utilisée pour effectuer cette vérification. Pour en savoir plus sur la configuration des paramètres de la capacité d'attachement, voir [Gestion des paramètres de capacité d'attachement SQL du Core](#).

Pour en savoir plus sur la capacité d'attachement SQL, voir [À propos de la capacité d'attachement SQL](#).

La liste suivante répertorie les fonctions pouvant être exécutées sur un serveur SQL protégé par le Core.

- **Définition d'informations d'identification sur un serveur SQL.** Le Rapid Recovery Core vous permet de définir des informations d'identification qui permettent au Core de s'authentifier auprès du serveur SQL et d'obtenir des informations. Vous pouvez définir des informations d'identification pour un serveur SQL protégé ou définir des informations d'identification par défaut pour tous les serveurs SQL protégés.
Pour en savoir plus sur la définition d'informations d'identification sur des serveurs SQL, voir [Définir des identifiants de connexion pour un serveur SQL](#).
- **Troncature des journaux SQL.** Lorsque vous forcez la troncature des journaux d'un serveur SQL, ce processus identifie l'espace disponible sur le serveur protégé. Ce processus ne récupère aucun espace.
Pour en savoir plus sur la troncature des journaux d'un serveur SQL à la demande, voir [Forcer la troncature de journal pour une machine SQL](#).
- **Forcement de la vérification de la capacité d'attachement d'un serveur SQL.** Cette fonction vérifie la cohérence des bases de données SQL et garantit que les fichiers MDF (données) et LDF (journaux) associés sont bien disponibles dans l'instantané de sauvegarde.
Pour en savoir plus sur le forçement d'une vérification de la capacité d'attachement d'un serveur SQL à la demande, voir [Forçement de la vérification de la capacité d'attachement d'un serveur SQL](#).

Hormis la définition d'informations d'identification, chacune des fonctions décrites ci-dessus peut être exécutée à la demande, ou configurée pour s'exécuter dans le cadre des tâches nocturnes du Core. Pour en savoir plus sur les tâches pouvant être planifiées la nuit, voir [Comprendre les travaux nocturnes](#). Pour en savoir plus sur l'exécution des tâches nocturnes, voir [Configuration des tâches nocturnes du Core](#).

Définir des identifiants de connexion pour un serveur SQL

Vous devez ajouter la protection de la machine SQL Server sur le Core Rapid Recovery avant de suivre cette procédure. Pour en savoir plus sur la protection de machines, voir [Protéger une machine](#).

Lorsque vous protégez des données sur une machine SQL Server, vous pouvez définir les informations d'identification d'une seule instance ou de tous les serveurs SQL dans la console Core Rapid Recovery.

Suivez les étapes de cette procédure pour définir les références de chaque serveur SQL.

- 1 Dans la zone de navigation de gauche de la console Core Rapid Recovery, sélectionnez la machine SQL Server protégée dont vous souhaitez définir les références.
La page **Synthèse** s'affiche pour le serveur SQL protégé.
- 2 Dans les liens de la partie supérieure de la page **Synthèse**, cliquez sur la flèche vers le bas ▼ à droite du menu SQL, puis dans le menu déroulant qui s'affiche, effectuez l'une des opérations suivantes :
 - Si vous souhaitez définir les références par défaut de toutes les instances de base de données SQL Server, cliquez sur **Définir les références par défaut pour toutes les instances**, puis dans la boîte de dialogue de **Modifier les références par défaut**, procédez comme suit :
 - 1 Dans le champ de texte **Nom d'utilisateur**, saisissez le nom d'un utilisateur disposant d'autorisations sur tous les serveurs SQL associés ; par exemple, Administrateur (ou si la machine se trouve dans un domaine, [nom du domaine]\Administrateur).
 - 2 Dans le champ de texte **Mot de passe**, saisissez le mot de passe du nom d'utilisateur spécifié pour la connexion au serveur SQL.
 - 3 Cliquez sur **OK** pour confirmer les paramètres et fermer la boîte de dialogue.
 - Si vous souhaitez définir les références d'une seule instance de base de données SQL Server, cliquez sur le nom d'affichage de la machine SQL Server protégée, puis dans la boîte de dialogue **Modifier les références de l'instance**, procédez comme suit :
 - 1 Sélectionnez le type de données de référence (par défaut, Windows ou SQL)
 - 2 Dans le champ de texte **Nom d'utilisateur**, saisissez le nom d'un utilisateur disposant d'autorisations sur le serveur SQL ; par exemple, Administrateur (ou si la machine se trouve dans un domaine, [nom du domaine]\Administrateur).
 - 3 Dans le champ de texte **Mot de passe**, saisissez le mot de passe du nom d'utilisateur spécifié pour la connexion au serveur SQL.
 - 4 Cliquez sur **OK** pour confirmer les paramètres et fermer la boîte de dialogue.

Forcer la troncature de journal pour une machine SQL

La troncature de journal est disponible pour les machines qui utilisent SQL Server. Suivez cette procédure pour forcer la troncature des journaux.

REMARQUE : Lorsqu'elle est exécutée pour une machine SQL, la troncature identifie l'espace libre sur un disque, mais ne réduit pas la taille des journaux.

- 1 Dans la zone de navigation gauche de la console Core de Rapid Recovery, sélectionnez la machine dont vous souhaitez forcer la troncature de journal.
La page **Résumé** correspondant à la machine protégée s'affiche.
- 2 Sur la page **Résumé** ou n'importe quelle page de cette machine protégée, cliquez sur le menu déroulant **SQL** en haut de la page et sélectionnez **Forcer la troncature de journal**.
- 3 Cliquez sur **Oui** pour confirmer que vous voulez forcer la troncature de journal.

À propos de la capacité d'attachement SQL

La capacité d'attachement SQL permet au Core Rapid Recovery de joindre des fichiers de base de données SQL principale (fichiers .MDF) et des fichiers journaux de base de données (fichiers .LDF) à l'instantané d'un serveur SQL protégé. L'instantané est capturé à l'aide d'une instance locale de Microsoft SQL Server.

Les utilisateurs de Rapid Recovery chargés de protéger les machines SQL Server peuvent choisir l'instance de SQL Server qui effectuera l'attachement et définir le mode d'exécution du processus (à la demande ou dans le cadre d'une tâche nocturne).

La vérification de la capacité d'attachement permet au Core de vérifier la cohérence des bases de données SQL et de s'assurer que les fichiers MDF et LDF sont bien disponibles dans l'instantané de sauvegarde.

Les vérifications de la capacité d'attachement peuvent être effectuées à la demande pour des points de restauration spécifiques ou dans le cadre d'une tâche nocturne.

Pour effectuer la vérification de la capacité d'attachement SQL à la demande, voir [Forcement de la vérification de la capacité d'attachement d'un serveur SQL](#). Pour effectuer la vérification de la capacité d'attachement SQL une fois par jour, lors de l'exécution de vos tâches nocturnes, activez l'option **Vérifier la capacité d'attachement des bases de données SQL** dans les tâches nocturnes. Pour en savoir plus sur la configuration des tâches nocturnes sur le Core, voir [Configuration des tâches nocturnes du Core](#). Pour en savoir plus sur la configuration des tâches nocturnes sur une machine spécifique (ici, un serveur SQL protégé), voir [Personnalisation des tâches nocturnes pour une machine protégée](#).

Dans les versions précédentes, l'installation et la configuration de la capacité d'attachement SQL sur la machine Core nécessitaient l'ouverture d'une instance locale de Microsoft SQL Server. À présent, le Core Rapid Recovery vous permet de vérifier la capacité d'attachement en ouvrant une instance de SQL Server sur le Core ou sur une machine SQL Server protégée. L'instance sélectionnée doit exécuter une version complète de SQL Server, achetée auprès de Microsoft ou d'un revendeur agréé. Microsoft ne permet pas l'utilisation de licences SQL passives.

L'instance de SQL Server indiquée sera ensuite utilisée pour toutes les vérifications de la capacité d'attachement. La capacité d'attachement est synchronisée entre les paramètres du Core et les tâches nocturnes. Par exemple, si vous choisissez d'utiliser l'instance Core de SQL Server pour exécuter vos tâches nocturnes, les vérifications de la capacité d'attachement à la demande utiliseront également le Core. À l'inverse, si vous choisissez d'utiliser une instance de SQL Server sur une machine protégée, toutes les vérifications de la capacité d'attachement (à la demande et nocturnes) utiliseront l'instance locale de la machine protégée.

Sélectionnez l'instance de SQL Server à utiliser lors du réglage des paramètres généraux du Core. Pour en savoir plus, voir [Gestion des paramètres de capacité d'attachement SQL du Core](#).

REMARQUE : pour vérifier la capacité d'attachement sur une machine SQL Server protégée, vous devez installer le logiciel agent Rapid Recovery sur ce serveur. La capacité d'attachement SQL ne prend pas en charge la protection sans agent.

La capacité d'attachement du Core Rapid Recovery prend en charge SQL Server 2005, 2008, 2008 R2, 2012 et 2014. Le compte utilisé pour effectuer le test doit posséder le rôle sysadmin (administrateur système) sur les instances de SQL Server.

Le format de stockage sur disque de SQL Server est le même que dans les environnements 64 bits et 32 bits et la capacité d'attachement fonctionne dans les deux versions. Une base de données détachée d'une instance de serveur s'exécutant dans un environnement peut être attachée sur une instance de serveur s'exécutant dans un autre environnement.

REMARQUE : la version de SQL Server sur le Core doit être égale ou supérieure à la version de SQL Server installée sur toutes les machines protégées.

Forcement de la vérification de la capacité d'attachement d'un serveur SQL

Pour forcer une vérification de la capacité d'attachement, une base de données SQL doit être présente sur un volume protégé. Si Rapid Recovery ne détecte pas la présence d'une base de données, la fonction de vérification de la capacité d'attachement n'apparaît pas dans la console Core.

Suivez cette procédure pour forcer le système à effectuer une vérification de capacité d'attachement pour un point de restauration de serveur SQL.

- 1 Dans le volet de navigation gauche de la console Core de Rapid Recovery, sélectionnez le serveur SQL protégé pour lequel vous souhaitez forcer la vérification de la capacité d'attachement, puis cliquez sur le menu **Points de restauration**.
- 2 Faites défiler l'écran vers le bas jusqu'au volet **Points de restauration**.
- 3 Parcourez les points de restauration jusqu'à trouver le point de restauration souhaité. Vous pouvez également cliquer sur la flèche (Développer) à droite d'un point de restauration dans la liste pour développer la vue.
Les informations du point de restauration développé indiquent les volumes inclus dans le point de restauration.
- 4 Dans le volet **Points de restauration**, sur la ligne représentant le point de restauration souhaité, cliquez sur  (Paramètres), puis sélectionnez **Forcer la vérification de la capacité d'attachement** dans le menu déroulant.
- 5 Dans la boîte de dialogue qui s'affiche, cliquez pour confirmer que vous souhaitez forcer la vérification de la capacité d'attachement.

La boîte de dialogue se ferme. Le système vérifie la capacité d'attachement.

Pour savoir comment afficher le statut de la vérification de capacité d'attachement, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Comprendre l'Instantané rapide pour Virtual

Installer le logiciel Agent de la Rapid Recovery vous permet de protéger les machines physiques et virtuelles présentes dans le Noyau de la Rapid Recovery. Les systèmes d'exploitation pris en charge sont indiqués dans la configuration matérielle de la section "Configuration du logiciel Agent de la Récupération rapide."

La Rapid Recovery propose désormais une nouvelle approche pour la protection des machines.

La fonctionnalité Rapid Snap for Virtual, également connue comme la protection sans agent, de la Rapid Recovery vous permet de protéger les machines virtuelles présentes sur un hôte Hyper-V ou VMware ESXi sans avoir à installer l'Agent de la Rapid Recovery sur chacune des MV.

⚠ PRÉCAUTION : Dell recommande de limiter la protection sans agent à 200 MV à la fois au maximum. Par exemple, ne sélectionnez pas plus de 200 MV dans l'assistant Protection de plusieurs machines. Dans le cas contraire, les performances s'en trouvent ralenties. Il n'y a aucune limite au nombre de MV qu'un Noyau peut protéger sans agent au cours du temps. Par exemple, vous pourriez protéger 200 MV aujourd'hui et 200 autres demain.

Protection des MV vCenter/ ESXi

La Rapid Recovery vous permet de protéger des MV vCenter/ ESXi sans avoir à installer l'Agent de la Rapid Recovery sur l'hôte ESXi ou de la MV, ce qui correspond à une protection sans agent. Pour protéger un environnement ESXi, le Noyau de la Rapid Recovery tire parti de la technologie d'instantanés native de VMware.

La protection sans agent de la Rapid Recovery utilise le client ESXi et l'interface de programmation d'applications (API) existante pour protéger les MV sélectionnées sur un même hôte sans avoir à installer le logiciel Agent de la Rapid Recovery. Le Noyau de la Rapid Recovery communique alors avec le disque de la machine virtuelle (VMDK) pour déterminer les détails nécessaires des volumes protégés. Étant donné que la Rapid Recovery crée des points de récupération basés sur les volumes, et non sur les VMDK, chacun de ces volumes peut être monté, restauré et exporté indépendamment.

❗ REMARQUE : la Rapid Recovery nécessite que VMware Tools soit installé sur les machines virtuelles (MV) que vous souhaitez protéger sur des hôtes vSphere ou ESXi. Lorsque VMware Tools est installé sur une MV sous un système d'exploitation Windows, les sauvegardes que le Noyau de la Rapid Recovery capture utilisent les Services de clichés instantanés de volume (VSS) de Microsoft. Pour plus d'informations sur le comportement des MV sans agent avec ou sans VMware Tools, veuillez consulter [Avantages liés à l'installation de VMware Tools pour la protection sans agent](#).

La protection sans agent utilise également le suivi des blocs modifiés (CBT, Changed Block Tracking) de VMware dans l'optique de réduire le temps nécessaire pour les instantanés par incréments. La fonction CBT identifie les blocs ayant été modifiés dans le fichier VMDK, permettant à la Rapid Recovery de sauvegarder uniquement les portions du disque ayant subi des modifications depuis le dernier instantané. Cette méthode permet des opérations de sauvegarde plus courtes et une consommation des ressources plus réduite des éléments de stockage et du réseau.

La protection sans agent présente de multiples avantages. Certains des plus importants sont les suivants :

- Aucun logiciel supplémentaire n'est nécessaire sur la machine hôte.
- Elle vous permet de choisir de protéger automatiquement les nouvelles MV ajoutées sur l'hôte ESXi.
- Un redémarrage n'est pas nécessaire lors du processus de protection.
- Des identifiants ne sont pas nécessaires pour chacune des MV.
- Elle vous permet de protéger une MV même lorsque cette dernière est hors tension.
- Elle vous permet d'effectuer des opérations de restauration sur des disques.

- Elle ne nécessite aucun espace disponible sur les volumes lors des transferts.
- Tous les systèmes d'exploitation sont compatibles avec la protection sans agent.
- Vous avez la possibilité d'exporter des volumes ou des disques dynamiques.

① REMARQUE : si la configuration des volumes dynamiques est complexe (en grappe, en miroir, fractionnés ou RAID), ils sont exportés en tant qu'images disques et redistribués en volumes une fois que l'opération d'exportation est terminée sur la MV exportée.

Bien qu'il existe de nombreuses raisons d'utiliser une protection sans agent pour les MV ESXi, il est sage de choisir la méthode de protection qui corresponde le plus à votre environnement et à vos besoins. En plus des avantages mentionnés précédemment, il faut également prendre ce qui suit en compte :

- Elle ne prend pas non plus en charge la protection de volumes dynamiques (par exemple, les volumes en grappe, en miroir, fractionnés ou RAID) au niveau du volume même. Elle les protège au niveau du disque.
- La Récupération en direct n'est pas prise en charge. Pour plus d'informations sur cette fonctionnalité, veuillez consulter [Compréhension des Live Recovery](#).
- Après chaque restauration d'un volume unique sur la MV protégée, vous devez redémarrer cette dernière.
- La protection sans agent ne collecte pas de métadonnées Microsoft SQL ou Microsoft Exchange.
- Il est impossible d'effectuer une vérification d'attachabilité SQL, une troncature de journal ou une vérification de montabilité sur les points de récupération capturés sur les machines protégées sans agent.
- Les étiquettes de volume et les lettres des lecteurs ne sont pas collectées ni affichées par la protection sans agent.
- La quantité réelle d'espace utilisé sur une MV n'est pas affichée si le disque virtuel est au format large avec effacement des données à la création du disque (thick provision eager zero).

Si vous choisissez d'utiliser la protection sans agent pour vos MV ESXi, et pour garantir le bon fonctionnement de la première, la configuration minimale de l'hôte doit être égale ou supérieure à ce qui suit :

- La machine hôte doit utiliser la version 5.0.0 et le numéro de build 623860 ou supérieur d'ESXi.
- La machine hôte doit satisfaire les exigences système minimales mentionnées dans le *Guide d'installation et de mise à niveau de la Rapid Recovery*.
- Pour une protection au niveau du volume, les VMDK doivent inclure soit des tables de partition MBR (« Master Boot Record », secteur de démarrage principal), soit des tables de partition GUID (GPT). Les VMDK ne disposant pas de ces tables de partition sont protégés en tant que disques entiers plutôt que comme volumes individuels.
- VMware Tools doit être installé sur chaque machine virtuelle VMware afin de garantir l'homogénéité des instantanés.

Protection des clusters et serveurs Hyper-V

Pour protéger un serveur Hyper-V sans agent, il n'est pas nécessaire d'installer l'Agent de la Rapid Recovery sur une quelconque MV. Il vous faut seulement l'installer sur le nœud de cluster ou sur la machine hôte. L'Agent protège le disque dur virtuel sur l'hôte et convertit les modifications apportées aux fichiers du disque dur en une image de volume ou une image disque, en fonction du système de fichiers. Un nouveau pilote fournit une assistance au niveau des fichiers pour les MV sur les hôtes et sur les volumes partagés au sein d'un cluster (CSV).

① REMARQUE : la Rapid Recovery prend en charge le format de fichiers VHDX et non le format VHD.

Pour protéger les MV présentes sur un CSV, le pilote et l'Agent de la Rapid Recovery doivent être installés sur chaque nœud du cluster au moyen de la fonctionnalité de déploiement automatique se trouvant dans l'assistant Protection de plusieurs machines. Depuis les nœuds, l'Agent peut protéger toutes les MV fonctionnant sur des CSV en créant deux types de modifications pour chacun des fichiers. Le premier est enregistré uniquement avant ou après un redémarrage causé par un instantané ou un nettoyage du système. Le second type de modification se trouve sur le disque et rend un instantané par incréments disponible même en cas de perte de courant ou d'arrêt incorrect. L'Agent installé sur le nœud fusionne toutes les modifications avant de transférer les données.

Lorsqu'un hôte ou un nœud est en cours d'exécution, la Rapid Recovery crée une sauvegarde homogène en termes d'application. Si l'hôte n'est pas en fonctionnement, aucune sauvegarde ne peut être effectuée ; cependant, si c'est un nœud qui n'est pas en cours d'exécution, la Rapid Recovery peut tout de même continuer la création d'instantanés des MV sur le cluster.

REMARQUE : pour des performances optimales, il est recommandé que le nombre maximal de transferts simultanés pour le nœud ou l'hôte Hyper-V soit défini sur 1, qui correspond au paramètre par défaut.

La protection Hyper-V sans agent possède la plupart des capacités des protections traditionnelles sur les MV où l'Agent est installé, dont :

- L'archivage
- La vérification de l'intégrité des points de récupération
- Le montage de points de récupération
- La détection automatique de nouvelles MV (seulement pour la protection sans agent)
- La réplication
- La restauration de MV
- La restauration de CSV
- La restauration sur CIFS en utilisant le format VHDX
- La restauration de fichiers dans un format VHDX invité
- Le cumul
- L'exportation virtuelle vers des MV sous Hyper-V ou d'autres hyperviseurs, dont ESXi, VMware Workstation et VirtualBox

Cependant, des limitations existent quand il s'agit de choisir une protection Hyper-V sans agent. Les fonctionnalités qui ne sont pas incluses comprennent :

- La vérification de l'intégrité du montage Exchange
- La vérification de l'attachabilité SQL
- La Récupération en direct
- La restauration de MV sur CIFS en utilisant le format VHD
- La restauration de fichiers dans un format VHD invité

REMARQUE : pour un instantané homogène en termes d'application, le contrôleur SCSI doit être installé sur chacune des MV. Sans ce contrôleur, l'instantané résulte nécessairement en un blocage.

Avantages liés à l'installation de VMware Tools pour la protection sans agent

Lorsque vous protégez des machines virtuelles (VM) sans utiliser Rapid Recovery Agent, Dell vous recommande d'installer VMware Tools sur les VM protégées des hôtes vSphere ou ESXi afin de tirer pleinement parti de la fonctionnalité Microsoft VSS (Volume Shadow Services).

La protection sans agent utilise la technologie d'instantané native de VMware pour sauvegarder les données protégées. Lorsque VMware Tools est installé sur une VM dotée d'un système d'exploitation Windows (SE), les sauvegardes capturées par le Core Rapid Recovery Core peuvent également utiliser VSS. Lorsque VMware Tools n'est pas installé, Rapid Recovery continue de capturer des instantanés, mais l'absence de ce logiciel peut affecter l'état des données sur votre machine virtuelle protégée.

Les données peuvent afficher l'un des deux états suivants :

- **Cohérence en cas d'incident.** Le système d'exploitation de la VM démarre et peut lire et analyser le système de fichiers.
- **Cohérence avec les applications.** Le système d'exploitation de la VM démarre et peut lire et analyser le système de fichiers. En outre, les fichiers des applications transactionnelles affichent un état cohérent. Par exemple, dans SQL Server, les journaux correspondent aux fichiers de la base de données, et la base de données s'ouvre facilement et rapidement.

Si vous restaurez une application transactionnelle dans un état cohérent en cas d'incident, la base de données revient au dernier état valide. Ce dernier état valide peut remonter au moment de l'incident, ou précéder l'incident. S'il précède l'incident, la base de données doit alors effectuer une restauration progressive afin de faire correspondre les fichiers de données aux informations des journaux. Ce processus prend du temps lors de l'ouverture initiale de la base de données et peut rallonger le démarrage de la machine.

Les conditions suivantes s'appliquent si VMware Tools est installé (ou non) et si la machine virtuelle est sous tension (ou non) :

Tableau 96. Conditions liées aux types de sauvegarde des VM

VMware Tools	VM sous tension	Type de sauvegarde
Non installé	Oui	Cohérence en cas d'incident
Non installé	Non (arrêt non planifié)	Cohérence en cas d'incident
Non installé	Non (arrêt planifié)	Cohérence avec les applications
Installé	Oui	Cohérence avec les applications
Installé	Non (arrêt non planifié)	Cohérence en cas d'incident
Installé	Non (arrêt planifié)	Cohérence avec les applications

Protéger des machines virtuelles vCenter/ESXi sans Rapid Recovery Agent

Procédez comme indiqué ci-après pour protéger sans agent des machines virtuelles ESXi.

REMARQUE : Rapid Recovery recommande que les outils VMware soient installés sur les machines virtuelles (VM) que vous souhaitez protéger sur des hôtes vSphere ou ESXi. Lorsque ces outils sont installés sur une machine virtuelle tournant sous Windows, les sauvegardes capturées par le core Rapid Recovery utilisent Microsoft Volume Shadow Services (VSS). Pour plus d'informations sur le comportement de machines virtuelles sans agent avec ou sans les outils VMware, voir [Avantages liés à l'installation de VMware Tools pour la protection sans agent](#).

PRÉCAUTION : Dell vous recommande de limiter la protection sans agent à un maximum de 200 VM à la fois. Par exemple, ne sélectionnez pas plus de 200 VM lorsque vous utilisez l'Assistant de protection de plusieurs machines. Protéger plus de 200 VM ralentit les performances. Il n'y a aucune limite au nombre de VM qu'un core peut protéger sans agent au fil du temps. Par exemple, vous pouvez protéger 200 VM aujourd'hui et 200 autres demain.

- 1 Dans la console Core Rapid Recovery, cliquez sur le menu déroulant **Protéger**, puis sur **Protéger plusieurs machines**. L'Assistant de protection de plusieurs machines s'ouvre.
- 2 Dans la page **Bienvenue**, sélectionnez l'une des options suivantes :
 - Normal
 - Avancé (afficher des étapes facultatives)
- 3 Cliquez sur **Suivant**.
- 4 Dans la page **Connexion** de l'assistant, dans la liste déroulante **Source**, sélectionnez **vCenter/ESXi(i)**.
- 5 Entrez les informations d'hôte et les identifiants comme dans le tableau suivant.

Tableau 97. Paramètres de connexion VCenter/ESXi(i)

Zone de texte	Description
Hôte	Le nom ou l'adresse IP du serveur VMware vCenter ou de l'hôte virtuel ESXi(i).
Port	Le port utilisé pour se connecter à l'hôte virtuel. Le paramètre par défaut est 443.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à l'hôte virtuel ; par exemple, Administrateur ou, si la machine se trouve dans un domaine, [nom de domaine] \Administrateur).
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à cet hôte virtuel.

- 6 Assurez-vous que **Protéger sans agent les VM sélectionnées** est bien sélectionné (cette option est sélectionnée par défaut).
- 7 Dans la page **Sélectionner des machines**, sélectionnez les VM que vous souhaitez protéger. Vous pouvez utiliser le menu déroulant pour afficher la liste des hôtes et des clusters ou une liste des machines virtuelles et des modèles.

REMARQUE : Le suivi VMware des blocs modifiés (CBT) doit être activée sur chacune des VM que vous souhaitez protéger. S'il n'est pas activé, Rapid Recovery active automatiquement CBT pour assurer la protection.

- 8 Si vous souhaitez protéger automatiquement de nouvelles machines virtuelles lors de leur ajout à l'hôte, sélectionnez **Protéger automatiquement les nouvelles machines**, puis effectuez les opérations décrites ci-après.
 - a Cliquez sur **Suivant**.
 - b Dans la page **Protection automatique**, sélectionnez les conteneurs auxquels vous prévoyez d'ajouter de nouvelles machines.
- 9 Cliquez sur **Suivant**.
- 10 Dans la page **Protection**, sélectionnez l'une des planifications de protection suivantes :
 - Pour utiliser la planification de protection par défaut, dans l'option Paramètres de planification, sélectionnez **Protection par défaut (instantanés toutes les heures de tous les volumes)**.
 - Si vous souhaitez définir un planning de protection différent, dans l'option Paramètres de planification, sélectionnez **Protection personnalisée**.
- 11 Effectuez la configuration comme suit :
 - Si vous avez sélectionné une configuration standard et choisi la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine spécifiée.

Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.
 - Si vous avez sélectionné une configuration standard et défini une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à [Créer des planifications de protection personnalisées](#).
 - Si vous avez sélectionné la configuration Avancée pour l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Suivant** et passez à l'[étape 13](#) pour afficher les options de référentiel et de chiffrement.
 - Si vous avez sélectionné une configuration standard pour l'Assistant de protection de machines et défini une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à [Créer des planifications de protection personnalisées](#).
- 12 Cliquez sur **Suivant**.
- 13 Dans la page **Référentiel**, les éléments suivants :
 - Si vous disposez déjà d'un référentiel et que vous souhaitez y stocker les données de cette machine pour sa protection, procédez de la façon suivante :
 - 1 Sélectionnez **Utiliser un référentiel existant**.
 - 2 Sélectionnez un référentiel existant dans la liste.
 - 3 Cliquez sur **Suivant**.

La page **Chiffrement** s'affiche. Passez à l'[étape 19](#) pour éventuellement définir le chiffrement.

 - Si vous souhaitez créer un référentiel, sélectionnez **Créer un référentiel**, puis effectuez les opérations décrites ci-après.
 - 1 Dans la page **Référentiel**, entrez les informations décrites dans le tableau suivant.

Tableau 98. Ajouter les paramètres du nouveau référentiel

Zone de texte	Description
Nom de référentiel	Entrez le nom d'affichage du référentiel. Par défaut, cette zone de texte contient le mot Repository et un numéro, qui correspond au nombre de référentiels de ce core. Par exemple, s'il s'agit du premier référentiel, son nom par défaut est Repository 1. Modifiez le nom si nécessaire. Les noms de référentiels doivent contenir entre 1 et 40 caractères alphanumériques, espaces compris. N'utilisez pas caractères interdits ni expressions interdites .
Opérations simultanées	Définissez le nombre de demandes simultanées que votre référentiel devra prendre en charge. La valeur par défaut est 64.
Commentaires	(Optionnel) Entrez une note décrivant ce référentiel. Vous pouvez entrer jusqu'à 254 caractères. Par exemple, tapez Référentiel DVM 2 .

- 2 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.

⚠ PRÉCAUTION : Définissez un dossier dédié au sein de la racine de l'emplacement de stockage de votre référentiel. Ne spécifiez pas l'emplacement racine. Par exemple, utilisez E:\Repository\ et non E:\. Si le référentiel que vous créez à cette étape est supprimé ultérieurement, tous les fichiers de son emplacement de stockage seront supprimés. Si vous définissez votre emplacement de stockage à la racine, tous les autres fichiers dans le volume (par ex., E:\) seront également supprimés, ce qui pourrait entraîner une perte de données catastrophique.

La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.

- 3 Cliquez sur **Ajouter un emplacement de stockage** pour définir l'emplacement spécifique du stockage du référentiel ou son volume. Ce volume doit être un emplacement de stockage principal.
- 4 Dans la zone **Emplacement de stockage**, spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez choisir d'ajouter un volume de stockage connecté localement (par exemple en tant que stockage à connexion directe, un réseau de zone de stockage, ou un stockage connecté par réseau). Vous pouvez également spécifier un volume de stockage sur un emplacement partagé CIFS (Common Internet File System).
 - Sélectionnez **Ajouter un fichier sur disque local** pour spécifier une machine locale, puis entrez les informations décrites dans le tableau suivant.

Tableau 99. Paramètres du disque local

Zone de texte	Description
Chemin de données	Entrez l'emplacement de stockage des données protégées. Par exemple, entrez X:\Repository\Data. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées. Par exemple, entrez X:\Repository\Metadata. Lorsque vous spécifiez le chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Vous pouvez utiliser la barre oblique inverse uniquement pour définir des niveaux dans le chemin. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

- Vous pouvez également cliquer sur **Ajouter le fichier sur un partage CIFS** pour spécifier un emplacement de partage réseau, puis entrez les informations décrites dans le tableau suivant.

Tableau 100. Identifiants pour le partage CIFS

Zone de texte	Description
Chemin UNC	Entrez le chemin de l'emplacement du partage réseau. Si cet emplacement se trouve à la racine, définissez un nom de dossier dédié (par exemple, Repository). L'extension de fichier doit commencer par \\. Lorsque vous spécifiez ce chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Les lettres a à z peuvent être en majuscules ou en minuscules. N'utilisez pas d'espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Nom d'utilisateur	Indiquez le nom d'utilisateur pour accéder à l'emplacement du partage réseau.
Mot de passe	Indiquez le mot de passe pour accéder à l'emplacement du partage réseau.

- 5 Dans la zone **Configuration du stockage**, cliquez sur **Plus de détails** et entrez les détails de l'emplacement de stockage décrits dans le tableau suivant.

Tableau 101. Détails de la configuration du stockage

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille minimale est de 1 Go. La valeur par défaut est de 250 Go. Vous pouvez choisir parmi les options suivantes : - Go - To REMARQUE : La taille spécifiée ne peut pas excéder la taille du volume. Si l'emplacement de stockage est un volume NTFS (New Technology File System) sous Windows XP ou Windows 7, la taille de fichier est limitée à 16 To. Si l'emplacement de stockage est un volume NTFS sous Windows 8, 8.1, Windows 10, ou Windows Server 2012, 2012 R2, la taille de fichier est limitée à 256 To. REMARQUE : Pour que Rapid Recovery puisse valider le système d'exploitation, WMI (Windows Management Instrumentation) doit être installé sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle l'utilisation du Windows Cache Manager dans le référentiel et facilite le réglage du référentiel pour des performances optimales sur différentes configurations. Définissez l'option sur une des valeurs suivantes : - Activé - Éteint - Synchroniser Si la fonction est définie comme activée (valeur par défaut), Windows contrôle la mise en cache. Cette option est appropriée pour Windows 10, et pour les versions de Windows Server 2012 et ultérieur. REMARQUE : L'activation de la stratégie de mise en cache d'écriture peut améliorer la vitesse des performances. Si vous utilisez Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, il est recommandé de désactiver cette stratégie. Si la fonction est désactivée, c'est Rapid Recovery qui contrôle la mise en cache. Si la fonction est définie sur Synchroniser, Windows contrôle la mise en cache et les entrées/sorties synchrones.
Octets par secteur	Spécifiez le nombre d'octets que devrait comprendre chaque secteur. La valeur par défaut est 512.
Nombre moyen d'octets par enregistrement	Spécifiez le nombre moyen d'octets par enregistrement. La valeur par défaut est 8192.

6 Cliquez sur **Suivant**.

Si vous avez choisi l'option **Avancé** à l'étape 1, la page **Chiffrement** s'affiche.

14 Si vous le souhaitez, dans la page Chiffrement, pour activer le chiffrement, sélectionnez **Activer le chiffrement**.

Les champs Clé de chiffrement apparaissent dans la page Chiffrement.

REMARQUE : Si vous l'activez, le chiffrement sera appliqué aux données de tous les volumes protégés de cette machine. Vous pouvez modifier ultérieurement les paramètres de chiffrement dans l'onglet Configuration de la console Core Rapid Recovery. Pour plus d'informations sur le chiffrement, reportez-vous à la rubrique [Comprendre les clés de chiffrement](#).

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining, chaînage des blocs de chiffrement) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous recommande vivement de créer une clé de chiffrement et de protéger la phrase de passe que vous définissez. Stockez cette phrase de passe dans un endroit sûr, car elle est d'une importance capitale pour la restauration des données. Sans la phrase de passe, la restauration des données est impossible.

- 15 Si vous souhaitez chiffrer ces machines protégées à l'aide d'une clé de chiffrement qui est déjà définie dans ce core Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement**, puis sélectionnez la clé appropriée dans le menu déroulant. Passez à l'étape 17.
- 16 Si vous souhaitez ajouter au core une clé de chiffrement et appliquer cette clé à ces machines protégées, entrez les informations décrites dans le tableau suivant.

Tableau 102. Paramètres de clé de chiffrement

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement. Les noms de clés de chiffrement doivent contenir entre 1 et 130 caractères alphanumériques. Vous ne pouvez pas inclure de caractères spéciaux (barre oblique inverse, barre oblique normale, barre verticale, deux-points, astérisque, guillemets, point d'interrogation, parenthèse ouvrante ou fermante, et commercial, dièse).
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lors de l'affichage des clés de chiffrement dans la console Core.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès. La bonne pratique consiste à éviter d'utiliser les caractères spéciaux mentionnés dans la description Nom de ce tableau. Notez la phrase de passe dans un endroit sûr. Le support Dell ne peut pas récupérer de phrase de passe. Une fois que vous avez créé une clé de chiffrement et que vous l'avez appliquée à une ou plusieurs machines protégées, vous ne pourrez pas restaurer les données si vous perdez la phrase de passe.
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.

- 17 Cliquez sur **Terminer**.
Rapid Recovery ajoute les VM sélectionnées et leur hôte à la liste des machines protégées.

Accéder aux diagnostics des machines protégées

Dans Rapid Recovery, vous pouvez télécharger et afficher des informations diagnostiques pour des machines protégées individuelles. En outre, Rapid Recovery permet de télécharger et d'afficher les données de journal du Core.

Pour accéder aux journaux, voir les procédures suivantes :

- [Téléchargement et affichage du fichier journal du Core](#)
- [Téléchargement et affichage du fichier journal d'une machine protégée](#)

Téléchargement et affichage du fichier journal d'une machine protégée

Si vous rencontrez des erreurs ou des problèmes avec une machine protégée, vous pouvez télécharger les journaux de cette machine afin de les consulter ou de les transmettre à votre représentant du support technique de Dell.

- 1 Dans la zone de navigation de gauche de la console Core, sous Machines protégées, cliquez sur la flèche pour développer le menu contextuel pour la machine protégée appropriée. Faites défiler vers le bas jusqu'à **Plus**, développez ce menu, puis sélectionnez **Journal de l'agent**.
La page **Télécharger le journal de l'agent** s'affiche.
- 2 Sur la page **Télécharger le journal de l'agent**, cliquez sur  **Cliquez ici pour commencer le téléchargement**.
- 3 Dans la boîte de dialogue **Ouverture d'AgentAppRecovery.log**, effectuez l'une des opérations suivantes :
 - Pour ouvrir le fichier journal, sélectionnez **Ouvrir avec**, choisissez une application (par exemple, Bloc-notes) permettant d'afficher le fichier journal texte, puis cliquez sur **OK**.
Le fichier AgentAppRecovery.log s'ouvre dans l'application sélectionnée.
 - Pour enregistrer le fichier localement, sélectionnez **Enregistrer le fichier**, puis cliquez sur **OK**.
Le fichier AgentAppRecovery.log est enregistré dans votre dossier Téléchargements. Il est possible de l'ouvrir à l'aide d'un éditeur de texte.

Téléchargement et affichage du fichier journal d'une machine protégée

Si vous rencontrez des erreurs ou des problèmes avec une machine protégée, vous pouvez télécharger les journaux de cette machine afin de les consulter ou de les transmettre à votre représentant du support technique de Dell.

- 1 Dans la zone de navigation de gauche de la Core Console, sous Machines protégées, cliquez sur la flèche pour développer le menu contextuel pour la machine protégée appropriée. Faites défiler vers le bas jusqu'à **Plus**, développez ce menu, puis sélectionnez **Journal de l'agent**.
La page **Télécharger le journal de l'agent** s'affiche.
- 2 Sur la page **Télécharger le journal de l'agent**, cliquez sur  **Cliquez ici pour lancer le téléchargement**.
- 3 Dans la boîte de dialogue **Ouverture d'AgentAppRecovery.log**, effectuez l'une des opérations suivantes :
 - Pour ouvrir le fichier journal, sélectionnez **Ouvrir avec**, choisissez une application (par exemple, Bloc-notes) permettant d'afficher le fichier journal texte, puis cliquez sur **OK**.
Le fichier AgentAppRecovery.log s'ouvre dans l'application sélectionnée.
 - Pour enregistrer le fichier localement, sélectionnez **Enregistrer le fichier**, puis cliquez sur **OK**.
Le fichier AgentAppRecovery.log est enregistré dans votre dossier Téléchargements. Il est possible de l'ouvrir à l'aide d'un éditeur de texte.

Liens connexes

[Téléchargement et affichage du fichier journal du Core](#)

Affichage de l'état d'une machine et des autres informations

Complétez cette procédure pour afficher l'état ainsi que les autres informations d'une machine.

Dans la console du Noyau de la Rapid Recovery, accédez à la machine protégée que vous souhaitez afficher.
Les informations concernant la machine s'affichent dans la page Récapitulatif. Les détails affichés incluent :

- Nom de l'hôte
- Dernier instantané pris
- Prochain instantané planifié
- État de chiffrement
- Numéro de version

Si Exchange Server est installé sur la machine, les informations détaillées du serveur sont également affichées et incluent :

- La dernière vérification de montabilité réussie
- La dernière vérification de somme de contrôle réussie
- Date de la dernière troncature des journaux

Les informations détaillées des volumes contenus sur cette machine s'affichent également et incluent :

- Le nom du volume
- La planification
- La planification actuelle
- Le prochain instantané
- Le type de système de fichiers
- L'espace utilisé sur l'espace total

Si vous avez installé SQL Server sur la machine, l'écran affiche aussi les informations détaillées de ce serveur, notamment :

L'état de la connexion

- Le nom
- Le chemin d'installation
- La version

Si Exchange Server est installé sur la machine, les informations détaillées du serveur et des banques de messagerie sont affichées et incluent :

- La version
- Le chemin d'installation
- Le chemin d'accès aux données
- Le nom de la base de données
- Le chemin des bases de données Exchange
- Le chemin des fichiers journaux
- Le préfixe des journaux
- Le chemin système
- Le type de banque de messagerie

Gérer les machines

Cette section décrit un ensemble de tâches que vous pouvez effectuer pour gérer les machines. Les sujets abordés sont les suivants :

- [Supprimer une machine](#)
- [Retirer la protection d'un cluster](#)
- [Afficher les informations sur la licence d'une machine](#)
- [Téléchargement et affichage du fichier journal d'une machine protégée](#)
- [Convertir un nœud de cluster protégé en machine protégée](#)

Supprimer une machine

Lorsque vous retirez la protection d'une machine sur le Core Rapid Recovery, vous avez le choix entre deux options : celle de conserver les points de restauration enregistrés jusqu'à présent sur le Core RR ou celle de supprimer les points de restauration. Si vous conservez les

points de restauration, vous obtenez ce que l'on appelle une machine à « points de restauration uniquement ». En utilisant ces points de restauration pour la machine qui a été supprimée de la protection actuelle, vous pouvez continuer à restaurer la machine ultérieurement, mais seulement jusqu'à son état tel qu'il avait été capturé dans un des points de restauration sauvegardés.

Si vous supprimez les points de restauration, cette opération supprime du Core Rapid Recovery toutes les données d'instantané de cette machine anciennement protégée.

 **PRÉCAUTION : si vous supprimez les points de restauration, vous ne serez plus en mesure de restaurer les données de cette machine.**

Suivez les étapes de la procédure ci-après pour retirer la protection d'une machine de votre environnement Rapid Recovery.

- 1 Dans la console Core Rapid Recovery, dans le volet de navigation de gauche se trouvant sous Machines protégées, cliquez sur la machine à supprimer.
- 2 Sur la page Synthèse de la machine appropriée, cliquez sur **Supprimer la machine**.
- 3 Dans la boîte de dialogue, si vous souhaitez également supprimer de la logithèque tous les points de restauration de cette machine, sélectionnez **Supprimer avec des points de restauration**.
- 4 Pour confirmer votre choix de supprimer la machine, cliquez sur **Oui**.
Rapid Recovery retire la protection de la machine et annule toutes les tâches actives de cette machine.

Annuler des opérations sur une machine

Vous pouvez annuler les opérations actuellement en cours d'exécution pour une machine. Vous pouvez spécifier d'annuler seulement l'instantané actif ou d'annuler toutes les opérations actives (notamment les exportations, répliquions, etc..)

- 1 À partir de la console Core Rapid Recovery, dans la zone de navigation de gauche se trouvant sous Machines protégées, cliquez sur la machine pour laquelle vous souhaitez annuler des opérations.
- 2 Cliquez sur **Événements**.
- 3 Cliquez sur l'icône Détails de la tâche à l'extrême droite pour l'événement ou l'opération en cours à annuler.
- 4 Dans la boîte de dialogue Surveiller la tâche active, cliquez sur **Annuler**.

Afficher les informations sur la licence d'une machine

Vous pouvez afficher les informations sur l'état de la licence active pour le logiciel Agent Rapid Recovery installé sur une machine protégée.

- 1 Dans la Rapid Recovery Core Console, accédez au menu Machines protégées et cliquez sur la machine à modifier.
La page **Synthèse** de la machine sélectionnée s'affiche.
- 2 Cliquez sur le menu **Paramètres**.
La page **Paramètres**, qui présente les paramètres de configuration de la machine sélectionnée, s'affiche.
- 3 Cliquez sur le lien **Octroi de licences** pour faire défiler la page Paramètres vers le bas de sorte à afficher les paramètres d'octroi de licences relatifs à la machine.
L'écran État s'ouvre et affiche des détails concernant la gestion de licence du produit.

VM export (Exportation NFS)

Cette section explique comment exporter un point de restauration pour créer une machine virtuelle.

À propos de l'exportation vers des machines virtuelles avec Rapid Recovery

À partir du Core Rapid Recovery, vous pouvez exporter un point de restauration à partir d'une logithèque vers une machine virtuelle. Ce processus, parfois qualifié d'exportation virtuelle, est un processus P2V (Physical-to-virtual, Physique-à-Virtuel) créant une machine virtuelle à partir d'un point de restauration. La machine virtuelle ainsi créée est un clone amorçable d'une machine protégée.

REMARQUE : le point de restauration utilisé doit faire partie d'une chaîne de points de restauration complète. Pour en savoir plus sur les chaînes de points de restauration, voir la rubrique [Points de restauration en chaîne et orphelins](#).

Vous pouvez effectuer une exportation virtuelle depuis la page Disque de secours virtuel de la console Core, ou en sélectionnant



Exportation de VM dans le menu déroulant **Restaurer** de la barre des boutons.

Lorsque vous effectuez une exportation virtuelle à partir du Core Rapid Recovery, deux choix s'offrent à vous :

- Vous pouvez effectuer une **exportation virtuelle ponctuelle**, qui représente un seul instantané créé à l'heure indiquée dans les informations du point de restauration.
- Vous pouvez créer un **disque virtuel de secours**. Avec le disque virtuel de secours, l'instantané de machine virtuelle créé à partir du point de restauration sélectionné est mis à jour en permanence par le Core, après chaque instantané planifié ou forcé sur la machine source. Cela permet de créer une ressource hautement disponible dédiée à la restauration des données. Si la machine protégée tombe en panne, vous pouvez démarrer la machine virtuelle pour la remplacer rapidement à titre temporaire. Cela vous permet de restaurer la machine protégée d'origine en subissant un temps d'arrêt modéré.

Le schéma suivant montre un déploiement type d'exportation de données vers une machine virtuelle.

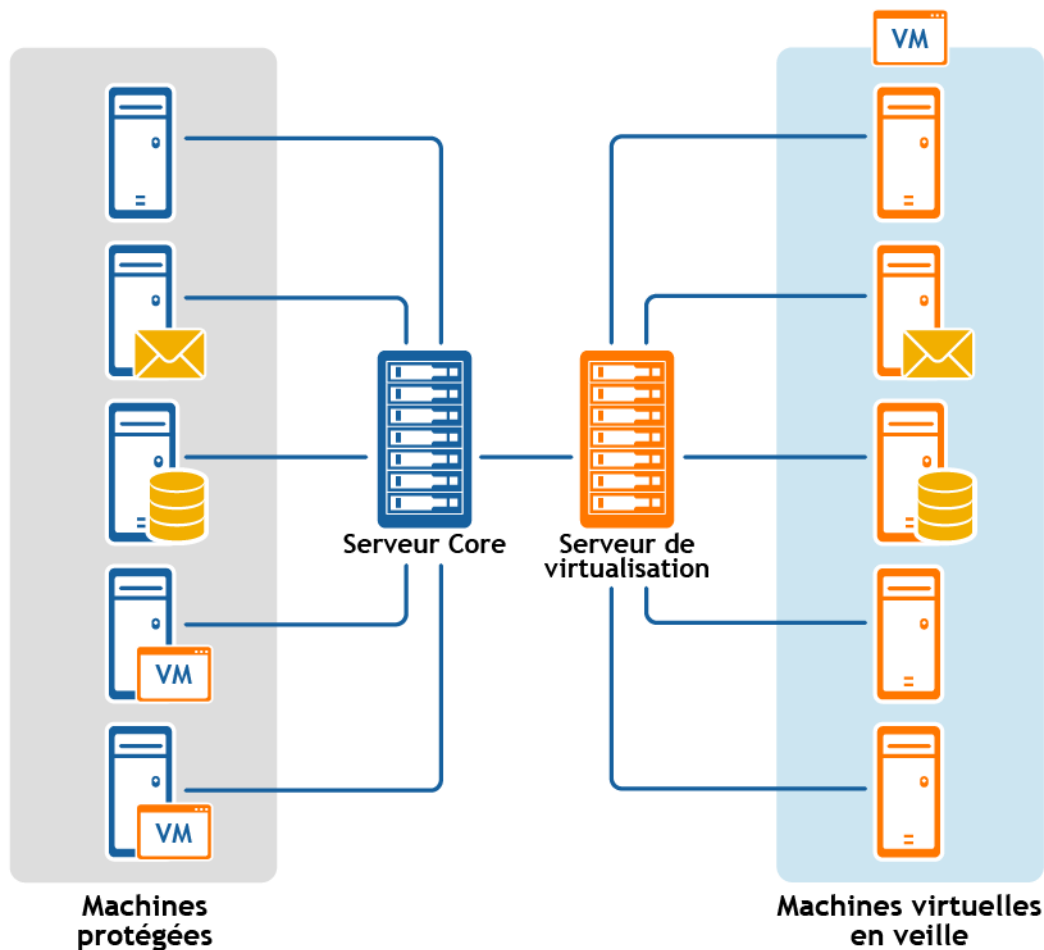


Figure 8. Déploiement sur un disque de secours virtuel

REMARQUE : dans une configuration impliquant une réplication, le Core indiqué représente le Core cible.

Lorsque vous effectuez une exportation vers une machine virtuelle, les informations suivantes sont exportées :

- Toutes les données sauvegardées d'un point de restauration
- Le système d'exploitation et les paramètres de la machine protégée d'origine

Vous pouvez effectuer une exportation virtuelle des points de restauration des machines virtuelles Windows ou Linux vers VMware, ESXi, Hyper-V et VirtualBox.

REMARQUE : pour ESXi, VMware Workstation ou Hyper-V, la version des machines virtuelles doit être une version sous licence, et non la version d'évaluation ou toute autre version gratuite.

Si vous avez paramétré la réplication entre deux Cores (source et cible), vous pouvez uniquement exporter des données depuis le Core cible une fois la réplication initiale terminée.

Exécution d'une exportation ESXi ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers ESXi.

- 1 Dans la barre des boutons de la console Core Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.

- 3 Cliquez sur **Suivant**.
- 4 Sur la page Machines, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Points de restauration, sélectionnez le point de restauration à utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page Destination de l'assistant Exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **ESX(i)**.
- 9 Entrez les paramètres d'accès à la machine, tel que décrit dans le tableau suivant, puis cliquez sur **Suivant**.

Tableau 103. Paramètres de la machine virtuelle

Options	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Entrez le port de la machine hôte. La valeur par défaut est 443.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour la connexion à la machine hôte.
Mot de passe	Saisissez le mot de passe pour la connexion à la machine hôte.

- 10 Sur la page Options de la machine virtuelle, entrez les informations, comme décrit dans le tableau suivant.

Tableau 104. Options de la machine virtuelle

Option	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Emplacement de la configuration VM	Sélectionnez un magasin de données dans la liste déroulante.
Nom de la machine virtuelle	Entrez un nom pour la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.
Provisionnement des disques	Sélectionnez le type d'allocation des disques parmi les options suivantes : - Dynamique. L'allocation dynamique crée un disque virtuel de la taille de l'espace utilisé sur les volumes d'origine, et non de la totalité de la taille du volume. Par exemple, si le volume d'origine est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 2 Go. - Statique. L'allocation statique crée un nouveau disque ou volume de la même taille que le volume d'origine à partir du serveur protégé, même si seule une partie du volume d'origine est utilisée. Par exemple, si le volume est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 1 To.
Adressage des disques	Spécifiez le type d'adressage des disques parmi les options suivantes : - Automatique - Manuel

Option	Description
	· Avec VM
Version	Sélectionnez la version d'ESXi utilisée pour créer la machine virtuelle à partir de la liste déroulante.

- 11 Cliquez sur **Suivant**.
- 12 Sur la page Volumes, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.
- 13 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'assistant et commencer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation ESXi continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle ESXi à l'aide de Rapid Recovery.

- 1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Destination** de l'Assistant d'exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **ESXi**.
- 7 Entrez les informations d'accès à la machine, tel que décrit dans le tableau suivant, puis cliquez sur **Suivant**.

Tableau 105. Identifiants ESXi

Option	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Entrez le port de la machine hôte. La valeur par défaut est 443.
Nom d'utilisateur	Entrez les données d'identification de connexion de la machine hôte.
Mot de passe	Entrez les données d'identification de connexion de la machine hôte.

- 8 Sur la page **Options de la machine virtuelle**, entrez les informations décrites dans le tableau suivant.

Tableau 106. Options de la machine virtuelle

Option	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Stockage des données	Sélectionnez un magasin de données dans la liste déroulante.

Option	Description
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.
Provisionnement des disques	Sélectionnez le type d'allocation des disques parmi les options suivantes : - Dynamique. L'allocation dynamique crée un disque virtuel de la taille de l'espace utilisé sur les volumes d'origine, et non de la totalité de la taille du volume. Par exemple, si le volume d'origine est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 2 Go. - Statique. L'allocation statique crée un nouveau disque ou volume de la même taille que le volume d'origine à partir du serveur protégé, même si seule une partie du volume d'origine est utilisée. Par exemple, si le volume est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 1 To.
Adressage des disques	Sélectionnez le type d'adressage de disques approprié (Automatique, Manuel ou avec VM).
Version	Spécifiez la version de la machine virtuelle.
Exécutez une exportation ponctuelle initiale	Exécutez l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé (facultatif).

9 Cliquez sur **Suivant**.

10 Dans la page **Volumes**, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.

11 Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

 **REMARQUE :** vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation VMware Workstation ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers VMware Workstation.

- Dans la barre de boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.
- Cliquez sur **Suivant**.
- Sur la page **Machines**, sélectionnez la machine protégée à exporter.
- Cliquez sur **Suivant**.
- Sur la page **Points de restauration**, sélectionnez le point de restauration à utiliser pour l'exportation.
- Cliquez sur **Suivant**.
- Sur la page **Destination** de l'Assistant d'exportation, dans le menu déroulant **Restaurer sur une machine virtuelle**, sélectionnez **VMware Workstation**, puis cliquez sur **Suivant**.

- 9 Sur la page Options de la machine virtuelle, entrez les paramètres d'accès à la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 107. Paramètres de la machine virtuelle

Option	Description
Emplacement de la machine VM	Spécifiez le chemin du dossier local ou du partage réseau dans lequel la machine virtuelle doit être créée. REMARQUE : si vous spécifiez un chemin de partage réseau, vous devez entrer des données d'identification de connexion valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.
Nom d'utilisateur	Saisissez les informations d'identification de connexion pour l'emplacement réseau à utiliser pour l'exportation. - Si vous spécifiez un chemin de partage réseau, vous devez entrer un nom d'utilisateur valide correspondant à un compte enregistré sur la machine cible. - Si vous entrez un chemin local, le nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les informations d'identification de connexion pour l'emplacement réseau à utiliser pour l'exportation. - Si vous spécifiez un chemin de partage réseau, vous devez saisir un mot de passe valide correspondant à un compte enregistré sur la machine cible. - Si vous entrez un chemin local, le mot de passe n'est pas nécessaire.
Nom de la VM	Entrez le nom de la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4. REMARQUE : le nom par défaut est le nom de la machine source.
Version	Spécifiez la version de VMware Workstation utilisée pour la machine virtuelle. Choisissez parmi les options suivantes : - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Taille de la RAM (Mo)	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) à attribuer à la machine virtuelle exportée. La valeur minimale est de 1.
Cores par processeur	Nombre de Cores à attribuer à chaque processeur. La valeur minimale est de 1.

- 10 Cliquez sur **Suivant**.
- 11 Sur la page Volumes, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 12 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'assistant et commencer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation dans l'onglet Disque de secours virtuel ou Événements.

Exécution d'une exportation VMware Workstation continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle VMware Workstation à l'aide de Rapid Recovery.

1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.
 - 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
 - 2 Cliquez sur **Suivant**.
 - Dans la barre d'icônes de la console Core, cliquez sur  Disque de secours virtuel.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.
- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Destination** de l'Assistant d'exportation de machine virtuelle, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **VMware Workstation**, puis cliquez sur **Suivant**.
- 7 Sur la page **Options de la machine virtuelle**, entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

Tableau 108. Paramètres de la machine virtuelle

Option	Description
Chemin cible	Spécifiez le chemin du dossier local ou du partage réseau dans lequel la machine virtuelle doit être créée. REMARQUE : Si vous spécifiez un chemin de partage réseau, vous devez entrer des données d'identification de connexion valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.
Nom d'utilisateur	Saisissez les références de connexion pour l'emplacement réseau à utiliser pour l'exportation. • Si vous spécifiez un chemin de partage réseau, vous devez entrer un nom d'utilisateur valide correspondant à un compte enregistré sur la machine cible. • Si vous entrez un chemin local, le nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les références de connexion pour l'emplacement réseau à utiliser pour l'exportation. • Si vous spécifiez un chemin de partage réseau, vous devez saisir un mot de passe valide correspondant à un compte enregistré sur la machine cible. • Si vous entrez un chemin local, le mot de passe n'est pas nécessaire.
Machine virtuelle	Entrez le nom de la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4. REMARQUE : Le nom par défaut est le nom de la machine source.
Version	Spécifiez la version de VMware Workstation utilisée pour la machine virtuelle. Choisissez parmi les options suivantes : • VMware Workstation 7.0 • VMware Workstation 8.0

Option	Description
	- VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.

- 8 Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
- 9 Cliquez sur **Suivant**.
- 10 Sur la page **Volumes**, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 11 Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

 **REMARQUE :** vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel ou Événements**.

Exécution d'une exportation Hyper-V ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers Hyper-V.

- 1 Dans la barre des boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'assistant d'exportation de machine virtuelle, sélectionnez **One-time Export** (Exportation ponctuelle).
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Machines**, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page **Destination**, dans le menu déroulant Exporter sur une machine virtuelle, sélectionnez **Hyper-V**.
- 9 Pour exporter vers une machine locale ayant le rôle Hyper-V, cliquez sur **Utiliser une machine locale**.
- 10 Pour indiquer que le serveur Hyper-V est situé sur une machine distante, cliquez sur **Hôte distant**, puis entrez les informations de l'hôte distant, comme décrit dans le tableau suivant.

Tableau 109. Informations sur l'hôte distant

Zone de texte	Description
Nom de l'hôte	Entrez l'adresse IP ou le nom d'hôte du serveur Hyper-V. Il s'agit de l'adresse IP ou du nom d'hôte du serveur Hyper-V distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire via lequel le Core communique avec la machine.
Nom d'utilisateur	Entrez le nom de l'utilisateur ayant les privilèges d'administrateur pour la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe associé au compte utilisateur possédant les privilèges d'administrateur sur la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.

11 Cliquez sur **Suivant**.

12 Sur la page **Options des machines virtuelles**, dans la zone de texte **Emplacement de la machine VM**, entrez le chemin de la machine virtuelle, par exemple, `D:\export`. Il sert à identifier l'emplacement de la machine virtuelle.

REMARQUE : Vous devez spécifier l'emplacement de la machine virtuelle pour le serveur Hyper-V local et le serveur Hyper-V distant. Le chemin doit être un chemin local valide pour le serveur Hyper-V. Les répertoires inexistantes sont créés automatiquement. N'essayez pas de les créer manuellement. L'exportation vers les dossiers partagés (par exemple, `\\data\share`) n'est pas autorisée.

13 Dans la zone de texte **Nom de la machine virtuelle**, saisissez le nom de la machine virtuelle.

Le nom que vous saisissez apparaît dans la liste des machines virtuelles de la console Hyper-V Manager.

14 Pour indiquer l'utilisation de la mémoire, cliquez sur l'une des options suivantes :

- **Utiliser la même quantité de RAM que la machine source.** Sélectionnez cette option pour indiquer que l'utilisation de RAM est identique entre la machine virtuelle et la machine source.
- **Utiliser une quantité spécifique de RAM.** Sélectionnez cette option si vous souhaitez spécifier la quantité de RAM en Mo. La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.

15 Pour spécifier le format du disque, en regard de **Format du disque**, cliquez sur l'une des options suivantes :

- VHDX
- VHD

REMARQUE : L'exportation Hyper-V prend en charge les formats de disque VHDX si la machine cible exécute Windows 8 (Windows Server 2012) ou une version ultérieure. Si VHDX n'est pas pris en charge dans votre environnement, l'option est désactivée.

Si l'exportation est effectuée vers Hyper-V de deuxième génération, seul le format de disque VHDX est pris en charge.

16 Pour définir la génération de Hyper-V à utiliser pour l'exportation, cliquez sur l'un des éléments suivants :

- Génération 1
- Génération 2

REMARQUE : Seule la génération 2 prend en charge l'option de démarrage sécurisé.

17 Définissez la carte réseau appropriée pour la VM exportée.

18 Sur la page **Volumes**, sélectionnez le ou les volumes à exporter ; par exemple, `C:\`.

REMARQUE : Si les volumes sélectionnés sont plus grands que les allocations maximales appropriées prises en charge par l'application, comme indiqué ci-dessous, ou dépassent la quantité d'espace disponible, une erreur est générée.

- Pour le format de disque VHDX, les volumes sélectionnés ne doivent pas dépasser 64 To.
- Pour le format de disque VHD, les volumes sélectionnés ne doivent pas dépasser 2 040 Go.

19 Dans la page **Volumes**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur les pages **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation Hyper-V continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle Hyper-V à l'aide de Rapid Recovery.

1 Dans la console Core Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 5 Cliquez sur **Suivant**.
- 6 Dans le menu déroulant Exporter vers une machine virtuelle de la page **Destination**, sélectionnez **Hyper-V**, puis effectuez l'une des opérations suivantes :
 - Pour exporter vers une machine locale ayant le rôle Hyper-V, cliquez sur **Utiliser une machine locale**.
 - Pour indiquer que le serveur Hyper-V se trouve sur une machine distante, cliquez sur **Hôte distant**, puis définissez les paramètres de l'hôte distant, comme indiqué dans le tableau suivant.

Tableau 110. Informations sur l'hôte distant

Zone de texte	Description
Nom de l'hôte	Entrez l'adresse IP ou le nom d'hôte du serveur Hyper-V. Il s'agit de l'adresse IP ou du nom d'hôte du serveur Hyper-V distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire via lequel le Core communique avec la machine.
Nom d'utilisateur	Entrez le nom de l'utilisateur ayant les privilèges d'administrateur pour la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe associé au compte utilisateur possédant les privilèges d'administrateur sur la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.

- 7 Cliquez sur **Suivant**.
- 8 Sur la page **Options des machines virtuelles**, dans la zone de texte **Emplacement de la machine VM**, entrez le chemin de la machine virtuelle, par exemple, **D:\export**. Il sert à identifier l'emplacement de la machine virtuelle.

REMARQUE : vous devez spécifier l'emplacement de la machine virtuelle pour le serveur Hyper-V local et le serveur Hyper-V distant. Le chemin doit être un chemin local valide pour le serveur Hyper-V. Les répertoires inexistantes sont créés automatiquement. N'essayez pas de les créer manuellement. L'exportation vers les dossiers partagés (par exemple, \\data\share) n'est pas autorisée.

- 9 Dans la zone de texte **Nom de la machine virtuelle**, saisissez le nom de la machine virtuelle.
Le nom que vous saisissez apparaît dans la liste des machines virtuelles de la console Hyper-V Manager.
- 10 Pour indiquer l'utilisation de la mémoire, cliquez sur l'une des options suivantes :

- **Utiliser la même quantité de RAM que la machine source.** Sélectionnez cette option pour indiquer que l'utilisation de RAM est identique entre la machine virtuelle et la machine source.
 - **Utiliser une quantité spécifique de RAM.** Sélectionnez cette option si vous souhaitez spécifier la quantité de RAM en Mo. La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
- 11 Pour spécifier le format du disque, en regard de Format du disque, cliquez sur l'une des options suivantes :
- VHDX
 - VHD
- REMARQUE :** l'exportation Hyper-V prend en charge les formats de disque VHDX si la machine cible exécute Windows 8 (Windows Server 2012) ou une version ultérieure. Si VHDX n'est pas pris en charge dans votre environnement, l'option est désactivée.
- Si l'exportation est effectuée vers Hyper-V de deuxième génération, seul le format de disque VHDX est pris en charge.
- 12 Pour définir la génération de Hyper-V à utiliser pour l'exportation, cliquez sur l'un des éléments suivants :
- Génération 1
 - Génération 2
- REMARQUE :** seule la génération 2 prend en charge l'option de démarrage sécurisé.
- 13 Définissez la carte réseau appropriée pour la VM exportée.
- 14 Sur la page **Volumes**, sélectionnez le ou les volumes à exporter ; par exemple, C:\.
- REMARQUE :** si les volumes sélectionnés sont plus grands que les allocations maximales appropriées prises en charge par l'application, comme indiqué ci-dessous, ou dépassent la quantité d'espace disponible, une erreur est générée.
- Pour le format de disque VHDX, les volumes sélectionnés ne doivent pas dépasser 64 To.
 - Pour le format de disque VHD, les volumes sélectionnés ne doivent pas dépasser 2 040 Go.
- 15 Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
- 16 Dans la page **Volumes**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.
- REMARQUE :** vous pouvez suivre l'état et l'avancement de l'exportation sur les pages **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation VirtualBox ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers VirtualBox.

- 1 Dans la barre de boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page Machines, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Points de restauration, sélectionnez le point de restauration à utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page Destination de l'Assistant d'exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **VirtualBox**, puis cliquez sur **Suivant**.
- 9 Sur la page Options des machines virtuelles, sélectionnez **Utiliser la machine Windows**.
- 10 Entrez les paramètres d'accès à la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 111. Paramètres de la machine virtuelle

Option	Description
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer.  REMARQUE : le nom par défaut est le nom de la machine source.
Chemin cible	Spécifiez un chemin cible local ou distant pour créer la machine virtuelle.  REMARQUE : le chemin cible ne doit pas être un répertoire racine. Si vous spécifiez un chemin de partage réseau, vous devez entrer les données d'identification de connexion (nom d'utilisateur et mot de passe) valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.

- 11 Pour spécifier un compte d'utilisateur associé à la machine virtuelle, sélectionnez **Spécifiez le compte utilisateur pour la machine virtuelle exportée**, puis entrez les informations suivantes. Ce compte fait référence à un compte d'utilisateur spécifique pour lequel la machine virtuelle va être enregistrée, dans le cas où il existe plusieurs comptes utilisateur sur la machine virtuelle. Lorsque ce compte utilisateur est connecté, seul cet utilisateur peut voir cette machine virtuelle dans le gestionnaire de VirtualBox. Si aucun compte n'est spécifié, la machine virtuelle va être enregistrée pour tous les utilisateurs existants de la machine Windows associée à VirtualBox.
 - Nom d'utilisateur : entrez le nom d'utilisateur pour lequel la machine virtuelle est enregistrée.
 - Mot de passe : entrez le mot de passe associé à ce compte utilisateur.
- 12 Cliquez sur **Suivant**.
- 13 Sur la page Volumes, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 14 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'Assistant et commencer l'exportation.

 **REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation dans l'onglet Disque de secours virtuel ou Événements.**

Exécution d'une exportation VirtualBox continue (disque de secours virtuel)

Pour effectuer cette étape, VirtualBox doit être installé sur la machine Core.

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle (VM) VirtualBox à l'aide de Rapid Recovery.

- 1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.

- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.

- Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.
- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Destination** de l'Assistant d'exportation, dans le menu déroulant **Restaurer sur une machine virtuelle**, sélectionnez **VirtualBox**.
- 7 Sur la page **Options de la machine virtuelle**, sélectionnez **Machine Linux distante**.
- 8 Entrez les informations concernant la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 112. Paramètres des machines Linux distantes

Option	Description
Nom de l'hôte VirtualBox	Entrez l'adresse IP ou le nom d'hôte du serveur VirtualBox. Il s'agit de l'adresse IP ou du nom d'hôte du serveur VirtualBox distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire duquel le core communique avec cette machine.
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer. REMARQUE : Le nom par défaut est le nom de la machine source.
Chemin cible	Spécifiez un chemin cible pour créer la machine virtuelle. REMARQUE : Il est recommandé de créer un dossier racine depuis la racine, de sorte que la machine virtuelle soit exécutée depuis la racine. Si vous n'utilisez pas la racine, vous allez devoir créer le dossier de destination manuellement sur la machine cible avant le paramétrage de l'exportation. Vous devez également attacher ou charger manuellement la machine virtuelle après l'exportation.
Nom d'utilisateur	Nom d'utilisateur du compte de la machine cible, par exemple, la racine.
Mot de passe	Mot de passe du compte utilisateur sur la machine cible.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.

- 9 Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
- 10 Cliquez sur **Suivant**.
- 11 Dans la page **Volumes**, sélectionnez les volumes de données à exporter, puis cliquez sur **Suivant**.
- 12 Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel** ou **Événements**.

Gestion des exportations

Si votre Core dispose d'une exportation virtuelle établie, les paramètres de configuration pour chaque exportation virtuelle apparaissent sur une ligne sur la page **Disque de secours virtuel**. Sur cette page, vous pouvez afficher l'état des exportations que vous avez actuellement

définies et gérer vos machines de disques de secours virtuels. Vous pouvez ajouter un disque de secours virtuel, forcer une exportation, suspendre ou reprendre un disque de secours virtuel ou supprimer la configuration d'exportation continue.

Lorsqu'une exportation ponctuelle est effectuée, la tâche est répertoriée dans la file d'attente des exportations de la page **Disque de secours virtuel**. Pendant ce temps, vous pouvez suspendre, reprendre ou annuler l'opération d'exportation.

REMARQUE : Rapid Recovery prend en charge les exportations Hyper-V vers Window 8, Window 8.1, Windows Server 2012 et 2012 R2.

L'exportation virtuelle vers une machine de disque de secours virtuel ne se produit pas si la machine virtuelle est sous tension.

Appliquez les étapes de cette procédure pour gérer vos exportations virtuelles.

- 1 Dans la barre d'icônes de la console Core, cliquez sur  Disque de secours virtuel.

La page **Disque de secours virtuel** s'affiche. Sur cette page, vous pouvez visualiser deux tableaux de paramètres d'exportation enregistrés. Ils comprennent les informations décrites dans le tableau suivant.

Tableau 113. Informations sur le disque de secours virtuel

Colonne	Description
Éléments sélectionnés	Pour chaque ligne du tableau récapitulatif, vous pouvez sélectionner la case à cocher pour réaliser des actions dans la liste des options de menu précédant le tableau.
Indicateur d'état	Les sphères colorées dans la colonne État indiquent l'état du disque de secours virtuel. Si vous passez le curseur de la souris sur le cercle de couleur, l'état exact s'affiche. • Vert. Le disque de secours virtuel est correctement configuré et activé et n'est pas suspendu. La prochaine exportation est effectuée immédiatement après la finalisation du prochain instantané. • Jaune. Le disque de secours virtuel est suspendu, mais les paramètres sont toujours définis et enregistrés dans le Core. Toutefois, après un nouveau transfert, la tâche d'exportation ne démarre pas automatiquement et aucune nouvelle exportation pour cette machine protégée n'est exécutée avant le changement d'état.
Nom de machine	Nom de la machine source.
Destination	Machine virtuelle et chemin vers lesquels les données sont exportées.
Type d'exportation	Type de plate-forme de machine virtuelle de l'exportation, tel que ESXi, VMware, Hyper-V ou VirtualBox.
Dernière exportation	Date et l'heure de la dernière exportation. Si une exportation vient d'être ajoutée et qu'elle n'est pas terminée, un message s'affiche indiquant que l'exportation n'a pas encore été effectuée. Si une exportation a échoué ou a été annulée, le message correspondant s'affiche.
Paramètres	Le menu déroulant  vous permet d'exécuter les fonctions suivantes : • Modifier. Permet de modifier les paramètres du disque de secours virtuel. • Forcer. Force une exportation virtuelle. • Suspendre. Suspend une exportation virtuelle. Disponible uniquement lorsque l'état est actif. • Reprendre. Reprend une exportation virtuelle. Disponible uniquement lorsque l'état est suspendu. • Supprimer. Supprime la configuration d'exportation continue. Ne supprimez pas la machine virtuelle exportée mise à jour récemment.

Tableau 114. Informations sur la file d'attente des exportations

Colonne	Description
Éléments sélectionnés	Pour chaque ligne du tableau récapitulatif, vous pouvez sélectionner la case à cocher pour réaliser des actions dans la liste des options de menu précédant le tableau.
Destination	Machine virtuelle et chemin vers lesquels les données sont exportées.
Type d'exportation	Type de plate-forme de machine virtuelle de l'exportation, tel que ESXi, VMware, Hyper-V ou VirtualBox.
Type de planification	Type d'exportation : ponctuelle ou continue.
État	Avancement de l'exportation, affiché en pourcentage dans une barre d'avancement.

- 2 Pour gérer les paramètres d'exportations enregistrés, sélectionnez une exportation, puis cliquez sur l'une des options suivantes :
 - **Modifier.** Ouvre l'**Assistant d'exportation de machine virtuelle** sur la page **VM Options** (Options VM). Sur cette page, vous pouvez modifier l'emplacement de la machine virtuelle exportée, modifier la version du type de machine virtuelle ou spécifier la RAM ou les processeurs pour l'exportation. Pour lancer immédiatement l'exportation de VM, sélectionnez **Effectuer l'exportation ponctuelle initiale**.
 - **Forcer.** Force une nouvelle exportation. Cette option peut s'avérer utile lorsque le disque de secours virtuel est suspendu et relancé, ce qui implique que la tâche d'exportation redémarrera uniquement après un nouveau transfert. Si vous ne souhaitez pas attendre le nouveau transfert, vous avez la possibilité de forcer une exportation.
 - **Suspendre.** Suspend une exportation active.
 - **Reprendre.** Reprend la configuration d'exportation continue au prochain instantané planifié ou forcé.
- 3 Pour supprimer une exportation du système, sélectionnez l'exportation, puis cliquez sur **Supprimer**.
La configuration de l'exportation est définitivement supprimée du système. La suppression de la configuration du disque de secours virtuel n'entraîne pas la suppression des machines virtuelles exportées suite à la configuration.
- 4 Pour gérer le nombre d'exportations qui s'exécutent en même temps, procédez comme suit :
 - Sous File d'attente des exportations, cliquez sur **Paramètres**.
 - Dans la boîte de dialogue **Nombre maximal d'exportations simultanées**, entrez le nombre d'exportations que vous souhaitez exécuter simultanément. Le nombre par défaut est 5.
 - Cliquez sur **Enregistrer**.
- 5 Pour annuler une exportation ponctuelle ou continue actuellement répertoriée dans la file d'attente des exportations, sélectionnez l'exportation, puis cliquez sur **Annuler**.
- 6 Pour ajouter une nouvelle exportation de disque de secours virtuel, vous pouvez cliquer sur **Ajouter** pour lancer l'assistant d'exportation. Pour plus d'informations sur la configuration d'un disque de secours virtuel pour une machine virtuelle, voir l'une des rubriques suivantes :
 - [Exportation de données vers une machine virtuelle ESXi](#)
 - [Exportation de données vers une machine virtuelle VMWare Workstation](#)
 - [Exportation de données vers une machine virtuelle Hyper-V](#)
 - [Exportation de données vers une machine virtuelle VirtualBox](#)

Exportation de données vers une machine virtuelle ESXi

Dans Rapid Recovery, vous pouvez exporter des données vers ESXi en effectuant une exportation ponctuelle ou en établissant une exportation continue (pour disque de secours virtuel). Suivez les procédures ci-dessous selon le type d'exportation à effectuer.

Exécution d'une exportation ESXi ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers ESXi.

- 1 Dans la barre des boutons de la console Core Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page Machines, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Points de restauration, sélectionnez le point de restauration à utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page Destination de l'assistant Exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **ESX(i)**.
- 9 Entrez les paramètres d'accès à la machine, tel que décrit dans le tableau suivant, puis cliquez sur **Suivant**.

Tableau 115. Paramètres de la machine virtuelle

Options	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Entrez le port de la machine hôte. La valeur par défaut est 443.
Nom d'utilisateur	Saisissez le nom d'utilisateur pour la connexion à la machine hôte.
Mot de passe	Saisissez le mot de passe pour la connexion à la machine hôte.

- 10 Sur la page Options de la machine virtuelle, entrez les informations, comme décrit dans le tableau suivant.

Tableau 116. Options de la machine virtuelle

Option	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Emplacement de la configuration VM	Sélectionnez un magasin de données dans la liste déroulante.
Nom de la machine virtuelle	Entrez un nom pour la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Utiliser la même quantité de mémoire vive que la machine source • Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.
Provisionnement des disques	Sélectionnez le type d'allocation des disques parmi les options suivantes : • Dynamique. L'allocation dynamique crée un disque virtuel de la taille de l'espace utilisé sur les volumes d'origine, et non de la totalité de la taille du volume. Par exemple, si le volume d'origine est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 2 Go. • Statique. L'allocation statique crée un nouveau disque ou volume de la même taille que le volume d'origine à partir du serveur protégé, même si seule une partie du volume d'origine est utilisée. Par exemple, si le

Option	Description
	volume est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 1 To.
Adressage des disques	Spécifiez le type d'adressage des disques parmi les options suivantes : • Automatique • Manuel • Avec VM
Version	Sélectionnez la version d'ESXi utilisée pour créer la machine virtuelle à partir de la liste déroulante.

- 11 Cliquez sur **Suivant**.
- 12 Sur la page Volumes, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.
- 13 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'assistant et commencer l'exportation.

 **REMARQUE :** vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation ESXi continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle ESXi à l'aide de Rapid Recovery.

- 1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Destination** de l'Assistant d'exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **ESXi**.
- 7 Entrez les informations d'accès à la machine, tel que décrit dans le tableau suivant, puis cliquez sur **Suivant**.

Tableau 117. Identifiants ESXi

Option	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Entrez le port de la machine hôte. La valeur par défaut est 443.
Nom d'utilisateur	Entrez les données d'identification de connexion de la machine hôte.
Mot de passe	Entrez les données d'identification de connexion de la machine hôte.

- 8 Sur la page **Options de la machine virtuelle**, entrez les informations décrites dans le tableau suivant.

Tableau 118. Options de la machine virtuelle

Option	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Stockage des données	Sélectionnez un magasin de données dans la liste déroulante.
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.
Provisionnement des disques	Sélectionnez le type d'allocation des disques parmi les options suivantes : - Dynamique. L'allocation dynamique crée un disque virtuel de la taille de l'espace utilisé sur les volumes d'origine, et non de la totalité de la taille du volume. Par exemple, si le volume d'origine est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 2 Go. - Statique. L'allocation statique crée un nouveau disque ou volume de la même taille que le volume d'origine à partir du serveur protégé, même si seule une partie du volume d'origine est utilisée. Par exemple, si le volume est de 1 To, mais qu'il ne contient que 2 Go d'espace utilisé, Rapid Recovery crée un disque virtuel de 1 To.
Adressage des disques	Sélectionnez le type d'adressage de disques approprié (Automatique, Manuel ou avec VM).
Version	Spécifiez la version de la machine virtuelle.
Exécutez une exportation ponctuelle initiale	Exécutez l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé (facultatif).

9 Cliquez sur **Suivant**.

10 Dans la page **Volumes**, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.

11 Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel ou Événements**.

Exportation de données vers une machine virtuelle VirtualBox

Dans Rapid Recovery, vous pouvez exporter des données à l'aide de l'exportation VirtualBox, en effectuant une exportation ponctuelle ou en établissant une exportation continue (pour disque de secours virtuel).

REMARQUE : l'exportation VirtualBox d'une machine protégée Windows 10 n'est actuellement pas prise en charge.

Suivez les procédures ci-dessous selon le type d'exportation à effectuer.

REMARQUE : pour effectuer ce type d'exportation, VirtualBox doit être installé sur la machine Core. Les versions de Virtual Box 4.2.18 ou ultérieures sont prises en charge par les hôtes Windows.

Exécution d'une exportation VirtualBox ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers VirtualBox.

- 1 Dans la barre de boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page Machines, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Points de restauration, sélectionnez le point de restauration à utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page Destination de l'Assistant d'exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **VirtualBox**, puis cliquez sur **Suivant**.
- 9 Sur la page Options des machines virtuelles, sélectionnez **Utiliser la machine Windows**.
- 10 Entrez les paramètres d'accès à la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 119. Paramètres de la machine virtuelle

Option	Description
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer. REMARQUE : le nom par défaut est le nom de la machine source.
Chemin cible	Spécifiez un chemin cible local ou distant pour créer la machine virtuelle. REMARQUE : le chemin cible ne doit pas être un répertoire racine. Si vous spécifiez un chemin de partage réseau, vous devez entrer les données d'identification de connexion (nom d'utilisateur et mot de passe) valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Utiliser la même quantité de mémoire vive que la machine source • Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.

- 11 Pour spécifier un compte d'utilisateur associé à la machine virtuelle, sélectionnez **Spécifiez le compte utilisateur pour la machine virtuelle exportée**, puis entrez les informations suivantes. Ce compte fait référence à un compte d'utilisateur spécifique pour lequel la machine virtuelle va être enregistrée, dans le cas où il existe plusieurs comptes utilisateur sur la machine virtuelle. Lorsque ce compte utilisateur est connecté, seul cet utilisateur peut voir cette machine virtuelle dans le gestionnaire de VirtualBox. Si aucun compte n'est spécifié, la machine virtuelle va être enregistrée pour tous les utilisateurs existants de la machine Windows associée à VirtualBox.
 - Nom d'utilisateur : entrez le nom d'utilisateur pour lequel la machine virtuelle est enregistrée.
 - Mot de passe : entrez le mot de passe associé à ce compte utilisateur.
- 12 Cliquez sur **Suivant**.
- 13 Sur la page Volumes, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 14 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'Assistant et commencer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation dans l'onglet Disque de secours virtuel ou Événements.

Exécution d'une exportation VirtualBox continue (disque de secours virtuel)

Pour effectuer cette étape, VirtualBox doit être installé sur la machine Core.

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle (VM) VirtualBox à l'aide de Rapid Recovery.

1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.

2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.

3 Cliquez sur **Suivant**.

4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.

5 Cliquez sur **Suivant**.

6 Sur la page **Destination** de l'Assistant d'exportation, dans le menu déroulant **Restaurer sur une machine virtuelle**, sélectionnez **VirtualBox**.

7 Sur la page **Options de la machine virtuelle**, sélectionnez **Machine Linux distante**.

8 Entrez les informations concernant la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 120. Paramètres des machines Linux distantes

Option	Description
Nom de l'hôte VirtualBox	Entrez l'adresse IP ou le nom d'hôte du serveur VirtualBox. Il s'agit de l'adresse IP ou du nom d'hôte du serveur VirtualBox distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire duquel le core communique avec cette machine.
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer.  REMARQUE : Le nom par défaut est le nom de la machine source.
Chemin cible	Spécifiez un chemin cible pour créer la machine virtuelle.  REMARQUE : Il est recommandé de créer un dossier racine depuis la racine, de sorte que la machine virtuelle soit exécutée depuis la racine. Si vous n'utilisez pas la racine, vous allez devoir créer le dossier de destination manuellement sur la machine cible avant le paramétrage de l'exportation. Vous devez également attacher ou charger manuellement la machine virtuelle après l'exportation.
Nom d'utilisateur	Nom d'utilisateur du compte de la machine cible, par exemple, la racine.
Mot de passe	Mot de passe du compte utilisateur sur la machine cible.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Utiliser la même quantité de mémoire vive que la machine source • Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo

Option	Description
	La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
9	Sélectionnez Effectuer une exportation ponctuelle initiale pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
10	Cliquez sur Suivant .
11	Dans la page Volumes , sélectionnez les volumes de données à exporter, puis cliquez sur Suivant .
12	Sur la page Récapitulatif , cliquez sur Terminer pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel ou Événements**.

Exportation de données vers une machine virtuelle VMWare Workstation

Dans Rapid Recovery, vous pouvez exporter des données vers VMware Workstation en effectuant une exportation ponctuelle ou en établissant une exportation continue (pour disque de secours virtuel). Suivez les procédures ci-dessous selon le type d'exportation à effectuer.

Exécution d'une exportation VMware Workstation ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers VMware Workstation.

- 1 Dans la barre de boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **Exportation ponctuelle**.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page Machines, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page Points de restauration, sélectionnez le point de restauration à utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page Destination de l'Assistant d'exportation, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **VMware Workstation**, puis cliquez sur **Suivant**.
- 9 Sur la page Options de la machine virtuelle, entrez les paramètres d'accès à la machine virtuelle, tel que décrit dans le tableau suivant.

Tableau 121. Paramètres de la machine virtuelle

Option	Description
Emplacement de la machine VM	Spécifiez le chemin du dossier local ou du partage réseau dans lequel la machine virtuelle doit être créée. REMARQUE : si vous spécifiez un chemin de partage réseau, vous devez entrer des données d'identification de connexion valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.
Nom d'utilisateur	Saisissez les informations d'identification de connexion pour l'emplacement réseau à utiliser pour l'exportation. • Si vous spécifiez un chemin de partage réseau, vous devez entrer un nom d'utilisateur valide correspondant à un compte enregistré sur la machine cible. • Si vous entrez un chemin local, le nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les informations d'identification de connexion pour l'emplacement réseau à utiliser pour l'exportation. • Si vous spécifiez un chemin de partage réseau, vous devez saisir un mot de passe valide correspondant à un compte enregistré sur la machine cible.

Option	Description
	Si vous entrez un chemin local, le mot de passe n'est pas nécessaire.
Nom de la VM	Entrez le nom de la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4.
	REMARQUE : le nom par défaut est le nom de la machine source.
Version	Spécifiez la version de VMware Workstation utilisée pour la machine virtuelle. Choisissez parmi les options suivantes : - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Taille de la RAM (Mo)	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) à attribuer à la machine virtuelle exportée. La valeur minimale est de 1.
Cores par processeur	Nombre de Cores à attribuer à chaque processeur. La valeur minimale est de 1.

- 10 Cliquez sur **Suivant**.
- 11 Sur la page Volumes, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 12 Sur la page Synthèse, cliquez sur **Terminer** pour fermer l'assistant et commencer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation dans l'onglet Disque de secours virtuel ou Événements.

Exécution d'une exportation VMware Workstation continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle VMware Workstation à l'aide de Rapid Recovery.

- 1 Dans la console Core de Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

- 2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.

- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Destination** de l'Assistant d'exportation de machine virtuelle, dans le menu déroulant Restaurer sur une machine virtuelle, sélectionnez **VMware Workstation**, puis cliquez sur **Suivant**.
- 7 Sur la page **Options de la machine virtuelle**, entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

Tableau 122. Paramètres de la machine virtuelle

Option	Description
Chemin cible	Spécifiez le chemin du dossier local ou du partage réseau dans lequel la machine virtuelle doit être créée.
REMARQUE : Si vous spécifiez un chemin de partage réseau, vous devez entrer des données d'identification de connexion valides correspondant à un compte enregistré sur la machine cible. Ce compte doit avoir des autorisations de lecture et d'écriture dans le partage réseau.	
Nom d'utilisateur	Saisissez les références de connexion pour l'emplacement réseau à utiliser pour l'exportation. - Si vous spécifiez un chemin de partage réseau, vous devez entrer un nom d'utilisateur valide correspondant à un compte enregistré sur la machine cible. - Si vous entrez un chemin local, le nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les références de connexion pour l'emplacement réseau à utiliser pour l'exportation. - Si vous spécifiez un chemin de partage réseau, vous devez saisir un mot de passe valide correspondant à un compte enregistré sur la machine cible. - Si vous entrez un chemin local, le mot de passe n'est pas nécessaire.
Machine virtuelle	Entrez le nom de la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4. REMARQUE : Le nom par défaut est le nom de la machine source.
Version	Spécifiez la version de VMware Workstation utilisée pour la machine virtuelle. Choisissez parmi les options suivantes : - VMware Workstation 7.0 - VMware Workstation 8.0 - VMware Workstation 9.0 - VMware Workstation 10.0 - VMware Workstation 11.0 - VMware Workstation 12.0
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : - Utiliser la même quantité de mémoire vive que la machine source - Utiliser une quantité particulière de RAM, puis spécifier le montant en Mo La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
Nombre de processeurs	Nombre de processeurs (UC) souhaité pour la machine virtuelle exportée. La valeur minimale est 1.
Cores par processeur	Nombre de Cores souhaité pour chaque processeur. La valeur minimale est 1.

- 8 Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
- 9 Cliquez sur **Suivant**.
- 10 Sur la page **Volumes**, sélectionnez les volumes à exporter, par exemple C:\ et D:\, puis cliquez sur **Suivant**.
- 11 Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur la page **Disque de secours virtuel ou Événements**.

Exportation de données vers une machine virtuelle Hyper-V

Dans Rapid Recovery, vous pouvez exporter des données à l'aide de l'exportation Hyper-V, en effectuant une exportation ponctuelle ou en établissant une exportation continue (pour disque de secours virtuel).

Rapid Recovery prend en charge l'exportation Hyper-V de première génération vers les hôtes suivants :

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Rapid Recovery prend en charge l'exportation Hyper-V de deuxième génération vers les hôtes suivants :

- Windows 8.1
- Windows Server 2012 R2

REMARQUE : les machines protégées ne peuvent pas être toutes exportées vers des hôtes de deuxième génération Hyper V.

Seules les machines protégées avec les systèmes d'exploitation UEFI (Unified Extensible Firmware Interface) prennent en charge l'exportation virtuelle vers les hôtes de deuxième génération Hyper V :

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012 R2 (UEFI)

REMARQUE : l'exportation Hyper-V vers une machine virtuelle de deuxième génération peut échouer si l'hôte Hyper-V ne dispose pas d'une mémoire vive allouée suffisante pour exécuter l'exportation.

Suivez les procédures ci-dessous selon le type d'exportation à effectuer.

Exécution d'une exportation Hyper-V ponctuelle

Suivez cette procédure pour effectuer une exportation ponctuelle vers Hyper-V.

- 1 Dans la barre des boutons de la console Core de Rapid Recovery, cliquez sur le menu déroulant **Restaurer**, puis sur **Exportation de VM**.
- 2 Dans l'assistant d'exportation de machine virtuelle, sélectionnez **One-time Export** (Exportation ponctuelle).
- 3 Cliquez sur **Suivant**.
- 4 Sur la page **Machines**, sélectionnez la machine protégée à exporter.
- 5 Cliquez sur **Suivant**.
- 6 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page **Destination**, dans le menu déroulant Exporter sur une machine virtuelle, sélectionnez **Hyper-V**.
- 9 Pour exporter vers une machine locale ayant le rôle Hyper-V, cliquez sur **Utiliser une machine locale**.
- 10 Pour indiquer que le serveur Hyper-V est situé sur une machine distante, cliquez sur **Hôte distant**, puis entrez les informations de l'hôte distant, comme décrit dans le tableau suivant.

Tableau 123. Informations sur l'hôte distant

Zone de texte	Description
Nom de l'hôte	Entrez l'adresse IP ou le nom d'hôte du serveur Hyper-V. Il s'agit de l'adresse IP ou du nom d'hôte du serveur Hyper-V distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire via lequel le Core communique avec la machine.
Nom d'utilisateur	Entrez le nom de l'utilisateur ayant les privilèges d'administrateur pour la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe associé au compte utilisateur possédant les privilèges d'administrateur sur la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.

11 Cliquez sur **Suivant**.

12 Sur la page **Options des machines virtuelles**, dans la zone de texte **Emplacement de la machine VM**, entrez le chemin de la machine virtuelle, par exemple, `D:\export`. Il sert à identifier l'emplacement de la machine virtuelle.

REMARQUE : Vous devez spécifier l'emplacement de la machine virtuelle pour le serveur Hyper-V local et le serveur Hyper-V distant. Le chemin doit être un chemin local valide pour le serveur Hyper-V. Les répertoires inexistantes sont créés automatiquement. N'essayez pas de les créer manuellement. L'exportation vers les dossiers partagés (par exemple, `\\data\share`) n'est pas autorisée.

13 Dans la zone de texte **Nom de la machine virtuelle**, saisissez le nom de la machine virtuelle.

Le nom que vous saisissez apparaît dans la liste des machines virtuelles de la console Hyper-V Manager.

14 Pour indiquer l'utilisation de la mémoire, cliquez sur l'une des options suivantes :

- **Utiliser la même quantité de RAM que la machine source.** Sélectionnez cette option pour indiquer que l'utilisation de RAM est identique entre la machine virtuelle et la machine source.
- **Utiliser une quantité spécifique de RAM.** Sélectionnez cette option si vous souhaitez spécifier la quantité de RAM en Mo. La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.

15 Pour spécifier le format du disque, en regard de **Format du disque**, cliquez sur l'une des options suivantes :

- VHDX
- VHD

REMARQUE : L'exportation Hyper-V prend en charge les formats de disque VHDX si la machine cible exécute Windows 8 (Windows Server 2012) ou une version ultérieure. Si VHDX n'est pas pris en charge dans votre environnement, l'option est désactivée.

Si l'exportation est effectuée vers Hyper-V de deuxième génération, seul le format de disque VHDX est pris en charge.

16 Pour définir la génération de Hyper-V à utiliser pour l'exportation, cliquez sur l'un des éléments suivants :

- Génération 1
- Génération 2

REMARQUE : Seule la génération 2 prend en charge l'option de démarrage sécurisé.

17 Définissez la carte réseau appropriée pour la VM exportée.

18 Sur la page **Volumes**, sélectionnez le ou les volumes à exporter ; par exemple, `C:\`.

REMARQUE : Si les volumes sélectionnés sont plus grands que les allocations maximales appropriées prises en charge par l'application, comme indiqué ci-dessous, ou dépassent la quantité d'espace disponible, une erreur est générée.

- Pour le format de disque VHDX, les volumes sélectionnés ne doivent pas dépasser 64 To.
- Pour le format de disque VHD, les volumes sélectionnés ne doivent pas dépasser 2 040 Go.

19 Dans la page **Volumes**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : vous pouvez suivre l'état et l'avancement de l'exportation sur les pages **Disque de secours virtuel** ou **Événements**.

Exécution d'une exportation Hyper-V continue (disque de secours virtuel)

Suivez les étapes de cette procédure pour effectuer une exportation continue vers une machine virtuelle Hyper-V à l'aide de Rapid Recovery.

1 Dans la console Core Rapid Recovery, effectuez l'une des opérations suivantes :

- Dans la barre des boutons de la console Core, cliquez sur le menu déroulant  **Restaurer**, puis sélectionnez **Exportation de VM**.

- 1 Dans l'Assistant d'exportation de machine virtuelle, sélectionnez **En continu (Disque de secours virtuel)**.
- 2 Cliquez sur **Suivant**.

- Dans la barre d'icônes de la console Core, cliquez sur  **Disque de secours virtuel**.
 - Sur la page **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant d'exportation de machine virtuelle.

2 Sur la page **Machines** de l'Assistant d'exportation de machine virtuelle, sélectionnez la machine protégée que vous souhaitez exporter.

3 Cliquez sur **Suivant**.

4 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour l'exportation.

5 Cliquez sur **Suivant**.

6 Dans le menu déroulant **Exporter vers une machine virtuelle** de la page **Destination**, sélectionnez **Hyper-V**, puis effectuez l'une des opérations suivantes :

- Pour exporter vers une machine locale ayant le rôle Hyper-V, cliquez sur **Utiliser une machine locale**.
- Pour indiquer que le serveur Hyper-V se trouve sur une machine distante, cliquez sur **Hôte distant**, puis définissez les paramètres de l'hôte distant, comme indiqué dans le tableau suivant.

Tableau 124. Informations sur l'hôte distant

Zone de texte	Description
Nom de l'hôte	Entrez l'adresse IP ou le nom d'hôte du serveur Hyper-V. Il s'agit de l'adresse IP ou du nom d'hôte du serveur Hyper-V distant.
Port	Entrez le numéro de port de la machine. Il s'agit du port par l'intermédiaire via lequel le Core communique avec la machine.
Nom d'utilisateur	Entrez le nom de l'utilisateur ayant les privilèges d'administrateur pour la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe associé au compte utilisateur possédant les privilèges d'administrateur sur la station de travail avec serveur Hyper-V. Il sert à spécifier les données d'identification de connexion de la machine virtuelle.

7 Cliquez sur **Suivant**.

8 Sur la page **Options des machines virtuelles**, dans la zone de texte **Emplacement de la machine VM**, entrez le chemin de la machine virtuelle, par exemple, **D:\export**. Il sert à identifier l'emplacement de la machine virtuelle.

REMARQUE : vous devez spécifier l'emplacement de la machine virtuelle pour le serveur Hyper-V local et le serveur Hyper-V distant. Le chemin doit être un chemin local valide pour le serveur Hyper-V. Les répertoires inexistantes sont créés automatiquement. N'essayez pas de les créer manuellement. L'exportation vers les dossiers partagés (par exemple, \\data\share) n'est pas autorisée.

9 Dans la zone de texte **Nom de la machine virtuelle**, saisissez le nom de la machine virtuelle.

Le nom que vous saisissez apparaît dans la liste des machines virtuelles de la console Hyper-V Manager.

10 Pour indiquer l'utilisation de la mémoire, cliquez sur l'une des options suivantes :

- Utiliser la même quantité de RAM que la machine source.** Sélectionnez cette option pour indiquer que l'utilisation de RAM est identique entre la machine virtuelle et la machine source.

- **Utiliser une quantité spécifique de RAM.** Sélectionnez cette option si vous souhaitez spécifier la quantité de RAM en Mo. La quantité minimum est de 1 024 Mo et la quantité maximum autorisée par l'application est de 65 536 Mo. La quantité d'utilisation maximum de mémoire est limitée par la quantité de mémoire vive disponible pour la machine hôte.
- 11 Pour spécifier le format du disque, en regard de Format du disque, cliquez sur l'une des options suivantes :
- VHDX
 - VHD
- REMARQUE :** l'exportation Hyper-V prend en charge les formats de disque VHDX si la machine cible exécute Windows 8 (Windows Server 2012) ou une version ultérieure. Si VHDX n'est pas pris en charge dans votre environnement, l'option est désactivée.
- Si l'exportation est effectuée vers Hyper-V de deuxième génération, seul le format de disque VHDX est pris en charge.
- 12 Pour définir la génération de Hyper-V à utiliser pour l'exportation, cliquez sur l'un des éléments suivants :
- Génération 1
 - Génération 2
- REMARQUE :** seule la génération 2 prend en charge l'option de démarrage sécurisé.
- 13 Définissez la carte réseau appropriée pour la VM exportée.
- 14 Sur la page **Volumes**, sélectionnez le ou les volumes à exporter ; par exemple, C:\.
- REMARQUE :** si les volumes sélectionnés sont plus grands que les allocations maximales appropriées prises en charge par l'application, comme indiqué ci-dessous, ou dépassent la quantité d'espace disponible, une erreur est générée.
- Pour le format de disque VHDX, les volumes sélectionnés ne doivent pas dépasser 64 To.
 - Pour le format de disque VHD, les volumes sélectionnés ne doivent pas dépasser 2 040 Go.
- 15 Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation virtuelle immédiatement et non pas après le prochain instantané programmé.
- 16 Dans la page **Volumes**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.
- REMARQUE :** vous pouvez suivre l'état et l'avancement de l'exportation sur les pages **Disque de secours virtuel** ou **Événements**.

Gestion des données vieillissantes

Cette section explique comment gérer les données d'instantané vieillissantes qui sont enregistrées sur votre logithèque. Elle fournit des informations sur la conservation des points de restauration dans votre logithèque, les stratégies de rétention et le processus résultant de la consolidation des points de restauration pour économiser de l'espace. Elle décrit également la nouvelle capacité permettant de déplacer les points de restauration de votre logithèque vers une appliance Dell DR de sauvegarde et déduplication.

En outre, cette section indique comment archiver des données pour un stockage longue durée sans qu'elles ne soient consolidées et comment accéder aux points de restauration archivés.

À propos de la conservation et de l'archivage des données de Rapid Recovery

Chaque fois que le Core capture un instantané, les données sont enregistrées sous forme de point de restauration dans votre logithèque. Les points de restauration s'accumulent naturellement au fil du temps. Pour y remédier, le Core utilise une stratégie de rétention afin de déterminer la durée de conservation des données d'instantané dans la logithèque. Lors de la consolidation nocturne, le Core applique cette stratégie de rétention afin de réduire l'espace de stockage occupé. Pendant cette étape, le système compare la date de chaque point de restauration à celle du point de restauration le plus récent. Le Core combine (ou « consolide ») ensuite les points de restauration les plus anciens. Au fil du temps, les anciens points de restauration sont progressivement remplacés par les plus récents, une fois leur période de rétention dépassée.

Pour conserver les points de restauration avant qu'ils ne soient combinés, puis supprimés, vous pouvez créer une archive de la console Core. Une archive est un fichier contenant l'intégralité des points de récupération des machines protégées sur votre Core au moment de sa création.

Vous pouvez stocker une archive dans un système de fichiers, ou sur un compte de stockage dans le Cloud.

Si vous avez besoin d'accéder aux données d'un point de restauration, vous pouvez ensuite joindre (Rapid Recovery 6.x et versions ultérieures) ou importer l'archive afin de restaurer ce point de restauration dans votre logithèque. Vous pouvez ensuite utiliser ces données comme s'il s'agissait d'un point de restauration enregistré sur votre Core.

REMARQUE : comme le Core reconnaît les dates de création des points de restauration d'une archive, vous pourrez consolider ou supprimer à nouveau les points importés lors de la prochaine tâche nocturne. Pour conserver vos anciens points de récupération, désactivez la consolidation sur les machines concernées ou prolongez la période de rétention.

Gestion des stratégies de conservation

Une stratégie de conservation est un ensemble de règles qui définit la durée pendant laquelle le Noyau conservera des points de récupération avant de les cumuler. Les stratégies de conservation peuvent être paramétrées pour démarrer le processus de cumul par heure, par jour, par semaine, par mois ou par an. Vous pouvez définir six règles au maximum (la stratégie par défaut en définit cinq).

Étant donné que vous pouvez sauvegarder fréquemment, toutes les 5 minutes si vous le désirez, la première règle d'une stratégie de récupération permet généralement de définir la durée de conservation de l'ensemble des points de récupération. Par exemple, si vous sauvegardez les fichiers d'une machine toutes les 15 minutes, 96 points de récupération seront créés dans la logithèque chaque jour, pour cette machine seulement, jusqu'au démarrage du cumul. Si vous ne gérez pas cette stratégie de conservation, la quantité de données sauvegardées peut rapidement saturer une logithèque.

REMARQUE : les administrateurs doivent savoir que des sauvegardes fréquentes ont un impact sur le trafic réseau. D'autres facteurs l'affectent également, dont les autres types de transferts (comme une réplication), le taux de modification des données, ainsi que les câbles, commutateurs et matériel réseau.

Le Noyau est préconfiguré avec une stratégie de conservation par défaut. Celle-ci conserve :

- Tous les points de récupération pendant trois jours
- Un point de récupération par heure pendant deux jours
- Un point de récupération par jour pendant quatre jours
- Un point de récupération par semaine pendant trois semaines
- Un point de récupération par mois pendant deux mois
- Un point de récupération par an pendant X années (désactivé dans la stratégie par défaut)

Selon cette stratégie par défaut, le point de récupération le plus ancien est généralement de 92 jours. Les données plus anciennes sont supprimées.

Définir la stratégie de conservation au niveau du Noyau l'applique automatiquement à toutes les machines protégées par ce Noyau. Vous pouvez modifier la stratégie par défaut en fonction de vos besoins.

Vous pouvez également créer une stratégie de conservation personnalisée pour n'importe quelle machine. Définir une stratégie au niveau de la machine vous permet de paramétrer une stratégie de conservation différente de celle du Noyau. Pour plus d'informations sur la configuration de stratégies de conservation, veuillez consulter [Configuration des paramètres de la stratégie de conservation par défaut du Noyau](#) et [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).

Configuration des paramètres de la stratégie de conservation par défaut du Noyau

La stratégie de conservation du Noyau détermine la période pendant laquelle les points de récupération d'une machine protégée sont conservés dans la logithèque.

La stratégie de conservation du Noyau est mise en œuvre par un processus de cumul faisant partie des tâches nocturnes en cours d'exécution. Puis, les points de récupération ayant dépassé l'âge spécifié dans la stratégie de conservation sont « cumulés » (combinés) en un nombre de points de récupération plus faible afin de couvrir une période de temps moins granulaire. Le fait d'appliquer la stratégie de conservation toutes les nuits permet de cumuler continuellement les sauvegardes moins récentes. Ainsi, les points de récupération les plus anciens sont supprimés, en fonction des spécifications de la stratégie de conservation.

Différents paramètres de conservation peuvent être configurés pour les Noyaux source et cible.

REMARQUE : cette section est destinée à personnaliser les paramètres de la stratégie de conservation du Noyau de la Rapid Recovery. Lorsque vous enregistrez les paramètres personnalisés de la stratégie de conservation du Noyau, vous établissez les paramètres de la stratégie de conservation par défaut qui peuvent être appliqués à toutes les machines protégées présentes sur ce Noyau. Pour plus d'informations sur la personnalisation des paramètres de la stratégie de conservation pour des machines protégées individuelles, veuillez consulter [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).

- 1 Accédez à la console du Noyau de la Rapid Recovery.
- 2 Sur la barre des icônes, cliquez sur  (Paramètres), puis effectuez l'une des actions suivantes :
 - Depuis la liste des paramètres du Noyau sur le côté gauche de la page Paramètres, cliquez sur **Tâches nocturnes**.
 - Faites défiler vers le bas le côté droit de la page Paramètres jusqu'à ce que vous aperceviez le titre **Tâches nocturnes**.Les paramètres du noyau des Tâches nocturnes apparaissent.
- 3 Dans **Tâches nocturnes**, cliquez sur  **Modification**.
La boîte de dialogue **Tâches nocturnes** s'affiche.
- 4 Pour spécifier les périodes pendant lesquelles conserver les données sauvegardées, au sein du volet Tâches nocturnes, sélectionnez **Cumul**, puis cliquez sur **Paramètres**.
La boîte de dialogue **Configuration** pour la stratégie de conservation par défaut du Noyau s'affiche.
- 5 Pour réinitialiser les paramètres de la stratégie de conservation du Noyau à leur valeur par défaut à n'importe quel moment, au bas de la boîte de dialogue intitulée Configuration, cliquez sur **Réinitialiser les paramètres à leur valeur par défaut**, puis cliquez sur **Oui** pour confirmer.
Tous les paramètres sont réinitialisés aux valeurs par défaut décrites dans le tableau de l'étape 6.
- 6 Pour configurer une stratégie de conservation, veuillez d'abord spécifier le paramètre principal qui détermine la durée de conservation des instantanés de sauvegarde originels. Puis, précisez un ensemble en cascade de spécifications de cumul qui déterminera les intervalles entre lesquels les points de récupération devront être cumulés.
Les options de la stratégie de conservation sont décrites dans le tableau suivant.

Tableau 125. Options de planification de la stratégie de conservation par défaut

Zone de texte	Description
Conserver tous les points de récupération pendant n [période de conservation]	Indique la période de conservation des points de récupération. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 3 jours.

Zone de texte	Description
	Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par heure pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation sur laquelle se base le paramètre principal pour déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 2 jours. Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par jour pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 4 jours. Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par semaine pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 3 semaines. Vous pouvez sélectionner une de ces options : semaines, mois ou années
... Puis conserver un point de récupération par mois pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 2 mois. Vous pouvez sélectionner une de ces options : mois ou années
... Puis conserver un point de récupération par an pendant n [période de conservation]	Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. Vous pouvez sélectionner : années

Le point de récupération le plus ancien est déterminé par les paramètres de la stratégie de conservation.

L'exemple suivant montre comment la période de conservation est calculée.

Conserver tous les points de récupération pendant trois jours.

... Puis conserver un point de récupération par heure pendant 3 jours

... Puis conserver un point de récupération par jour pendant 4 jours

... Puis conserver un point de récupération par semaine pendant 3 semaines

... Puis conserver un point de récupération par mois pendant 2 mois

... Puis conserver un point de récupération par mois pendant 1 an

Dans cet exemple, le point de récupération le plus ancien a un an, quatre mois et six jours.

- 7 Lorsque vous êtes satisfait des paramètres de la stratégie de conservation, cliquez sur **Enregistrer**.

La boîte de dialogue intitulée **Configuration** se ferme.

- 8 Dans la boîte de dialogue **Tâches nocturnes**, cliquez sur **OK**.

La boîte de dialogue **Tâches nocturnes** se ferme. La stratégie de conservation que vous avez définie est appliquée au cours du cumul nocturne.

Vous pouvez également appliquer ces paramètres lorsque vous configurez la stratégie de conservation d'une machine protégée individuelle. Pour plus d'informations sur la configuration d'une stratégie de conservation pour une machine protégée, veuillez consulter [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).

Personnalisation des paramètres de la stratégie de conservation pour une machine protégée

La stratégie de conservation d'une machine protégée précise la durée de conservation des points de récupération au sein de la logithèque. Généralement, toutes les machines protégées utilisent la stratégie de conservation par défaut établie pour le Noyau, à moins que vous n'ayez paramétré une stratégie de conservation personnalisée, comme il est décrit dans cette procédure.

Suivez cette procédure pour paramétrer une stratégie de conservation personnalisée sur une machine protégée, y compris une machine répliquée.

- 1 Depuis le menu Machines protégées situé dans la console du Noyau de la Rapid Recovery, cliquez sur le nom de la machine que vous souhaitez modifier.
La page **Récapitulatif** de la machine sélectionnée apparaît.
- 2 Cliquez sur le menu **Paramètres**.
La page **Paramètres** apparaît, affichant les paramètres de configuration pour la machine sélectionnée.
- 3 Il est également possible de cliquer sur le lien **Tâches nocturnes** et de faire défiler la page Paramètres vers le bas pour visualiser les paramètres des tâches nocturnes.
- 4 Sous le titre Tâches nocturnes, cliquez sur  **Modification**.
La boîte de dialogue **Tâches nocturnes** s'affiche.
- 5 Pour spécifier les périodes pendant lesquelles conserver les données sauvegardées, sélectionnez **Cumul**, puis cliquez sur **Paramètres**.
La boîte de dialogue **Configuration** pour la stratégie de conservation s'affiche.
- 6 Si vous êtes en train de personnaliser les paramètres d'une stratégie de conservation pour une machine répliquée et que vous voyez apparaître un message d'avertissement vous invitant à effectuer une vérification de l'intégrité de votre logithèque, faites-le. Dans l'autre cas, passez à l'étape suivante.
 - a Si vous êtes prêt à effectuer cette opération, cliquez sur **Vérifier l'intégrité**
 - b Cliquez sur **Oui** pour confirmer l'opération de vérification de l'intégrité.

REMARQUE : l'exécution de cette opération peut être particulièrement longue, en fonction de la taille de votre logithèque. Au cours de cette opération, il est impossible d'effectuer une autre action (instantané, réplication, exportation virtuelle, etc.) dans cette logithèque. Pour plus d'informations à propos de cette opération, veuillez consulter [À propos de la vérification de l'intégrité des référentiels DVM](#).

- Une fois que l'opération de vérification de l'intégrité a effectué toutes les opérations subordonnées, reprenez cette procédure et passez à l'étape suivante.
- 7 Dans la boîte de dialogue **Configuration**, effectuez l'une des actions suivantes :
 - Pour utiliser la stratégie de conservation par défaut sur cette machine protégée, sélectionnez **Utiliser la stratégie de conservation par défaut du Noyau**, puis cliquez sur **Enregistrer**. La stratégie par défaut est appliquée à cet agent.
 - Pour personnaliser une stratégie de conservation pour cet agent, sélectionnez **Utiliser une stratégie de conservation personnalisée**, puis passez à l'étape suivante.

La boîte de dialogue **Configuration** se développe pour afficher les informations de la stratégie de conservation personnalisée.

- 8 Saisissez la planification personnalisée de conservation des points de récupération, comme il est décrit dans le tableau suivant.

Tableau 126. Options de planification de la stratégie de conservation personnalisée

Zone de texte	Description
Conserver tous les points de récupération pendant n [période de conservation]	Indique la période de conservation des points de récupération. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 3 jours. Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par heure pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation sur laquelle se base le paramètre principal pour déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 2 jours. Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par jour pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 4 jours. Vous pouvez sélectionner une de ces options : jours, semaines, mois ou années
... Puis conserver un point de récupération par semaine pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 3 semaines. Vous pouvez sélectionner une de ces options : semaines, mois ou années
... Puis conserver un point de récupération par mois pendant n [période de conservation]	Fournit un niveau de conservation plus granulaire. Cette option est la fondation permettant de déterminer pendant combien de temps les points de récupération sont conservés. Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. La valeur par défaut est 2 mois. Vous pouvez sélectionner une de ces options : mois ou années
... Puis conserver un point de récupération par an pendant n [période de conservation]	Saisissez un nombre représentant la période de conservation, puis sélectionnez l'unité. Vous pouvez sélectionner : années

L'exemple suivant montre comment la période de conservation est calculée.

Conserver tous les points de récupération pendant trois jours.

... Puis conserver un point de récupération par heure pendant 3 jours

... Puis conserver un point de récupération par jour pendant 4 jours

... Puis conserver un point de récupération par semaine pendant 3 semaines

... Puis conserver un point de récupération par mois pendant 2 mois

... Puis conserver un point de récupération par mois pendant 1 an

Dans cet exemple, le point de récupération le plus ancien a un an et trois mois.

- 9 Si vous souhaitez conserver tous les points de récupération dans votre logithèque principale, désélectionnez l'option **Déplacer les points de récupération obsolètes vers une logithèque R3** et passez l'étape suivante.
 - 10 Si vous souhaitez déplacer des points de récupération depuis votre logithèque principale vers une logithèque R3 stockée sur un appareil de sauvegarde Dell série DR, procédez comme suit :
 - a Sélectionnez l'option **Déplacer les points de récupération obsolètes vers une logithèque R3**.
 - b Précisez l'âge à partir duquel vous souhaitez déplacer les points de récupération depuis votre logithèque principale vers la logithèque R3.

Vous pouvez préciser l'âge en semaine, en mois ou en années. La période minimale que vous pouvez définir est une semaine.
 - c Depuis le menu déroulant **Sélectionner une logithèque**, sélectionnez la logithèque R3 devant recevoir les points de récupération spécifiés.
- REMARQUE :** quel que soit l'emplacement où se trouvent les points de récupération (une logithèque DVM locale ou une logithèque R3 à distance située sur un appareil de sauvegarde DR), ils sont toujours soumis à la stratégie de conservation et au cumul. Si vous devez conserver des points de récupération plus anciens, l'une des méthodes possibles est l'archivage. La seconde est de désactiver le cumul ou de prolonger la période de conservation pour les machines protégées concernées.
- 11 Cliquez sur **Enregistrer**.

Forçage de la consolidation d'une machine protégée

Vous pouvez contourner votre stratégie de rétention planifiée en forçant la consolidation des points de restauration au niveau de la machine protégée.

- 1 À partir du menu Machines protégées de la console Core Rapid Recovery, cliquez sur le nom d'une machine protégée.

La page **Synthèse** de la machine sélectionnée s'affiche.
- 2 Cliquez sur le menu déroulant **Plus** en haut de la vue de la machine protégée, puis sélectionnez **Stratégie de rétention**.

La page **Stratégie de rétention** de la machine spécifiée s'affiche.
- 3 Cliquez sur **Forcer la consolidation**.
- 4 Dans la boîte de dialogue, cliquez sur **Oui** pour confirmer.

Rapid Recovery lance la consolidation de cette machine, quelle que soit la planification de la stratégie de rétention.

Réplication

Cette section décrit comment configurer et gérer la réplication des données protégées depuis un Core source Rapid Recovery vers un Core cible Rapid Recovery pour permettre une restauration après sinistre.

Réplication avec Rapid Recovery

Cette section fournit des informations conceptuelles et pratiques pour vous aider à comprendre et à configurer la réplication dans Rapid Recovery.

La **réplication** est un processus qui consiste à copier les points de restauration d'un Core Rapid Recovery vers un autre Core Rapid Recovery afin de les restaurer en cas de sinistre. Ce processus exige une relation d'appariement source-cible entre au moins deux Cores.

Le Core source copie les points de restauration des machines protégées sélectionnées, puis transmet les données d'instantané de manière asynchrone et continue vers le Core cible.

Sauf si vous modifiez son comportement par défaut en définissant une planification de réplication, le Core lance une tâche de réplication immédiatement après chaque instantané de sauvegarde, vérification de somme de contrôle, vérification de la capacité d'attachement ou tâche nocturne. Pour en savoir plus, voir [Planifier la réplication](#).

Pour garantir une protection optimale des données, les administrateurs utilisent généralement un Core cible hébergé sur un site de restauration après sinistre distant. Vous pouvez configurer la réplication sortante vers un centre de données d'entreprise, vers un site de restauration après sinistre distant (à savoir, un Core cible « auto-géré »), vers un fournisseur tiers de services gérés (MSP) ou un fournisseur de stockage Cloud qui héberge des services de sauvegarde et de restauration après sinistre hors site. Lors de la réplication vers un Core cible tiers, vous pouvez utiliser des flux de travail intégrés permettant de demander des connexions et de recevoir des notifications automatiques en retour.

La réplication est gérée en fonction des machines protégées. Toute machine (ou toutes les machines) protégée ou répliquée sur un Core source peut être configurée pour être répliquée vers un Core cible.

Scénarios de réplication possibles :

- **Réplication sur un emplacement local.** Le Core cible est situé dans un centre de données local ou un emplacement sur site, et la réplication est assurée à tout moment. Dans cette configuration, la perte du Core ne peut pas empêcher la restauration.
- **Réplication sur un emplacement hors site.** Le Core cible est situé dans une installation hors site prévue pour la restauration en cas de perte (sinistre).
- **Réplication mutuelle.** Deux centres de données se trouvant à deux emplacements différents contiennent chacun un Core et protègent les machines en se servant réciproquement de sauvegarde hors site en vue d'une restauration après sinistre. Dans ce scénario, chaque Core réplique les machines protégées sur le Core situé dans l'autre centre de données.
- **Réplication hébergée ou en Cloud.** Les partenaires MSP de Rapid Recovery gèrent plusieurs Cores cibles dans un centre de données ou dans un Cloud public. Sur chacun de ces Cores, le partenaire MSP permet à un ou plusieurs clients de répliquer des points de restauration d'un Core source situé sur le site du client vers le Core cible situé sur le site du MSP moyennant des frais.

① | **REMARQUE :** dans ce scénario, les clients ont uniquement accès à leurs propres données.

Configurations de réplication possibles :

- **Réplication d'un point unique vers un point unique.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core source unique vers un Core cible unique.

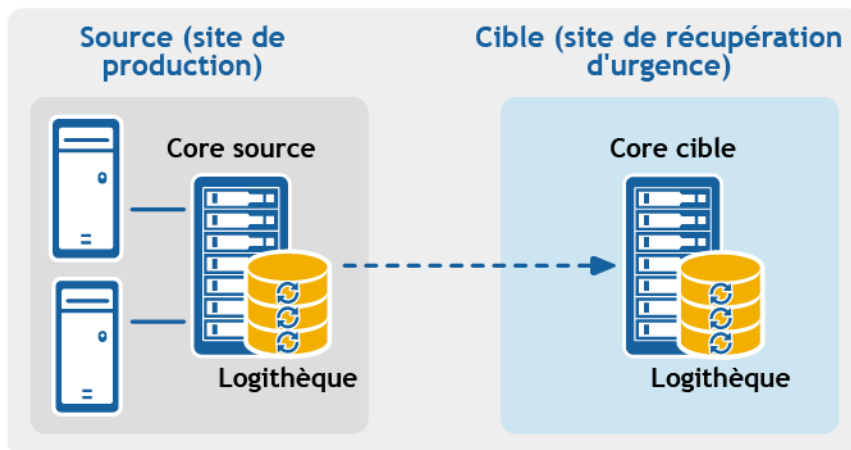


Figure 9. Configuration de réplication d'un point unique vers un point unique

- **Réplication de plusieurs points vers un point unique.** Réplique les machines protégées de plusieurs Cores source vers un Core cible unique.

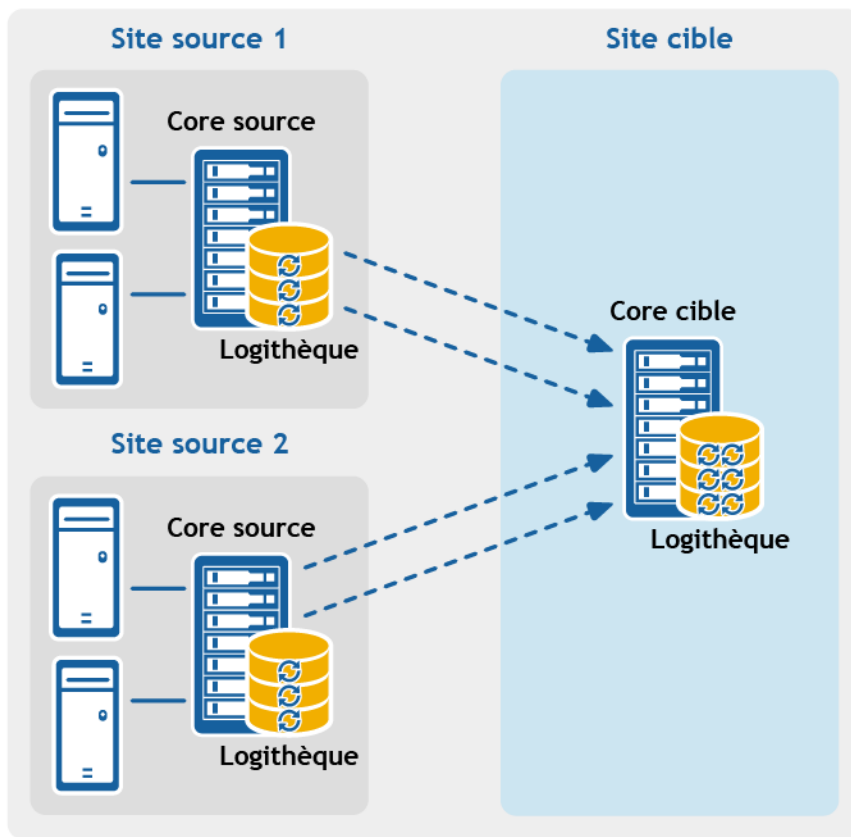


Figure 10. Configuration de réplication de plusieurs points vers un point unique

- **Réplication d'un point unique vers plusieurs points.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core source unique vers plusieurs Cores cibles.

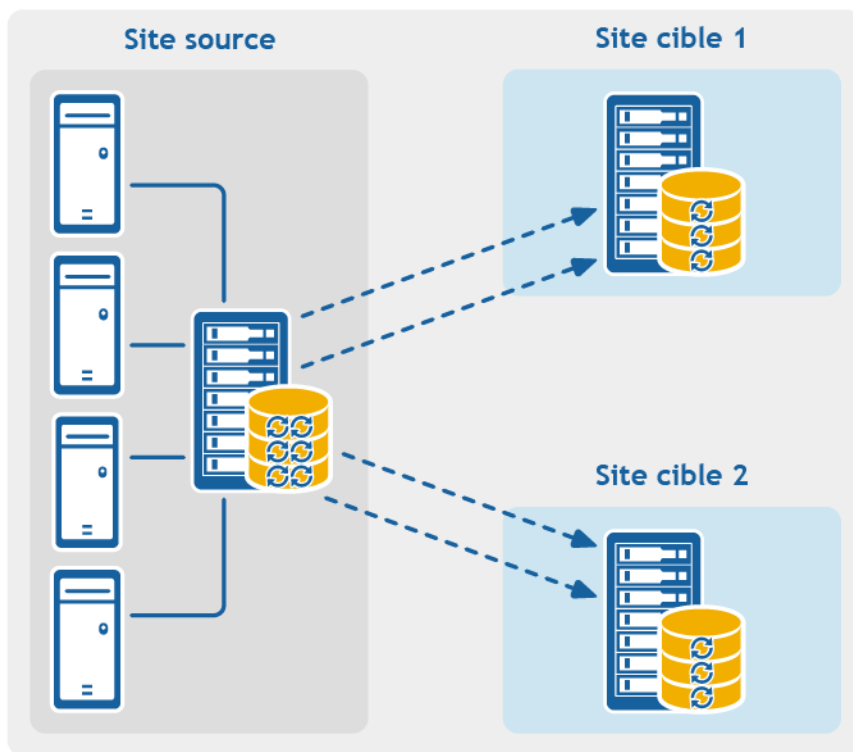


Figure 11. Configuration de réplication d'un point unique vers plusieurs points

- **Réplication multicible.** Réplique une ou plusieurs machine(s) protégée(s) d'un Core cible vers un autre Core cible, offrant ainsi des options de basculement ou de restauration supplémentaires sur le Core répliqué.

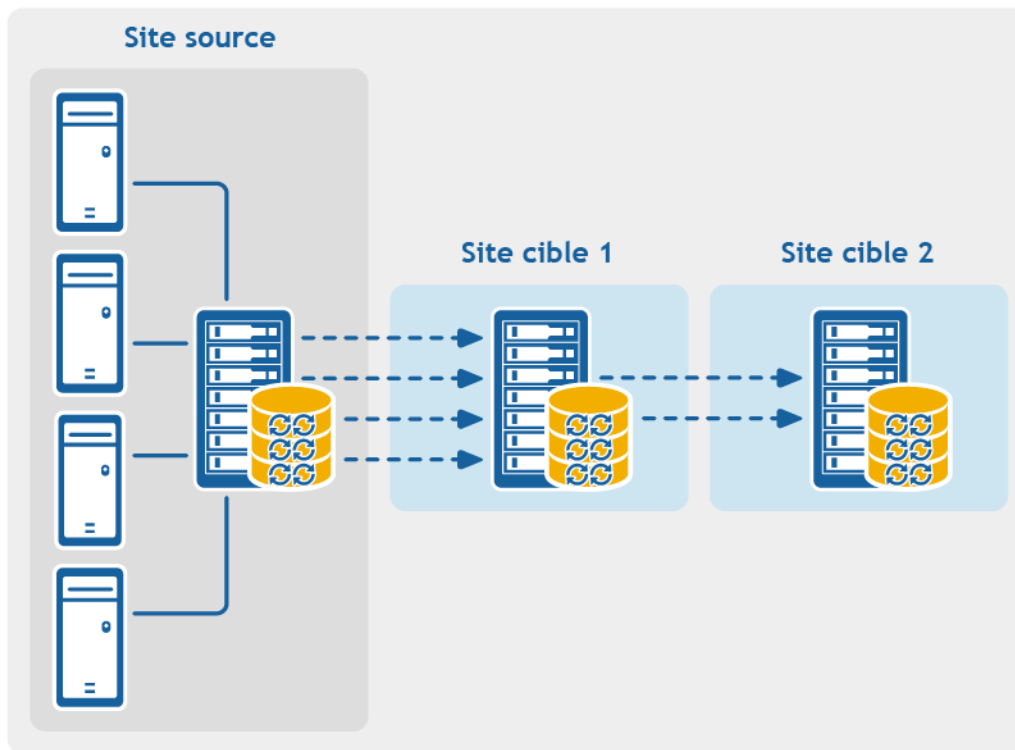


Figure 12. Configuration de réplication multicible

Si vous utilisez des appliances de sauvegarde Dell Data Protection (ex. : séries DL1x00 ou DL4x00), veillez à ce que le Core cible de la réplication dispose d'une licence logicielle valide. Chaque appliance matérielle achetée inclut une licence pour la cible de réplication. La clé de licence se trouve dans l'e-mail de bienvenue que vous avez reçu lors de l'achat de l'appliance. Pour obtenir de l'aide, consultez notre page d'aide relative aux licences à l'adresse <https://support.software.dell.com/licensing-assistance> ou envoyez un e-mail à license@software.dell.com.

Points de restauration en chaîne et orphelins

Rapid Recovery crée des instantanés d'une machine protégée, puis les enregistre dans une logithèque en tant que *points de restauration*. Le premier point de restauration enregistré sur le Core s'appelle l'*image de base*. L'image de base comprend le système d'exploitation, les applications et les paramètres pour chaque volume que vous choisissez de protéger, ainsi que toutes les données sur ces volumes. Les points de restauration suivants sont appelés *instantanés incrémentiels*, ils sont constitués uniquement des données modifiées trouvées sur les volumes protégés depuis la dernière sauvegarde. L'image de base et tous les instantanés incrémentiels forment ensemble une *chaîne de points de restauration* complète.

À partir d'une chaîne de points de restauration complète, vous pouvez facilement restaurer les données à l'aide de la gamme complète d'options de restauration disponibles sur Rapid Recovery. Ces options incluent la restauration de fichier, de volume et même la restauration BMR (bare metal restore).

Puisque vous ne pouvez pas restaurer des données qui n'existent pas, dans le cas d'une chaîne de points de restauration incomplète, vous ne pouvez pas restaurer les données au niveau du volume ou effectuer une restauration BMR. Dans ces cas-là, vous pouvez toujours restaurer toutes les données qui existent dans un point de restauration au niveau des fichiers.

Si les informations que vous souhaitez restaurer à partir d'un point de restauration sont dans une sauvegarde précédente qui n'est pas disponible dans le Core (une version précédente d'instantané incrémentiel ou l'image de base), le point de restauration est alors dit *orphelin*. Les points de restauration orphelins sont typiques dans certains scénarios de réplication.

Par exemple, lorsque vous définissez la réplication pour la première fois, les options de restauration des données à partir des points de restauration répliqués sont limitées. Tant que toutes les données sauvegardées du Core source sont transmises au Core cible, créant ainsi des chaînes complètes de points de restauration à partir des orphelins, vous ne pouvez effectuer qu'une restauration au niveau des fichiers.

Lorsque la réplication commence

Par défaut, les tâches de transfert de réplication sont automatiquement mises en file d'attente par le Core immédiatement après chaque sauvegarde régulière planifiée. Ainsi, sauf si vous avez personnalisé la planification de réplication pour une machine protégée, la planification de réplication est basée sur la planification d'instantané de sauvegarde standard.

Lorsque vous commencez à configurer la réplication, s'il y a un ou plusieurs point(s) de restauration sur le Core source, le processus de réplication commence immédiatement, sauf si :

- Vous sélectionnez l'option de suspension initiale de la réplication, ou
- Vous sélectionnez l'option Utiliser un disque source pour effectuer le transfert initial.

Si vous suspendez la réplication au début, elle ne reprendra que lorsque vous le souhaitez.

Si vous configurez une réplication et spécifiez l'utilisation d'un disque source, la réplication vers le Core cible commencera en même temps que le prochain instantané de sauvegarde programmé.

❗ REMARQUE : Vous pouvez également forcer une sauvegarde de la machine protégée après avoir établi la réplication. Ceci fait commencer la réplication immédiatement après que l'instantané de la machine protégée soit terminé.

Si vous spécifiez un disque source lorsque vous configurez la réplication, seuls les futurs transferts de sauvegarde seront répliqués. Si vous souhaitez que des points de restauration existants de la machine protégée d'origine existent sur le Core cible, vous devez implanter les données depuis la machine protégée. Pour implanter les données, créez un disque source à partir du Core source, puis consommez le disque source sur le Core cible.

Vous pouvez également personnaliser la planification de réplication pour une machine protégée. Par exemple, si vous utilisez la planification de protection par défaut d'une sauvegarde par heure, vous pouvez spécifier que le Core source réplique vers le Core cible selon un autre rythme (par exemple, un jour sur deux à 2 h 00).

Détermination de vos besoins et votre stratégie d'implantation

Les rubriques suivantes présentent la restauration depuis des données répliquées et le besoin ou non d'implanter des données de point de restauration depuis le Core source.

Lorsque l'implantation de données est requise

Lorsque vous établissez d'abord la réplication, sauf si vous spécifiez « Utiliser un disque source », le Core source commence la transmission de tous les points de restauration de la machine sélectionnée vers le Core cible. La transmission de vos données sur le réseau peut prendre beaucoup de temps. Cela dépend de la vitesse de votre réseau, de la robustesse de votre architecture réseau et de la quantité de données à transmettre vers le Core cible. Par exemple, si les données sauvegardées sur le Core source font 10 Go et que la vitesse de transfert de la liaison WAN est de 24 Mbits/s, le transfert prend environ une heure.

En fonction de la quantité d'informations que vous souhaitez copier vers le Core cible, le disque source peut ajouter des centaines ou des milliers de gigaoctets de données. La plupart des organisations choisissent de ne pas consommer la bande passante requise et préfèrent définir et consommer un disque source. Pour plus d'informations, voir [Considérations sur les performances pour le transfert de données répliquées](#).

Si vous spécifiez l'utilisation d'un disque source dans les paramètres de la réplication, seuls les points de restauration enregistrés sur le Core source *après* avoir établi une réplication seront répliqués vers le Core cible. Les sauvegardes enregistrées sur le Core source *avant* que la

réplication ne soit établie ne seront pas présents sur le Core cible tant que vous n'implantez pas clairement les données à l'aide du processus suivant.

Pour éviter de ralentir votre réseau avec un transfert éprouvant de données historiques, implantez vos données de sauvegarde existantes sur le Core cible à l'aide d'un **disque source**. Un disque source est un fichier d'archive qui **copie** un ensemble d'images de base dédoublées et d'instantanés incrémentiels depuis le Core source. Le fichier du disque source contient l'intégralité des précédents points de restauration pour les machines protégées que vous souhaitez répliquer à partir du Core source vers le Core cible.

Déplacez le fichier du disque source vers un volume de stockage que vous rendrez ensuite disponible pour le Core cible. Ensuite, vous **consommez** les informations depuis le disque source. Ceci implique d'attacher le volume avec l'image du disque source sur le Core cible et d'importer des données dans la logithèque de la Core Console. Ce processus répare les orphelins, en unifiant des instantanés incrémentiels répliqués sur le Core cible avec leurs images de base, pour former une ou plusieurs chaînes de points de restauration plus complète(s). Ce processus est parfois appelé copier-consommer.

Planter des données à partir de votre Core source n'est pas toujours nécessaire. Par exemple :

- Si vous configurez une réplication pour un nouveau Core Rapid Recovery, l'implantation n'est pas requise.
- Si les données d'un ancien instantané ne sont pas critiques pour vos données répliquées et que vous ne devez pas récupérer de données enregistrées après avoir défini la réplication, l'implantation n'est pas requise.

① REMARQUE : Dans ce cas, Dell recommande d'enregistrer une nouvelle image de base immédiatement avant ou immédiatement après la configuration des réplifications. Cette étape garantit qu'une chaîne de points de restauration complète existe sur le Core cible pour restaurer les données à l'avenir.

- Si vous avez enregistré une image de base immédiatement avant la configuration des réplifications et avez besoin d'effectuer une restauration uniquement à partir des données enregistrées après cette date, l'implantation n'est pas requise.
- Si vous configurez la réplication sans spécifier de disque source, les données d'instantané sont transmises sur le réseau à partir du Core source vers le Core cible.

Si vous êtes concerné par l'une de ces situations, vous n'avez pas besoin d'implanter des données. Dans de tels cas, la réplication peut être réalisée entièrement depuis le Core source.

Si vous configurez la réplication d'un Core avec des points de restauration existants et devez restaurer au niveau du volume, si vous voulez effectuer une restauration BMR ou si vous souhaitez restaurer des données à partir d'une ancienne image de base ou d'un instantané incrémentiel, l'implantation est requise. Dans ces situations, évaluez vos besoins et votre stratégie d'implantation. Passez en revue les informations de cette rubrique et décidez si vous allez planter vers votre Core cible et quelle approche vous utiliserez.

Approches d'implantation de données

Si vous souhaitez que vos machines répliquées sur un Core cible aient accès aux données enregistrées précédemment sur le Core source d'origine, implantez votre Core cible à l'aide de l'une des méthodes suivantes :

- 1 Implantation vers le Core cible sur une connexion réseau.** Spécifiez l'utilisation d'un disque source lorsque vous définissez la réplication. Vous pouvez ensuite partager le dossier contenant le disque source avec le Core cible, puis consommer le fichier du disque source sur le réseau. Pour les données volumineuses ou les connexions les plus lentes, l'implantation par cette méthode peut prendre des heures et consommer beaucoup de bande passante réseau.
① REMARQUE : Dell ne recommande pas l'implantation de données volumineuses sur une connexion réseau. L'implantation initiale peut impliquer des volumes de données très importants, ce qui peut surcharger une connexion WAN standard.
- 2 Le transfert de données de sauvegarde depuis le Core source à l'aide d'un support de stockage physique.** Transférez le fichier du disque source vers périphérique de stockage externe amovible. Cette approche est particulièrement utile dans le cas d'ensembles volumineux de données ou d'une connexion réseau lente. L'implantation avec cette méthode nécessite d'effectuer les étapes suivantes :
 - a Créez une archive source depuis le Core source, en l'enregistrant sur le support amovible.
 - b Amenez le disque source là où se trouve le Core cible.
 - c Attachez le disque au Core cible.
 - d Consommez les données à partir du disque source dans la logithèque du Core cible.

Si vous répliquez vers un Core tiers, une fois que votre support est reçu par le MSP, un représentant du centre de données attachera votre support et vous préviendra lorsque tout sera prêt pour que vous consommiez (ou importiez) les données d'implantation vers le Core.

① REMARQUE : Compte tenu des volumes importants de données devant être copiés vers le périphérique de stockage, une connexion eSATA, USB 3.0 ou toute autre connexion haut débit est recommandée. Si la taille totale de l'archive des données d'implantation est supérieure à l'espace disponible sur le support amovible, elle est alors répartie sur plusieurs périphériques.

- 3 **Pour les Cores source cible stockés sur des hôtes virtuels, le transfert des données de sauvegarde à l'aide d'un disque dur virtuel.** Si vos Cores source et cible sont tous sur un hôte virtuel, vous pouvez définir et consommer un disque source sur un support de stockage virtuel. L'implantation avec cette méthode nécessite d'effectuer les étapes suivantes :
- Créez un fichier de disque source depuis le Core source, enregistrez-le dans un volume de stockage virtuel.
 - Détachez le volume à partir du Core source et attachez-le au Core cible.
 - Consommez les données à partir du disque source dans la logithèque du Core cible.

① REMARQUE : Tandis que la réplication d'instantanés incrémentiels peut se produire entre les Cores sources et les Cores cibles avant la fin de l'implantation, les instantanés répliqués transmis de la source au Core restent orphelins jusqu'à la consommation des données initiales et sont associés aux images de base répliquées.

Liens connexes

- Pour plus de détails sur le processus de la consommation du disque source, voir la rubrique [Consommation du disque source sur un Core cible](#).
- Pour en savoir plus sur les points de restauration orphelins, voir [Supprimer une chaîne de points de restauration orphelins](#).
- Pour plus d'informations sur la préparation d'un disque source, voir [Description des disques sources](#) et [Consommation du disque source sur un Core cible](#).

Liens connexes

[Consommation du disque source sur un Core cible](#)
[Supprimer une chaîne de points de restauration orphelins](#)

Considérations sur les performances pour le transfert de données répliquées

Si la bande passante entre les Cores sources et cibles ne peut pas supporter le transfert des points de restauration stockés, configurez une réplication et spécifiez l'utilisation d'un disque source. Ce processus plante dans le Core cible des images de base et des points de restauration venant des serveurs protégés sélectionnés sur le Core source. Le processus d'implantation peut être réalisé à n'importe quel moment. L'implantation peut être effectuée en tant que partie du transfert initial des données, qui sert de fondation en cas de répliqués planifiés réguliers. Vous pouvez également planter des données pour une machine précédemment répliquée si la réplication a été suspendue ou supprimée. Dans ce dernier cas, l'option « Créer des chaînes de points de restauration » vous permet de copier vers un disque source les points de restauration pas encore répliqués.

Lors de la préparation de la réplication, veuillez considérer les facteurs suivants :

- Taux de modification.** Le taux de modification indique la vitesse d'accumulation des données protégées. Le taux dépend de la quantité de données modifiée sur les volumes protégés et de l'intervalle de protection des volumes. Certains types de machine ont généralement un taux de modification plus élevé, comme c'est le cas pour un serveur d'e-mail Exchange. Une façon de réduire la vitesse de modification est de réduire l'intervalle de protection.
- Bande passante.** La bande passante est la vitesse de transfert présente entre le Core source et le Core cible. Il est essentiel que la bande passante soit supérieure au taux de modification afin de suivre le rythme des points de restauration créés par les instantanés. Pour les transferts de données lourdes transmises de Core à Core, il se peut que plusieurs flux parallèles puissent avoir besoin de fonctionner à une vitesse de connexion Ethernet de 1 Go.

REMARQUE : Ce qui correspond généralement, selon la plupart des FAI, à la bande passante totale disponible. Tous les périphériques sur le réseau partagent la bande passante sortante. Vérifiez que la bande passante disponible est suffisante pour que la réplication puisse accepter le taux de modification.

- **Nombre de machines protégées.** Il est important de prendre en considération le nombre de machines protégées par Core source, ainsi que la quantité que vous prévoyez de répliquer sur le Core cible. Vous n'êtes pas obligé de répliquer toutes les machines protégées sur le Core source ; Rapid Recovery vous permet de répliquer sur la base d'une machine protégée, pour vous permettre de choisir de répliquer uniquement certaines machines, si vous le souhaitez. Si toutes les machines protégées sur un Core source doivent être répliquées, la vitesse de modification est généralement plus élevée. Ce facteur est pertinent si la bande passante entre les Cores source et cible est insuffisante pour la quantité et la taille des points de restauration en cours de réplication.

Le taux de modification maximal pour les types de connexion WAN est représenté dans le tableau ci-dessous, avec des exemples de bande passante nécessaire par gigaoctet pour un taux de modification raisonnable.

Tableau 127. Exemples de bandes passantes par gigaoctets

Haut débit	Bande passante	Taux de modification maximal
ADSL	768 Kbits/s et plus	330 Mo par heure
Câble	1 Mbits/s et plus	429 Mo par heure
T1	1,5 Mbits/s et plus	644 Mo par heure
Fibre	20 Mbits/s et plus	8,38 Go par heure

REMARQUE : Pour des résultats optimaux, suivez les recommandations indiquées dans le tableau précédent.

Si une liaison est défaillante pendant le transfert des données, la réplication reprend à partir du point d'échec du transfert précédent (une fois la liaison restaurée).

En fonction de la configuration du réseau, la réplication peut être longue. Assurez-vous de bien avoir suffisamment de bande passante pour la réplication et d'autres transferts Rapid Recovery comme les sauvegardes, ainsi que toute autre application critique que vous devez exécuter.

Si vous ne parvenez pas à effectuer un transfert de données sur le réseau sans erreur, notamment pour certaines machines protégées ou répliquées, essayez de modifier la vitesse du transfert de données pour ces machines. Pour plus d'informations, voir [À propos de la modification des paramètres de transfert](#) et [Limitation de la vitesse de transfert](#).

À propos de la réplication et des points de restauration chiffrés

Bien qu'il ne contienne pas de sauvegardes du registre et des certificats du Core source, le disque source contient les clés de chiffrement du Core source si les points de restauration en cours de réplication du Core source au Core cible sont chiffrés. Les points de restauration répliqués restent chiffrés après avoir été transmis vers le Core cible. Les propriétaires ou les administrateurs du Core cible ont besoin de la phrase secrète pour récupérer les données chiffrées.

À propos des stratégies de rétention de la réplication

Les stratégies de rétention sur les Cores source et cible ne sont pas synchronisées. La consolidation et la suppression à la demande fonctionnent indépendamment sur chacun des Cores, pour l'action initiale, ainsi que lors de l'exécution des tâches nocturnes.

Pour en savoir plus sur les stratégies de rétention, voir [Gestion des stratégies de conservation](#).

Réplication vers un core cible autogéré

Cette configuration s'applique à la réplication vers un emplacement hors site et à la réplication mutuelle. Les étapes suivantes sont prérequis :

- Rapid Recovery Core doit être installé sur toutes les machines source et cible.
- Si vous configurez Rapid Recovery pour une réplication multipoint à point, vous devez réaliser cette tâche sur tous les cores source et sur le core cible. Pour une explication de ces configurations de réplication, voir [Réplication](#).
- Si vous avez besoin de créer un lecteur de départ et de le transférer sur un volume de stockage amovible physique afin d'effectuer le transfert initial des points de restauration existants, vous devez disposer d'un périphérique de stockage mobile adapté prêt à l'emploi. Vous devez également disposer d'un accès physique à la machine core source pour attacher le lecteur sur lequel copier l'archive source.
- Si vous utilisez un lecteur de départ sur un core cible autogéré, vous ou un administrateur de confiance devez avoir un accès physique au core cible.

Un core cible autogéré est un core auquel vous avez accès. Par exemple, un core autogéré est souvent géré par votre entreprise dans un emplacement hors site ou il est hébergé sur un lieu différent de celui du core source. La réplication peut être configurée entièrement sur le core source, sauf si vous choisissez de créer des données de départ à l'aide d'un lecteur de départ. Dans ce cas, vous devez créer un lecteur de départ à l'aide de cette procédure et attacher ensuite ce lecteur au core cible pour consommer les données archivées de points de restauration. Pour plus d'informations, reportez-vous à [Détermination de vos besoins et votre stratégie d'implantation](#).

Procédez comme indiqué ci-après pour configurer votre core source afin qu'il se réplique vers un core cible autogéré.

- 1 Allez à la console Core Rapid Recovery du core source.
- 2 Dans la barre de boutons, cliquez sur  **Répliquer**.
L'**Assistant de réplication** apparaît.
- 3 Dans la page **Core cible** de l'Assistant de réplication, si vous établissez une réplication avec un core cible qui a été précédemment couplé avec ce core source, sélectionnez **Utiliser un core cible existant**, puis sélectionnez le core cible approprié dans la liste déroulante. Passez à l'étape 5.
- 4 Dans la page **Core cible** de l'Assistant de réplication, si vous établissez pour la première fois une réplication avec un core cible à partir de ce core source, sélectionnez **J'ai mon propre core cible**, puis entrez les informations décrites dans le tableau suivant.

Tableau 128. Informations sur le core cible

Zone de texte	Description
Nom d'hôte	Entrez le nom d'hôte ou l'adresse IP de la machine core vers lequel vous souhaitez répliquer.
Port	Le numéro du port sur lequel le core Rapid Recovery va communiquer avec le référentiel sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Entrez le nom d'utilisateur permettant d'accéder à la machine.
Mot de passe	Entrez le mot de passe d'accès à la machine.

- 5 Cliquez sur **Suivant**.

 **REMARQUE :** Si aucun référentiel n'existe sur le core cible, un avertissement s'affiche, vous signalant que vous pouvez coupler le core source avec le core cible, mais que vous ne pourrez répliquer les agents (machines protégées) vers cet emplacement que lorsqu'un référentiel y aura été établi. Pour plus d'informations sur la façon de configurer un référentiel vers un core, voir [Créer un référentiel DVM](#).

- 6 Dans la page **Demande**, entrez le nom de cette configuration de réplication ; par exemple, SourceCore1. Il s'agit du nom d'affichage qui sera utilisé pour le volet Réplication entrante dans la page Réplication du core cible.
- 7 Cliquez sur **Suivant**.

- 8 Dans la page **Machines protégées**, sélectionnez les machines protégées à répliquer, puis utilisez les listes déroulantes dans la colonne Référentiel pour sélectionner un référentiel pour chacune de ces machines protégées.
- 9 Si vous voulez effectuer le processus de départ pour le transfert de la base de données, procédez comme suit :

REMARQUE : En raison des quantités importantes de données à copier vers le périphérique de stockage portable, Dell recommande d'utiliser une connexion eSATA, USB 3.0 ou autre à haut débit vers ce périphérique de stockage portable.

- a Dans la page **Machines protégées** de l'Assistant de réplication, sélectionnez **Utiliser un lecteur de départ pour effectuer le transfert initial**.
 - Si vous disposez actuellement d'une ou plusieurs machines protégées se répliquant vers un core cible, vous pouvez inclure ces machines protégées dans le lecteur de départ, en sélectionnant **Inclure sur le lecteur de départ les points de restauration déjà répliqués**.
- b Cliquez sur **Suivant**.
- c Dans la page **Emplacement du lecteur de départ** de l'Assistant de réplication, utilisez la liste déroulante **Type d'emplacement** pour sélectionner l'un des types de destination suivants :
 - Local
 - Réseau
 - Cloud
- d Entrez les détails du fichier sur le lecteur de départ comme indiqué dans le tableau suivant, en fonction du type d'emplacement que vous avez sélectionné en c.

Tableau 129. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où doit résider l'archive du lecteur de départ. Par exemple, D:\work\archive.
Réseau	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où doit résider l'archive du lecteur de départ. Par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Il est utilisé pour établir les références de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe pour le partage réseau. Il est utilisé pour établir les références de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
	Conteneur	Sélectionnez un conteneur associé à votre compte dans le menu déroulant.
	Nom de dossier	Entrez le nom du dossier dans lequel vous souhaitez enregistrer les données archivées. Le nom par défaut est Rapid-Recovery-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION]

- e Cliquez sur **Suivant**.
- f Dans la page **Options du lecteur de départ** de l'Assistant Réplication, entrez les informations décrites dans le tableau suivant.

Tableau 130. Options du lecteur de départ

Élément	Description
Taille maximale	Les grandes archives de données peuvent être divisées en plusieurs segments. Sélectionnez la taille maximale du segment à réserver pour la création du lecteur source en effectuant l'une des opérations suivantes : • Sélectionnez Toute la cible pour réserver l'intégralité de l'espace disponible dans le chemin indiqué dans la page Emplacement du lecteur de départ. Par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le disque D: sera réservé si nécessaire pour la copie du lecteur de départ, mais il n'est pas réservé immédiatement après le démarrage de la copie. • Sélectionnez la zone de texte, entrez une quantité, puis sélectionnez une unité de mesure dans la liste déroulante afin de personnaliser la quantité maximale d'espace à réserver. La valeur par défaut est de 250 Mo.
Action de recyclage	Au cas où le chemin contiendrait déjà un lecteur d'amorçage, sélectionnez l'une des options suivantes : • Ne pas réutiliser : N'écrase ni n'efface aucune donnée de départ existante. Si l'emplacement n'est pas vide, l'écriture sur le lecteur de départ échouera. • Remplacer ce core. Écrase toutes les données pré-existantes appartenant à ce core mais laisse intactes les données des autres cores. • Effacer complètement. Efface toutes les données du répertoire avant d'écrire sur le lecteur de départ.
Commentaire	Entrez un commentaire décrivant le lecteur de départ.
Ajouter tous les agents au lecteur source	Sélectionnez cette option pour répliquer à l'aide du lecteur de départ toute les machines protégées sur le core source. Cette option est sélectionnée par défaut.
Créer des chaînes de points de restauration (réparer les orphelins)	Sélectionnez cette option pour répliquer l'intégralité de la chaîne de points de restauration vers le lecteur source. Cette option est sélectionnée par défaut. REMARQUE : Le processus normal dans AppAssure 5.4 ne répliquait vers le lecteur de départ que le dernier point de restauration, ce qui réduisait la durée et l'espace requis pour créer le lecteur de source. Choisir de créer des chaînes de points de restauration vers le lecteur de départ nécessite de disposer de suffisamment d'espace suffisant sur le lecteur de départ pour y stocker les derniers points de restauration des machines protégées et peut rallonger la durée d'exécution de la tâche.

g Effectuez l'une des opérations suivantes :

- Si vous avez désélectionné la case à cocher **Ajouter tous les agents au lecteur de départ**, cliquez sur **Suivant**.
- Si vous avez sélectionné **Ajouter tous les agents au lecteur de départ**, passez à l'étape 10.

h Dans la page **Machines protégées** de l'Assistant de réplication, sélectionnez les machines protégées que vous voulez répliquer vers le core cible à l'aide du lecteur de départ.

10 Cliquez sur **Terminer**.

11 Si vous avez créé un lecteur de départ, envoyez-le au core cible.

Le couplage d'un core source vers le core cible est terminé.

Sauf si vous avez sélectionné l'option de suspension initiale de la réplication, celle-ci démarre immédiatement.

- 1 Si vous avez sélectionné l'option d'utiliser un lecteur de départ, la réplication produit des points de restauration orphelins sur le core cible jusqu'à ce que le lecteur de départ soit utilisé et fournisse les images de base nécessaires.
- 2 Si vous avez spécifié d'utiliser un disque, transférez le fichier d'archive du lecteur de départ vers un volume (dossier partagé, disque virtuel ou support de stockage amovible). Puis, utilisez le lecteur de départ.

Affichage des réplifications entrantes et sortantes

Si vous cliquez sur l'icône **Réplication**  de la barre d'icônes, la page **Réplication** s'affiche. Cette page vous aide à mieux comprendre la réplication dans le champ de ce Core. Celle-ci comprend deux volets :

- Le volet **Réplication sortante** répertorie tous les machines protégées dans ce Core qui sont répliquées sur un autre Core.
- Le volet **Réplication entrante** répertorie les machines répliquées sur ce Core, et le Core source à partir duquel ces machines sont répliquées.

Cette section décrit les informations affichées dans les volets suivants.

Les informations sur la réplication sortante à partir de ce Core Rapid Recovery sont décrites dans le tableau suivant.

Tableau 131. Informations sur la réplication sortante

Élément de l'UI	Description
Sélectionner des éléments	Pour chaque ligne du tableau récapitulatif, vous pouvez sélectionner la case à cocher pour effectuer des actions contenues dans la liste des options du menu, au-dessus du tableau.
Type	Affiche le type de machine. Vous pouvez développer un Core cible pour afficher les différentes machines répliquées.
Indicateur d'état	État de la réplication Les cercles de couleur dans la colonne État indiquent si une machine répliquée est en ligne ou indisponible. Si vous passez le curseur de la souris sur le cercle de couleur, l'état exact s'affiche. Les états possibles sont les suivants : vert (réplication établie et machine en ligne), jaune (réplication suspendue), rouge (erreur d'authentification) et gris (hors ligne ou indisponible).
Replication Name (Nom de réplication)	Le nom d'affichage du Core vers lequel sont répliquées les machines de ce Core source.
Machines	Répertorie le nombre de machines répliquées vers le Core cible sélectionné.
Synchroniser	La date et l'heure du dernier transfert de réplication vers le Core cible.
	Lorsque vous cliquez sur le menu déroulant Actions de cette colonne, vous apercevez une liste d'actions à effectuer, celles-ci permettent de modifier la relation de réplication spécifique.

Vous pouvez exécuter des actions sur deux Cores ou plus répertoriés dans la grille des réplifications sortantes. Pour exécuter des actions sur plusieurs Cores cibles, cochez la case de chacun des Cores de la grille. Ensuite, à partir du menu situé au-dessus de la grille, sélectionnez l'action à exécuter. Vous pouvez exécuter les actions décrites dans le tableau suivant.

Tableau 132. Actions globales disponibles dans le volet Réplication sortante

Élément de l'UI	Description
Ajouter un Core cible	Vous permet de définir un autre Core cible pour répliquer les machines protégées sur ce Core source.
Actualiser	Actualise les informations présentées dans le tableau.
Forcer	Force la réplication.
Suspendre	Interrompt la réplication établie.
Reprendre	Reprend une réplication en pause.

Élément de l'IU	Description
Copier	Ouvre l'Assistant de réplication, cela permet la copie des points de récupération existants des machines protégées sélectionnées vers un disque source.
Supprimer	Supprime la réplication sortante.
Disques sources	Cette option de menu s'affiche si des données ont été copiées sur un disque source lors de la configuration de la réplication. Affiche les informations sur le fichier du disque source, y compris les données et l'heure de sauvegarde du disque source. Les menus déroulants indiquent le Core cible et les machines protégées à partir desquels les fichiers du disque source ont été générés.
	Lorsque vous cliquez sur le menu déroulant Actions de cette colonne, vous apercevez une liste d'actions à effectuer, celles-ci permettent de modifier la relation de réplication spécifique.

Les informations sur la réplication entrante à partir d'un autre Core sont décrites dans le tableau suivant.

Tableau 133. Informations sur la réplication entrante

Élément de l'IU	Description
Sélectionner des éléments	Pour chaque ligne du tableau récapitulatif, vous pouvez sélectionner la case à cocher pour effectuer des actions contenues dans la liste des options du menu, au-dessus du tableau.
Type	Affiche le type de machine. Vous pouvez développer un Core source pour afficher les machines répliquées.
Indicateur d'état	État de la réplication Les cercles de couleur dans la colonne État indiquent si une machine répliquée est en ligne ou indisponible. Si vous passez le curseur de la souris sur le cercle de couleur, l'état exact s'affiche. Les états possibles sont les suivants : vert (réplication établie et machine en ligne), jaune (réplication suspendue), rouge (erreur d'authentification) et gris (hors ligne ou indisponible).
Replication Name (Nom de réplication)	Le nom d'affichage du Core source contenant machines protégées répliquées sur ce Core cible. Ce nom peut également être spécifié lors de l'établissement de la réplication sur le Core source à l'aide de l'Assistant de réplication.
Machines	Indique le nombre de machines protégées sur le Core source étant répliquées sur ce Core cible.
Synchroniser	La date et l'heure du dernier transfert de réplication depuis le Core source.
	Lorsque vous cliquez sur le menu déroulant Actions de cette colonne, vous apercevez une liste d'actions à effectuer, celles-ci permettent de modifier la relation de réplication spécifique.

Vous pouvez exécuter des actions sur deux Cores source ou plus répertoriés dans la grille des réplications entrantes. Pour exécuter des actions sur plusieurs Cores source, cochez la case de chacun des Cores de la grille. Ensuite, à partir du menu situé au-dessus de la grille, sélectionnez l'action à exécuter. Vous pouvez exécuter les actions décrites dans le tableau suivant.

Tableau 134. Actions globales disponibles dans le volet Réplication entrante

Élément de l'IU	Description
Actualiser	Actualise les informations présentées dans le tableau.
Forcer	Force la réplication.
Suspendre	Interrompt la réplication établie.
Reprendre	Reprend une réplication en pause.
Supprimer	Supprime une réplication entrante.

Configuration d'une réplication

Pour répliquer des données à l'aide de la Rapid Recovery, vous devez configurer les nœuds source et cible pour réplication. Une fois ceci fait, vous pouvez alors répliquer les données de machines protégées, surveiller et gérer les répliqués et procéder à des récupérations.

Le processus de réplication dans la Rapid Recovery implique d'effectuer les opérations suivantes :

- Configurer une logithèque sur le nœud cible. Pour plus d'informations sur l'ajout d'une logithèque à un nœud cible, veuillez consulter [Créer un référentiel DVM](#).
- Configurer une réplication autogérée. Pour plus d'informations sur la réplication d'un nœud cible autogéré, veuillez consulter [Réplication vers un core cible autogéré](#).
- Configurer une réplication tierce. Pour plus d'informations sur la réplication vers un nœud cible tiers, veuillez consulter [Réplication vers un Core cible tiers](#).
- Répliquer une machine protégée existante. Pour plus d'informations sur la réplication d'une machine déjà protégée par le nœud source, veuillez consulter [Ajouter une machine à une réplication existante](#).
- Consommer le disque de départ. Pour plus d'informations sur la consommation de données du disque de départ sur le nœud cible, veuillez consulter [Consommation du disque source sur un Core cible](#).
- Définir la priorité de la réplication pour une machine protégée. Pour plus d'informations sur la priorité de la réplication des machines protégées, veuillez consulter [Définir la priorité de réplication d'une machine protégée](#).
- Planifier une réplication pour une machine protégée. Pour plus d'informations sur la planification d'une réplication, veuillez consulter [Planifier la réplication](#).
- Surveiller la réplication en fonction des besoins. Pour plus d'informations sur la surveillance des répliqués, veuillez consulter [Affichage des répliqués entrants et sortants](#).
- Gérer les paramètres de la réplication en fonction des besoins. Pour plus d'informations sur la gestion des répliqués, veuillez consulter [Gestion des paramètres de réplication](#).
- Récupérer les données répliquées en cas d'incident ou de perte de données. Pour plus d'informations sur la récupération des données répliquées, veuillez consulter [Restaurer des données répliquées](#).

Réplication vers un Core cible tiers

Un Core tiers est un Core cible géré par un MSP (fournisseur d'infrastructure infogérée). La réplication sur un Core géré par un tiers ne nécessite pas l'accès au Core cible par le client.

Le processus de réplication vers un Core tiers implique des tâches qui doivent être effectuées par le client, ainsi que par le fournisseur tiers. Après la demande de réplication sur le ou les Cores source par le client, le MSP doit effectuer la configuration sur le Core cible en examinant la demande.

❗ REMARQUE : Cette configuration s'applique aux répliqués hébergés et Cloud. Le Core Rapid Recovery doit être installé sur toutes les machines du Core source. Si vous configurez Rapid Recovery pour une réplication multipoint à point, vous devez effectuer cette tâche sur tous les Cores source.

Pour répliquer sur un Core cible géré un fournisseur tiers, effectuez les tâches suivantes :

- Envoyer une demande de réplication à un fournisseur de service tiers
- Examiner une demande de réplication envoyée par un client
- Ignorer une demande de réplication envoyée par un client

Envoyer une demande de réplication à un fournisseur de service tiers

Si vous êtes un utilisateur final qui s'abonne à un core géré par un fournisseur tiers, tel qu'un MSP, suivez cette procédure pour envoyer une demande de réplication à votre fournisseur de service tiers.

- 1 Naviguez jusqu'au Core Rapid Recovery.
- 2 Depuis la barre des boutons d'icône, cliquez sur  **Répliquer**.
L'assistant de réplication s'affiche.
- 3 Sur la page **Core cible** de l'Assistant de réplication, cliquez sur **J'ai un abonnement auprès d'un tiers proposant des services de sauvegarde et de récupération après sinistre hors site** puis saisissez les informations, tel que décrit dans le tableau ci-dessous.

Tableau 135. Informations sur le core cible tiers

Zone de texte	Description
Nom de l'hôte	Entrez le nom de l'hôte, l'adresse IP ou le nom de domaine qualifié de la machine core tiers.
Port	Entrez le numéro de port qui vous a été fourni par votre fournisseur de services tiers. Le numéro de port par défaut est 8006.

- Si le core que vous voulez ajouter a déjà été couplé au core source, vous pouvez :
 - 1 Sélectionner **Utiliser un core cible existant**.
 - 2 Sélectionner le core cible dans la liste déroulante.
 - 3 Cliquez sur **Suivant**.
 - 4 Passez à l'étape 7.
- 4 Cliquez sur **Suivant**.
 - 5 Sur la page **Request (Requête)** de l'Assistant de réplication, entrez les informations tel que décrit dans le tableau suivant.

Tableau 136. Détails du core cible tiers

Zone de texte	Description
Adresse e-mail	Entrez l'adresse e-mail associée à votre abonnement au service tiers.
Identifiant client (facultatif)	De manière facultative, entrez l'identifiant client qui vous a été fourni par le fournisseur de service.

- 6 Cliquez sur **Suivant**.
- 7 Sur la page **Machines protégées** de l'Assistant de réplication, sélectionnez les machines protégées à répliquer sur le Core tiers.
- 8 Si vous voulez effectuer le processus d'implantation pour le transfert des données de base, suivez les étapes ci-dessous.

REMARQUE : compte tenu des volumes importants de données devant être copiés vers le périphérique de stockage amovible, une connexion eSATA, USB 3.0 ou toute autre connexion haut débit vers ce périphérique de stockage est recommandée.

- a Sur la page **Machines protégées**, sélectionnez **Utiliser un disque source pour effectuer le transfert initial**.
 - Si vous avez actuellement une ou plusieurs machines protégées répliquées vers un Core cible, vous pouvez inclure ces machines sur le disque source en choisissant l'option **Inclure les points de restauration déjà répliqués dans le disque source**.
- b Cliquez sur **Suivant**.
- c Sur la page **Emplacement du disque source** de l'Assistant de réplication, utilisez la liste déroulante **Type d'emplacement** pour choisir l'un des types de destination suivants :
 - Local

- Réseau
- Cloud

d Entrez les détails de l'archive comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape c.

Tableau 137. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive du disque source ; par exemple, D:\work\archive.
Réseau	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
		 REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud .
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.
	Nom du dossier	Entrez le nom du dossier d'enregistrement des données archivées. Le nom par défaut est Rapid-Recovery-Archive-[DATE DE CREATION]-[HEURE DE CREATION]

e Cliquez sur **Suivant**.

f Sur la page **Options du disque source**, entrez les informations comme décrit dans le tableau suivant.

Tableau 138. Options du disque source

Élément	Description
Taille maximale	Les archives de données de grande taille peuvent être divisées en plusieurs segments. Sélectionnez la quantité d'espace maximale à réserver pour la création du disque source en faisant l'une des choses suivantes : • Sélectionnez Cible entière pour réserver tout l'espace disponible dans le chemin d'accès fourni sur la page Emplacement du disque source (par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le disque D: est réservé). • Cliquez sur la zone de texte vierge, entrez une quantité, puis choisissez une unité de mesure dans la liste déroulante pour personnaliser l'espace maximal à réserver.
Action de recyclage	Si le chemin contient déjà un disque source, sélectionnez l'une des options suivantes : • Ne pas réutiliser. Ne remplace pas ou n'efface pas les données d'implantation existantes de l'emplacement. Si l'emplacement n'est pas vide, l'écriture du disque source échoue. • Remplacer ce Core. Remplace les données d'implantation existantes appartenant au core, mais laisse intactes les données des autres cores. • Effacer entièrement. Efface toutes les données d'implantation du répertoire avant une écriture du disque source.
Commentaire	Entrez un commentaire pour décrire le disque source.

Élément	Description
Ajouter tous les agents au disque source	Sélectionnez cette option pour répliquer toutes les machines protégées sur le core source en utilisant le disque source. Cette option est sélectionnée par défaut.
Construire des chaînes de points de restauration (réparer les orphelins)	Sélectionnez cette option pour répliquer la chaîne de points de restauration complète sur le disque source. Cette option est sélectionnée par défaut.
	REMARQUE : Une implantation type dans AppAssure 5.4 réplique uniquement le dernier point de restauration sur le disque source, ce qui réduit le temps et l'espace nécessaires à la création du disque source. Si vous choisissez de créer des chaînes de points de restauration sur le disque source, vous aurez besoin de suffisamment d'espace sur le disque source pour stocker les derniers points de restauration à partir de la ou des machines protégées spécifiées, et l'exécution de la tâche peut durer plus longtemps.

- g Effectuez l'une des opérations suivantes :
 - Si vous avez désélectionné la case **Ajouter tous les agents au disque source**, cliquez sur **Suivant**.
 - Si vous avez sélectionné **Ajouter tous les agents au disque source**, passez à l'étape 9.
- h Sur la page **Machines** de l'Assistant de réplication, sélectionnez les machines protégées à répliquer sur le Core cible en utilisant le disque source.
- 9 Cliquez sur **Terminer**.
- 10 Si vous créez un disque source, envoyez-le en suivant les instructions de votre fournisseur de service tiers.

Examine une demande de réplication envoyée par un client

Lorsqu'un utilisateur final a terminé la procédure [Envoyer une demande de réplication à un fournisseur de service tiers](#), une demande de réplication est envoyée du Core source au Core cible tiers. Si vous êtes le fournisseur tiers, vous pouvez examiner la demande, puis l'approuver afin de commencer la réplication pour votre client ou la refuser pour empêcher la réplication de se produire.

Choisissez parmi les options suivantes :

- [Approuver une demande de réplication](#)
- [Refuser une demande de réplication](#)

Approuver une demande de réplication

Suivez la procédure ci-dessous pour approuver une demande de réplication sur un core cible tiers.

- 1 Sur le Core cible, naviguez jusqu'à la console Core Rapid Recovery.
- 2 À partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 3 Sur la page **Réplication**, cliquez sur **Requête (#)**.
La section **Demandes de réplication en attente** s'affiche.
- 4 Sous Demandes de réplication en attente, cliquez sur le menu déroulant en regard de la demande à examiner, puis cliquez sur **Examiner**.
La fenêtre **Vérifier la demande de réplication** s'affiche.

REMARQUE : Les informations qui apparaissent dans la section **Identité du core source** de cette fenêtre sont fonction de la demande remplie par le client.

- 5 Dans **Identité du core source**, effectuez l'une des actions suivantes :
 - Sélectionnez **Remplacer un core répliqué existant**, puis sélectionnez un core à partir de la liste déroulante.

- Sélectionnez **Créer un Core source**, puis vérifiez que le nom du Core, l'adresse e-mail client et l'identifiant client qui ont été fournis sont corrects. Modifier les informations si nécessaire.
- 6 Sous Agents, sélectionnez les machines pour lesquelles l'approbation s'applique, puis utilisez les listes déroulantes dans la colonne Logithèque pour sélectionner la logithèque appropriée pour chacune des machines.
 - 7 Si vous le désirez, dans la zone de texte **Commentaire**, entrez une description ou un message à inclure dans la réponse qui sera envoyée au client.
 - 8 Cliquez sur **Envoyer la réponse**.
La réplication est acceptée.

Refuser une demande de réplication

Suivez la procédure ci-dessous pour refuser une demande de réplication envoyée à un core tiers par un client.

Pour refuser une demande sans l'examiner, voir [Ignorer une demande de réplication envoyée par un client](#).

- 1 Sur le Core cible, naviguez jusqu'à la console Core Rapid Recovery.
- 2 À partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 3 Sur la page **Réplication**, cliquez sur **Requête (#)**.
La section **Demandes de réplication en attente** s'affiche.
- 4 Sous Demandes de réplication en attente, cliquez sur le menu déroulant en regard de la demande à examiner, puis cliquez sur **Examiner**.
La fenêtre **Vérifier la demande de réplication** s'affiche.
- 5 Cliquez sur **Refuser**.
La réplication est refusée. La notification de refus apparaît dans la partie Alertes de l'onglet Événements du Core source.

Ignorer une demande de réplication envoyée par un client

En tant que fournisseur tiers d'un service de core cible, vous avez la possibilité d'ignorer une demande de réplication envoyée par un client. Cette option peut être utilisée si une demande a été envoyée par erreur ou que vous voulez refuser une demande sans même l'examiner.

Pour en savoir plus sur les demandes de réplication, voir [Examine une demande de réplication envoyée par un client](#).

Suivez la procédure ci-dessous pour ignorer une demande de réplication envoyée par un client.

- 1 Sur le Core cible, naviguez jusqu'à la console Core Rapid Recovery.
- 2 À partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 3 Sur la page **Réplication**, cliquez sur **Requête (#)**.
La section **Demandes de réplication en attente** s'affiche.
- 4 Sous Demandes de réplication en attente, cliquez sur le menu déroulant en regard de la demande à ignorer, puis cliquez sur **Ignorer**.
- 5 Dans la boîte de dialogue **Demande ignorée**, cliquez sur **Oui** pour confirmer la commande.
Une notification indiquant que la demande a été ignorée est envoyée au Core source, et la demande est supprimée de la page Réplication du Core cible.

Ajouter une machine à une réplication existante

Après l'établissement de la réplication entre des Cores source et cible, il est possible d'ajouter des machines protégées à répliquer sur la cible. Exécutez la procédure suivante sur le Core source pour ajouter une nouvelle machine protégée à un Core cible apparié pour la réplication.

Pour en savoir plus sur la réplication, voir [Réplication](#) et [Réplication vers un core cible autogéré](#).

- 1 Naviguez jusqu'à la console Core Rapid Recovery sur le Core source.
- 2 Dans la barre de boutons, cliquez sur  **Réplication**.
L'assistant de réplication s'ouvre sur la page **Machines protégées**.
- 3 Sur la page **Machines protégées**, sélectionnez les machines protégées à répliquer, puis utilisez les listes déroulantes dans la colonne Logithèque pour sélectionner une logithèque pour chacune des machines protégées.
- 4 Si vous voulez effectuer le processus d'implantation pour le transfert des données de base, suivez les étapes ci-dessous :

REMARQUE : compte tenu des volumes importants de données devant être copiés vers le périphérique de stockage amovible, une connexion eSATA, USB 3.0 ou toute autre connexion haut débit vers ce périphérique de stockage est recommandée.

- a Sur la page **Machines protégées**, sélectionnez **Utiliser un disque source pour effectuer le transfert initial**.
 - Si vous avez actuellement une ou plusieurs machines protégées répliquées vers un Core cible, vous pouvez inclure ces machines sur le disque source en choisissant l'option **Inclure les points de restauration déjà répliqués dans le disque source**.
- b Cliquez sur **Suivant**.
- c Sur la page **Emplacement du disque source** de l'assistant, utilisez la liste déroulante **Type d'emplacement** pour choisir l'un des types de destination suivants :
 - Local
 - Réseau
 - Cloud
- d Entrez les détails de l'archive comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape c.

Tableau 139. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, d:\work\archive.
Réseau	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud .		
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.

Option	Zone de texte	Description
	Nom du dossier	Entrez le nom du dossier d'enregistrement des données archivées. Le nom par défaut est Rapid-Recovery-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION]

e Cliquez sur **Suivant**.

f Sur la page **Options du disque source** de l'assistant, entrez les informations comme décrit dans le tableau suivant.

Tableau 140. Options du disque source

Élément	Description
Taille maximale	Les archives de données de grande taille peuvent être divisées en plusieurs segments. Sélectionnez la quantité d'espace maximale à réserver pour la création du disque source en faisant l'une des choses suivantes : • Sélectionnez Cible entière pour réserver tout l'espace disponible dans le chemin d'accès fourni sur la page Emplacement du disque source (par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le disque D: est réservé). • Cliquez sur la zone de texte vierge, entrez une quantité, puis choisissez une unité de mesure dans la liste déroulante pour personnaliser l'espace maximal à réserver.
Action de recyclage	Si le chemin contient déjà un disque source, sélectionnez l'une des options suivantes : • Ne pas réutiliser. Ne remplace pas ou n'efface pas les données d'implantation existantes de l'emplacement. Si l'emplacement n'est pas vide, l'écriture du disque source échoue. • Remplacer ce core. Remplace les données d'implantation existantes appartenant au core, mais laisse intactes les données des autres cores. • Effacer complètement. Efface toutes les données d'implantation du répertoire avant une écriture du disque source.
Commentaire	Entrez un commentaire pour décrire le disque source.
Ajouter tous les agents au disque source	Sélectionnez cette option pour répliquer toutes les machines protégées sur le core source en utilisant le disque source. Cette option est sélectionnée par défaut.
Créer des chaînes de point de restauration (réparer les orphelins)	Sélectionnez cette option pour répliquer la chaîne de points de restauration complète sur le disque source. Cette option est sélectionnée par défaut. REMARQUE : Une implantation type dans Rapid Recovery 5.4 réplique uniquement le dernier point de restauration sur le disque source, ce qui réduit le temps et l'espace nécessaires à la création du disque source. Si vous choisissez de créer des chaînes de points de restauration sur le disque source, vous aurez besoin de suffisamment d'espace sur le disque source pour stocker les derniers points de restauration à partir de la ou des machines protégées spécifiées, et l'exécution de la tâche peut durer plus longtemps.

g Effectuez l'une des opérations suivantes :

- Si vous avez désélectionné la case **Ajouter tous les agents au disque source**, cliquez sur **Suivant**.
- Si vous avez sélectionné **Ajouter tous les agents au disque source**, passez à l'étape 5.

h Sur la page **Machines protégées** de l'assistant, sélectionnez les machines protégées à répliquer sur le Core cible en utilisant le disque source.

5 Cliquez sur **Terminer**.

Consommation du disque source sur un Core cible

Suivez la procédure ci-dessous pour consommer les données du disque source sur le Core cible.

REMARQUE : Cette procédure est uniquement nécessaire si un disque source a été créé dans le cadre de **Réplication vers un core cible autogéré** ou **Réplication vers un Core cible tiers**.

- 1 Si le fichier du disque source a été enregistré sur un périphérique de stockage amovible, tel qu'un disque dur externe USB, connectez le disque au Core cible.
- 2 Sur le Core cible, ouvrez la Rapid Recovery Core Console et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 3 Sur la page **Réplication**, sous Réplication entrante, cliquez sur le menu déroulant pour sélectionner le Core source concerné, puis cliquez sur **Consommer**.
La boîte de dialogue **Consommer** s'affiche.
- 4 Dans le champ de texte **Type d'emplacement**, sélectionnez l'une des options suivantes dans la liste déroulante :
 - Local
 - Réseau
 - Cloud
- 5 Entrez les détails de l'archive du disque source comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape 4.

Tableau 141. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement	Entrez le chemin de l'archive.
Réseau	Emplacement	Entrez le chemin de l'archive.
	Nom d'utilisateur	Entrez le nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez le mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.
		REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud .
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.
	Nom du dossier	Entrez le nom du dossier dans lequel les données archivées sont enregistrées ; par exemple, Rapid-Recovery-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION]

- 6 Cliquez sur **Vérifier le fichier**.
Le Core recherche le fichier.

Une fois le fichier trouvé, les zones de texte suivantes s'affichent dans la fenêtre Consommer, renseignées avec les données collectées dans l'étape 4, l'étape 5 et le fichier. La plage de dates affiche les dates des points de restauration les plus anciens et les plus récents contenus dans le disque source. Tout commentaire saisi lors de la création du disque source est importé automatiquement.

- 7 Dans la boîte de dialogue **Consommer**, sous Agents, sélectionnez les machines à partir desquelles vous souhaitez consommer les données.
- 8 Cliquez sur **Consommer**.
- 9 Pour suivre l'avancement de la consommation des données, cliquez sur la page  Événements.

Abandonner un disque source

Si vous créez un disque source pour le consommer sur le Core cible, mais choisissez plus tard de ne pas le consommer, vous pouvez abandonner le disque source.

Tant que vous n'aurez pas abandonné ou consommé le disque source, un lien pour le disque source en attente demeure dans le volet Réplication sortante sur le Core source.

Tant que vous ne transmettez pas l'information du disque source, les points de restauration orphelins (qui existent sur la machine d'origine protégée, mais pas sur le Core cible) ne peuvent pas être utilisés pour restaurer les données.

⚠ PRÉCAUTION : Si vous abandonnez le disque source, les points de restauration d'origine (définis dans le fichier du disque source) seront ensuite transmis sur le réseau vers le Core cible au cours de la prochaine tâche de réplication. La transmission d'anciens points de restauration sur le réseau pourrait ralentir fortement le réseau, surtout s'il y a beaucoup de points de restauration.

Suivez les étapes de la procédure suivante pour abandonner un disque source en attente.

❗ REMARQUE : Abandonner le disque source dans la console Core n'affecte pas le fichier du disque source à son emplacement de stockage.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Sur la page **Réplication**, dans le volet Réplication sortante, cliquez sur **Disques sources (#)**.
Dans le volet Réplication sortante, une section s'affiche contenant des informations sur les disques source en attente.
- 3 Vous pouvez également cliquer sur la flèche vers le bas ▼ pour développer le menu déroulant.
Les informations sur les disques source en attente s'affichent, y compris le Core cible et la plage de dates des points de restauration inclus dans le disque source.
- 4 Cliquez sur  pour ouvrir le menu déroulant correspondant au disque source à abandonner, puis sélectionnez **Abandonner**.
- 5 Dans la fenêtre de confirmation, confirmez que vous voulez abandonner le disque source.
Le disque source est supprimé.

Si plus aucun disque source n'est présent dans le Core source, le lien Disques sources (#) et la section disques source en attente sont supprimés de l'onglet Réplication sortante.

Gestion des paramètres de réplication

Rapid Recovery vous permet de surveiller, de programmer et de modifier la réplication de manière globale, au niveau du Core ou de la machine protégée.

Vous pouvez modifier les paramètres de réplication suivants :

- Pour programmer des tâches de réplication, voir [Planifier la réplication](#).
- Pour créer le disque source d'une machine protégée déjà appariée pour la réplication, voir [Utiliser la fonction de copie pour créer un disque source](#).
- Pour surveiller l'avancement d'une tâche de réplication, voir [Affichage des réplications entrantes et sortantes](#).
- Pour suspendre ou reprendre une tâche de réplication suspendue, voir [Suspendre et reprendre la réplication](#).
- Pour forcer la réplication d'une machine protégée entrante ou sortante, voir [Forcer la réplication](#).
- Pour gérer les paramètres de tous les Cores cible et toutes les procédures de réplication, voir [Gestion des paramètres de réplication sortante](#).
- Pour gérer les paramètres d'un Core cible, voir [Modification des paramètres du Core cible](#).

- Pour gérer les paramètres de priorité d'une machine protégée en cours de réplication sur un Core cible, voir [Définir la priorité de réplication d'une machine protégée](#).

Planifier la réplication

À moins que vous ne changiez le comportement par défaut en définissant une planification de réplication, le Core démarre une tâche de réplication immédiatement après avoir terminé : chaque instantané de sauvegarde, vérification de somme de contrôle, vérification de capacité d'attachement, et les tâches nocturnes. Pour plus d'informations, voir [Planifier la réplication](#).

Vous pouvez modifier la planification de réplication pour réduire la charge sur le réseau.

Suivez les étapes de la procédure qui suit pour définir une planification de réplication pour toute machine répliquée.

- 1 Sur le Core cible, ouvrez la console Core Rapid Recovery et à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Dans le volet de réplication sortante, cliquez sur  pour ouvrir le menu déroulant en regard du Core pour lequel vous souhaitez programmer la réplication, puis cliquez sur **Planifier**.
Le **Planning de réplication de [nom du Core]** s'ouvre.
- 3 Sélectionnez l'une des trois options suivantes :
 - **En permanence.** La réplication s'effectue après chaque nouvelle capture d'instantané, vérification de la somme de contrôle, vérification de la capacité d'attachement, et après la fin de toutes les tâches nocturnes.
 - **Tous les jours (Démarrer la réplication uniquement lors de la période spécifiée).** Commence la réplication uniquement pendant la plage horaire indiquée.
 - 1 Dans la zone de texte **De**, entrez l'heure le plus tôt auquel vous voulez que la réplication commence.
 - 2 Dans la zone de texte **À**, entrez l'heure le plus tardif auquel vous voulez que la réplication commence.

 **REMARQUE :** Si la réplication est en cours lorsque l'heure programmé se termine, la tâche de réplication se termine après la période prévue.
 - **Personnalisé.** Démarre la réplication uniquement durant la plage horaire fournie. Vous pouvez définir une plage horaire pour les jours de la semaine et une autre pour les week-ends.
 - 1 En regard de Jours de semaine, dans la zone de texte **De**, entrez l'heure le plus tôt auquel vous voulez que la réplication se produise pendant un jour de semaine ; puis dans la zone de texte **À**, entrez l'heure le plus tardif auquel vous voulez que la réplication se produise pendant un jour de semaine.
 - 2 En regard de Week-end, dans la zone de texte **De**, entrez l'heure le plus tôt auquel vous voulez que la réplication se produise pendant le week-end ; puis dans la zone de texte **À**, entrez l'heure le plus tardif auquel vous voulez que la réplication se produise pendant le week-end.
- 4 Cliquez sur **Enregistrer**.
Les horaires s'appliquent à toute réplication sur le Core cible sélectionné.

Utiliser la fonction de copie pour créer un disque source

Si vous aviez choisi de ne pas créer de disque source lors de la configuration de la réplication, vous pouvez créer un disque source en utilisant la fonction de copie dans le menu déroulant des machines protégées.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Sur la page **Réplication**, dans le volet Réplication sortante, cliquez sur ▼ Pour développer le Core qui protège la machine pour laquelle vous souhaitez créer un disque source.
La sélection se développe pour afficher chaque machine protégée dans le Core spécifié.
- 3 Cliquez dans la ligne du tableau pour sélectionner chaque machine pour laquelle vous souhaitez créer un disque source.
- 4 Dans le menu sous le volet Réplication sortante, cliquez sur **Copier**.

L'Assistant de réplication apparaît.

- 5 Sur la page **Emplacement du disque source**, utilisez la liste déroulante **Emplacement** pour choisir un des types de destination suivants :
 - Local
 - Réseau
 - Cloud
- 6 Entrez les détails de l'archive du disque source comme l'indique le tableau suivant, selon le type d'emplacement choisi lors de l'étape précédente.

Tableau 142. Détails de l'archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, d:\work\archive.
Réseau	Emplacement de sortie	Entrez l'emplacement de la sortie. Permet de définir le chemin de l'emplacement de l'archive ; par exemple, \\servername\sharename.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Permet de définir les données de référence de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe du chemin d'accès réseau. Permet de définir les données de référence de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante.  REMARQUE : Pour sélectionner un compte Cloud, vous devez l'ajouter préalablement dans Core Console. Pour plus d'informations, voir Ajouter un compte cloud.
	Conteneur	Sélectionnez un conteneur associé au compte dans le menu déroulant.
	Nom du dossier	Entrez le nom du dossier d'enregistrement des données archivées. Le nom par défaut est Rapid-Recovery-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION]

- 7 Cliquez sur **Suivant**.
- 8 Sur la page Options du disque source, entrez les informations comme décrit dans le tableau suivant.

Tableau 143. Options du disque source

Élément	Description
Taille maximale	Les archives de données de grande taille peuvent être divisées en plusieurs segments. Sélectionnez la quantité d'espace maximale à réserver pour la création du disque source en faisant l'une des choses suivantes : • Sélectionnez Cible entière pour réserver tout l'espace disponible dans le chemin d'accès fourni sur la page Emplacement du disque source (par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le disque D: est réservé). • Cliquez sur la zone de texte vierge, entrez une quantité, puis choisissez une unité de mesure dans la liste déroulante pour personnaliser l'espace maximal à réserver.
Action de recyclage	Si le chemin contient déjà un disque source, sélectionnez l'une des options suivantes : • Ne pas réutiliser. Ne remplace pas ou n'efface pas les données d'implantation existantes de l'emplacement. Si l'emplacement n'est pas vide, l'écriture du disque source échoue. • Remplacer ce Core. Remplace les données d'implantation existantes appartenant au core, mais laisse intactes les données des autres cores. • Effacer entièrement. Efface toutes les données d'implantation du répertoire avant une écriture du disque source.
Commentaire	Entrez un commentaire pour décrire le disque source.

Élément	Description
Ajouter tous les agents au disque source	Sélectionnez cette option pour répliquer toutes les machines protégées sur le core source en utilisant le disque source. Cette option est sélectionnée par défaut.
Créer des chaînes de point de restauration (réparer les orphelins)	Sélectionnez cette option pour répliquer la chaîne de points de restauration complète sur le disque source. Cette option est sélectionnée par défaut.
	REMARQUE : Une implantation type dans Rapid Recovery 5.4 x répliquait uniquement le dernier point de restauration sur le disque source, ce qui réduit le temps et l'espace nécessaires à la création du disque source. Si vous choisissez de créer des chaînes de points de restauration sur le disque source, vous aurez besoin de suffisamment d'espace sur le disque source pour stocker les derniers points de restauration à partir des machines protégées spécifiées, et l'exécution de la tâche peut durer plus longtemps.

- 9
- Effectuez l'une des opérations suivantes :
- Si vous avez désélectionné la case **Ajouter tous les agents au disque source**, cliquez sur **Suivant**.
 - Si vous avez sélectionné **Ajouter tous les agents au disque source**, passez à [l'étape 10](#).
- 10
- Sur la page **Machines protégées** de l'assistant, sélectionnez les machines protégées pour lesquelles vous souhaitez créer un disque source.
- 11
- Cliquez sur **Terminer**.

Surveiller la réplication

Lorsqu'une réplication est configurée, vous pouvez surveiller l'état des tâches de réplication des Cores source et cible. Vous pouvez actualiser les informations sur l'état, afficher les détails de la réplication et plus encore.

- 1
- Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication). La page **Réplication** s'affiche.
- 2
- Sur cette page, vous pouvez afficher les informations sur les tâches de réplication et surveiller leur état, comme décrit dans le tableau suivant.

Tableau 144. Tâches de réplication

Section	Description	Actions disponibles
Disques sources (#)	Une fois que vous avez spécifié l'utilisation d'un disque source lors de la définition de la réplication, tant que vous ne l'aurez pas abandonné ou consommé, un lien de Disques source (#) apparaît dans le volet de réplication sortante sur le Core source. Le nombre affiché indique combien de disques source sont en attente. REMARQUE : Ce lien ne s'affiche pas, sauf si un disque source est en attente. Cliquez sur ce lien pour afficher tous les disques source sur lesquels le Core cible a écrit, mais qui ne sont pas encore consommés. Développez à nouveau le menu déroulant pour afficher des informations sur les disques sources en attente, y	Dans le menu déroulant, cliquez sur Abandonner pour abandonner ou annuler le processus d'implantation. Menu wn

Section	Description	Actions disponibles
	compris le Core cible et la plage de dates des points de restauration inclus dans le disque source.	
Réplication sortante	Répertorie tous les Cores cible vers lesquels le Core source est en cours de réplication. Sont affichés un indicateur d'état, le nom du Core cible, le nombre de machines en cours de réplication, ainsi que l'état d'avancement de la transmission d'une réplication.	Sur un Core source, dans le menu déroulant , vous pouvez sélectionner les options suivantes : • Détails : répertorie l'ID, l'URL, le nom d'affichage, l'état, l'ID de client, l'adresse e-mail et les commentaires définis pour le Core répliqué. • Modifier les paramètres. Répertorie le nom d'affichage et permet de modifier l'hôte et le port du Core cible. • Programmer. Permet de définir des horaires personnalisés pour la réplication sur ce Core cible. • Ajouter des machines Permet de choisir un hôte dans une liste déroulante, de sélectionner des machines protégées répliquées pour la réplication et de créer un disque source pour le transfert initial de la nouvelle machine protégée. Si vous le souhaitez, vous pouvez choisir d'inclure des points de restauration pour les machines déjà ajoutées à la réplication. • Supprimer. Vous permet de supprimer la relation de réplication entre Cores source et cible. En effectuant cette opération, vous arrêtez toute réplication sur ce Core.
Réplication entrante	Répertorie toutes les machines source depuis lesquelles la cible reçoit les données répliquées. Sont affichés le nom du Core distant, son état, les machines et l'état d'avancement. Répertorie tous les Cores source depuis lesquelles la cible reçoit les données répliquées. Les noms d'affichage pour les Cores source répertoriés sont créés à partir de la valeur dans l'Assistant de réplication lorsque vous définissez la réplication. Sont affichés un indicateur d'état, le nom du Core distant, et l'avancement d'une transmission de réplication.	Sur le Core cible, dans le menu déroulant , vous pouvez sélectionner les options suivantes : • Détails. Répertorie l'identifiant, le nom d'hôte, l'identifiant client, l'adresse e-mail et les commentaires du Core répliqué. • Consommer. Consomme les données initiales depuis le disque source, puis les enregistre dans la logithèque locale. • Supprimer. Vous permet de supprimer la relation de réplication entre le Core cible et source. En effectuant cette opération, vous arrêtez toute réplication à partir de ce Core.
Demandes de réplication en attente	Cette information s'applique uniquement aux fournisseurs de services infogérés. Lorsqu'un client clique sur le lien Demandes du volet de réplication entrante, un tableau récapitulatif s'affiche avec ID de clients, adresse e-mail et nom d'hôte de la requête.	Dans le menu déroulant, cliquez sur Ignorer pour ignorer ou rejeter la demande, ou Révision pour passer en revue la requête en attente.

Suspendre et reprendre la réplication

Vous pouvez suspendre une réplication de façon temporaire pour les Cores source (sortant) ou cible (entrant).

L'option pour suspendre la réplication est disponible uniquement lorsque la réplication est active. L'option pour reprendre la réplication est disponible uniquement lorsque la réplication est suspendue.

Pour suspendre ou reprendre une réplication, procédez comme suit.

- 1 Ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Pour suspendre la réplication pour toutes les machines répliquées, effectuez les opérations suivantes :
 - a Cliquez sur la case à cocher dans la partie supérieure du tableau récapitulatif pour sélectionner le Core source ou cible.
 - b Cliquez sur **Pause** dans le menu au-dessus du tableau récapitulatif.
La réplication de toutes les machines protégées dans le Core sélectionné est suspendue.
- 3 Pour suspendre la réplication de certaines machines, effectuez les opérations suivantes :
 - a Cliquez sur la flèche ▼ à droite de n'importe quel Core.
L'affichage s'agrandit pour faire apparaître toutes les machines protégées à partir du Core sélectionné qui sont en cours de réplication.
 - b Cliquez dans la première colonne pour sélectionner chaque machine pour lesquelles vous souhaitez suspendre la réplication. Cliquez sur n'importe quelle sélection à nouveau pour décocher une machine que vous ne souhaitez pas suspendre.
 - c Cliquez sur **Pause** dans le menu au-dessus du tableau récapitulatif.
La réplication des machines protégées sélectionnées est suspendue.
- 4 Pour reprendre la réplication de toutes les machines répliquées, effectuez les opérations suivantes :
 - a Cliquez sur la case à cocher dans la partie supérieure du tableau récapitulatif pour sélectionner le Core source ou cible.
 - b Cliquez sur **Reprendre** dans le menu situé au-dessus du tableau récapitulatif.
La réplication de toutes les machines protégées du Core sélectionné reprend.
- 5 Pour reprendre la réplication de certaines machines uniquement, effectuez les opérations suivantes :
 - a Cliquez sur la flèche ▼ à droite de n'importe quel Core.
L'affichage s'agrandit pour faire apparaître toutes les machines protégées à partir du Core sélectionné qui sont en cours de réplication.
 - b Cliquez dans la première colonne pour sélectionner chaque machine pour lesquelles vous souhaitez reprendre la réplication. Cliquez sur n'importe quelle sélection à nouveau pour décocher une machine que vous ne souhaitez pas reprendre.
 - c Cliquez sur **Reprendre** dans le menu situé au-dessus du tableau récapitulatif.
La réplication des machines protégées sélectionnées reprend.

Forcer la réplication

Depuis le Core source, vous pouvez forcer la réplication à n'importe quel moment, au lieu d'attendre le tour d'une tâche de réplication dans la file d'attente après un événement spécifique, comme une sauvegarde ou une vérification de capacité d'attachement.

Suivez cette procédure pour forcer la réplication sur le Core source ou cible.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Effectuez l'une des opérations suivantes :
 - Pour forcer la réplication sur un Core source, à partir du volet **Réplication sortante**, sélectionnez un Core et, dans le menu situé au-dessus du tableau Synthèse, cliquez sur  **Forcer**.
 - Pour forcer la réplication sur un Core cible, à partir du volet **Réplication entrante**, sélectionnez un Core et, dans le menu situé au-dessus du tableau Synthèse, cliquez sur  **Forcer**.
La boîte de dialogue Forcer la réplication s'affiche.
- 3 Facultatif : si vous souhaitez réparer les éventuelles chaînes de points de restauration orphelines, sélectionnez **Restaurer les chaînes de points de restauration orphelines**.
- 4 Pour confirmer, cliquez sur **Oui** dans la boîte de dialogue Forcer la réplication.
La boîte de dialogue se ferme et la réplication est forcée.

Gestion des paramètres de réplication sortante

Les changements apportés à ces paramètres affectent le transfert des données vers tous les Cores cibles associés au Core source.

- 1 Ouvrez la console Core de Rapid Recovery sur le Core source puis, dans la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Dans le volet **Réplication sortante**, dans la partie supérieure du tableau récapitulatif, cliquez sur  (Paramètres).
La boîte de dialogue **Paramètres de réplication** s'affiche.
- 3 Dans la boîte de dialogue **Paramètres de réplication**, modifiez les paramètres de réplication comme indiqué dans le tableau suivant.

Tableau 145. Paramètres de réplication

Option	Description
Durée de vie du cache (secondes)	Indiquez un délai entre chaque demande d'état du Core cible effectuée par le Core source.
Expiration du délai d'attente de la session d'image de volume (minutes)	Indiquez le délai pendant lequel le Core source tente de transférer une image de volume vers le Core cible.
Nombre max. de flux parallèles	Indiquez le nombre de connexions réseau pouvant être utilisées simultanément par une seule machine protégée pour répliquer les données de cette machine.
Vitesse de transfert max. (Mb/s)	Spécifiez la limite de la vitesse de transfert des données répliquées.
Taille maximale du transfert de données (Go)	Indiquez la taille maximale en Go du transfert de blocs de données répliquées.
Restaurer les valeurs par défaut	Sélectionnez cette option pour rétablir les valeurs par défaut des paramètres de réplication.

 **REMARQUE : vérifiez si vous disposez de réglages personnalisés avant de sélectionner cette option. Vous ne serez pas invité à confirmer cette action**

- 4 Une fois la sélection effectuée, cliquez sur **Enregistrer** pour enregistrer les paramètres de réplication et fermer la boîte de dialogue.

Modification des paramètres du Core cible

Vous pouvez modifier les paramètres de l'hôte et du port de chaque Core cible depuis le Core source.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.

Dans le volet **Réplication sortante**, le tableau récapitulatif contient une ligne pour chaque Core cible qui a été configuré pour répliquer des points de restauration depuis ce Core source.
- 2 Cliquez sur  (Paramètres) dans le menu déroulant pour le Core cible que vous souhaitez modifier, puis sélectionnez **Modifier les paramètres**.
La boîte de dialogue **Paramètres** s'affiche.
- 3 Vous pouvez modifier toutes les options décrites dans le tableau suivant.

Tableau 146. Paramètres du Core cible

Option	Description
Hôte	Entrez l'hôte du Core cible.
Port	Entrez un port que le Core cible utilisera pour communiquer avec le Core source.

 **REMARQUE :** Le port par défaut est 8006.

- 4 Cliquez sur **Enregistrer**.

Définir la priorité de réplication d'une machine protégée

La priorité de réplication détermine quelles sont les tâches de réplication envoyées en premier au Core. La priorisation est définie par ordre sur une échelle de 1 à 10, 1 correspondant au niveau de priorité le plus élevé, et 10 au niveau le plus bas. Lorsque vous établissez la réplication initiale d'une machine, sa priorité est définie sur 5. Vous pouvez afficher et modifier la priorité au niveau de la machine protégée, à partir du Core source.

Il peut arriver que certaines tâches de réplication soient abandonnées. Par exemple, des tâches de réplication peuvent être abandonnées si votre environnement rencontre des taux de changement anormalement élevés ou que la bande passante de votre réseau est insuffisante. Cette situation est particulièrement probable si vous définissez des planifications limitant les heures d'exécution de la réplication dans votre environnement. Pour en savoir plus sur le réglage des planifications de réplication, voir [Planifier la réplication](#).

Pour s'assurer que la réplication commence par les machines les plus importantes, définissez la priorité des serveurs critiques sur un petit nombre (compris entre 1 et 5). Définissez la priorité des machines moins importantes sur un nombre plus élevé (compris entre 6 et 10).

Le fait de définir sur 4 la priorité de réplication de toutes les machines protégées leur permet d'être répliquées avant les machines pour lesquelles la priorité de réplication par défaut (à savoir 5) est définie. Les tâches de réplication des machines présentant une priorité de 3 sont mises en file d'attente avant celles présentant une priorité de 4, et ainsi de suite. Plus le numéro de priorité est petit, plus les tâches de réplication sont exécutées rapidement. Il est très simple de se souvenir que la priorité 1 est la plus importante. Les machines présentant une priorité de réplication de 1 sont placées en tête de la file d'attente de réplication.

Suivez les étapes ci-dessous pour modifier les paramètres qui définissent la priorité de réplication des machines protégées.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche.
- 2 Dans le volet **Réplication sortante**, cliquez sur la flèche ▼ à droite de n'importe quel Core source.
L'affichage s'agrandit pour afficher toutes les machines protégées depuis ce Core source qui sont en train d'être répliquées vers le Core cible désigné.
- 3 Cliquez sur le menu déroulant  (Paramètres) de la machine protégée à rendre prioritaire, puis cliquez sur **Paramètres**.
Une boîte de dialogue s'affiche.
- 4 Cliquez sur la liste déroulante **Priorité** et sélectionnez un niveau de priorité, compris entre **1 (maximum)** et **10 (minimum)**, selon vos besoins.
- 5 Cliquez sur **Enregistrer**.
La boîte de dialogue se ferme et la priorité de réplication de la machine sélectionnée est mise à jour.

Suppression d'une réplication

La réplication est la duplication intentionnelle de points de restauration pour une machine protégée depuis un Core Rapid Recovery (le Core source) vers un second cœur (la cible).

L'objectif de la réplication est de maintenir un double des données d'origine toujours accessible pour la machine protégée. Pour optimiser la sécurité des données, Dell recommande de placer le Core cible à un emplacement géographique différent de celui du Core source.

À moins que vous ne changiez le comportement par défaut en définissant une planification de réplication, le Core démarre une tâche de réplication immédiatement après avoir terminé : chaque instantané de sauvegarde, vérification de somme de contrôle, vérification de capacité d'attachement, et les tâches nocturnes. Pour plus d'informations, voir [Planifier la réplication](#).

Lorsque vous retirez une réplication, vous interrompez les futures copies de points de restauration du Core source vers le Core cible. Retirer la réplication n'affecte jamais les données enregistrées sur le Core source original.

De plus, lorsque vous retirez une réplication, vous avez la possibilité de laisser ou de supprimer les points de restauration répliqués à partir de la machine d'origine sur votre Core cible. Si vous conservez les points de restauration d'une machine répliquée que vous supprimez, les points de restauration de cette machine sont alors représentés dans le Core en tant que machine comportant uniquement des points de restauration. Vous pouvez naviguer dans les données de ces points de restauration conservés, ou restaurer des fichiers au niveau fichier, alors qu'ils sont conservés sur le Core cible.

Vous pouvez retirer la réplication des périphériques de l'une des manières suivantes :

- [Suppression d'une réplication sortante depuis le Core source](#)
- [Retirer une réplication entrante du Core cible](#)

Suppression d'une réplication sortante depuis le Core source

Suivez cette procédure pour retirer une ou plusieurs machine(s) protégée(s) de la réplication sur le Core source.

- 1 Sur le Core source, ouvrez la console Core Rapid Recovery et, à partir de la barre d'icônes, cliquez sur  (Réplication). La page **Réplication** s'affiche.

Dans le volet **Réplication sortante**, le tableau récapitulatif contient une ligne pour chaque Core cible qui a été configuré pour répliquer des points de restauration depuis ce Core source.

2 Vous pouvez également cliquer sur la flèche ▼ à droite de n'importe quel Core cible. L'affichage s'agrandit pour afficher toutes les machines protégées depuis ce Core source qui sont en train d'être répliquées vers le Core cible désigné.

3 Sélectionnez les machines protégées que vous souhaitez retirer de la réplication sortante comme suit :
 - Pour retirer complètement la relation de réplication existante entre ce Core source et n'importe quel Core cible, cliquez sur le menu déroulant  (Paramètres) pour n'importe quel Core cible, puis sélectionnez **Supprimer**.
 - Pour retirer la réplication sortante d'un sous-ensemble de machines du Core cible sélectionné, développez l'affichage pour afficher toutes les machines en cours de réplication et cochez la case correspondant à chaque machine répliquée que vous souhaitez retirer. Désélectionnez toutes les machines pour lesquelles vous souhaitez poursuivre la réplication. Puis, à partir du menu situé au-dessus du tableau récapitulatif, cliquez sur  **Supprimer**.

Un message de confirmation s'affiche et vous demande si vous souhaitez retirer les relations de réplication.
4 Dans la boîte de dialogue qui s'affiche, cliquez sur **Oui** pour confirmer la suppression.

Retirer une réplication entrante du Core cible

Suivez cette procédure pour retirer une machine protégée de la réplication sur le Core cible.

REMARQUE : Vous pouvez également supprimer une réplication d'une machine protégée depuis le volet de réplication sortante sur la page de réplication du Core source. Pour plus d'informations, voir [Suppression d'une réplication sortante depuis le Core source](#)

- 1 Sur le Core cible, ouvrez la console Core Rapid Recovery et à partir de la barre d'icônes, cliquez sur  (Réplication).
La page **Réplication** s'affiche. Dans le volet Réplication entrante, le tableau de synthèse contient une ligne pour chaque Core source ayant des machines protégées que ce Core cible réplique.
- 2 Sélectionnez les machines répliquées à retirer, comme suit :
 - Pour supprimer **toutes** les machines répliquées à partir du Core source vers le Core cible, dans le volet de réplication entrante, cochez la case de ce Core.
 - Pour supprimer un sous-ensemble plus restreint de machines d'un même Core source, effectuez les opérations suivantes :
 - a Cliquez sur la flèche ▼ à droite du Core source.
L'affichage s'agrandit pour afficher toutes les machines du Core source sélectionné qui sont répliquées sur votre Core cible.
 - b Cochez la case de chaque machine répliquée que vous souhaitez retirer.
 - c À partir de la ligne parent de la source sélectionnée, cliquez sur le menu déroulant  (Paramètres), puis sélectionnez **Supprimer**.
La boîte de dialogue **Retirer la réplication** s'affiche.
- 3 Dans la boîte de dialogue **Retirer la réplication**, procédez comme suit :
 - Si vous souhaitez laisser les points de restauration répliqués sur le Core cible, décochez l'option **Supprimer les points de restauration existants**.
 - Si vous souhaitez supprimer tous les points de restauration répliqués de cette machine, ainsi que la réplication du Core source, sélectionnez **Supprimer les points de restauration existants**.
- 4 Cliquez sur **Oui** pour confirmer la suppression.

AVERTISSEMENT : Si vous sélectionnez cette option, tous les points de restauration répliqués vers ce Core seront supprimés.

Les machines protégées sélectionnées sur le Core source seront supprimées de la réplication vers ce Core cible. Facultatif : si vous avez sélectionné l'option pour supprimer des points de restauration, ils sont supprimés de la logithèque de ce Core.

Restaurer des données répliquées

La fonctionnalité de réplication « quotidienne » est assurée sur le Core source, tandis que seul le Core cible est capable d'accomplir les fonctions nécessaires à une restauration après sinistre.

En cas de restauration après sinistre, le Core cible peut utiliser les points de restauration répliqués pour restaurer les machines protégées et le Core. Vous pouvez effectuer les options de restauration suivantes depuis le Core cible :

- **Monter des points de restauration.** Pour plus d'informations, voir [Monter un point de restauration](#).
- **Restaurer vers les points de restauration.** Pour plus d'informations, voir [À propos de la restauration de volumes à partir d'un point de restauration](#) ou [Restaurer les volumes d'une machine Linux à l'aide de la ligne de commande](#).
- **Effectuer l'exportation d'une machine virtuelle (VM).** Pour plus d'informations, voir [À propos de l'exportation vers des machines virtuelles avec Rapid Recovery](#).
- **Effectuer une restauration BMR.** Pour plus d'informations, voir [Exécution d'une restauration complète sur des machines Windows](#).

Restauration de données

Gestion de la récupération

Le Noyau de la Récupération rapide peut restaurer des données instantanément ou récupérer des machines sur des machines virtuelles ou physiques, à partir de points de récupération. Ces points de récupération contiennent des instantanés des volumes agents, capturés au niveau des blocs. Ces instantanés prennent en compte les applications, c'est-à-dire que toutes les transactions en cours et les journaux des transactions s'accumulant sont complétés, et les caches envoyés au disque, avant de créer l'instantané. Utiliser des instantanés prenant en compte les applications conjointement à une Récupération vérifiée permet au Noyau d'effectuer plusieurs types de récupération, dont :

- Récupération de fichiers et de dossiers
- Récupération de volumes de données à l'aide de la Récupération en direct
- Récupération de volumes de données pour Microsoft Exchange Server et Microsoft SQL Server à l'aide de la Récupération en direct
- Restauration complète à l'aide de la Récupération universelle
- Restauration complète sur un matériel différent à l'aide de la Récupération universelle
- Exportation ad-hoc et exportation continue sur des machines virtuelles

Instantanés et points de restauration

Cette section explique comment utiliser et gérer les instantanés et les points de restauration générés par Rapid Recovery. Elle fournit des informations sur le montage, l'affichage et le forçage, ainsi que la migration et la suppression des points de restauration.

Gérer les instantanés et les points de restauration

Un point de restauration est une collection d'instantanés des volumes de disque individuels, stockés dans la logithèque. Les instantanés capturent et stockent l'état d'un volume de disque à un moment donné dans le temps pendant que les applications qui génèrent les données continuent d'être utilisées. Dans Rapid Recovery, vous pouvez forcer un instantané, suspendre temporairement les instantanés et afficher les listes des points de restauration actifs de la logithèque, et les supprimer, si nécessaire. Les points de restauration servent à restaurer les machines protégées ou à effectuer un montage dans un système de fichiers local.

Les instantanés sont créés par Rapid Recovery au niveau des blocs et tiennent compte de l'état et du fonctionnement des applications. Cela implique que toutes les transactions en cours et les journaux de transactions enchaînés sont terminés et que les caches sont vidés sur disque avant la création de l'instantané.

Rapid Recovery utilise un pilote de filtre de volume de bas niveau qui s'attache aux volumes montés, puis suit toutes les modifications au niveau du bloc du prochain instantané. Microsoft VSS (Volume Shadow Services) facilite la création d'instantanés cohérents lors du blocage des applications.

Affichage de la page des points de restauration d'une machine protégée

Suivez les étapes de la procédure suivante pour afficher la liste complète des points de restauration d'une machine protégée.

REMARQUE : Si vous protégez les données depuis un serveur de cluster DAG ou un CCR, les points de restauration associés ne s'afficheront pas au niveau du cluster. Ils sont visibles uniquement au niveau du nœud ou de la machine.

- 1 Dans la Rapid Recovery Core Console, accédez à la machine protégée dont vous souhaitez afficher les points de restauration.
- 2 Dans le menu situé en haut de la page, cliquez sur **Points de restauration**.
La page Points de restauration s'affiche. Elle comporte un volet Résumé des points de restauration et un volet Points de restauration.

Vous pouvez afficher les informations récapitulatives sur les points de restauration de la machine, tel que décrit dans le tableau suivant.

Tableau 147. Informations récapitulatives sur les points de restauration

Infos	Description
Total des points de restauration	Indique le nombre total de points de restauration enregistrés dans la logithèque de cette machine.
Données totales protégées	Indique la quantité d'espace de stockage utilisée dans la logithèque pour ces points de restauration.
Logithèque DVM	Indique le nom de la logithèque dans laquelle ces points de restauration sont stockés.
Statut de la logithèque DVM	Affiche sous forme de graphique la quantité d'espace consommé par les points de restauration. Indique le pourcentage d'espace utilisé dans la logithèque, la quantité d'espace et l'espace total de la logithèque. Cliquez sur le graphique pour afficher la quantité d'espace restant.

Vous pouvez afficher les informations sur les points de restauration de la machine, tel que décrit dans le tableau suivant.

Tableau 148. Informations sur les points de restauration

Infos	Description
Icône	Représentation graphique d'un point de restauration  ou, si développé, d'un volume avec le point de restauration  . Les points de restauration présentent une flèche droite  permettant de développer les informations.
Chiffré	Indique si le point de restauration est chiffré.
État	Indique l'état actuel du point de restauration.
Contenu	Répertorie les volumes inclus dans le point de restauration. Cliquez sur  (Informations) pour afficher l'utilisation de l'espace et le système de fichiers.
Type	Définit un point de restauration comme image de base ou instantané incrémentiel (différentiel).
Date de création	Affiche la date de création du point de restauration.
Taille	Affiche la quantité d'espace que le point de restauration consomme dans la logithèque.
	Le menu déroulant Paramètres permet d'exécuter certaines fonctions pour le point de restauration sélectionné.

- 3 Si vous le souhaitez, vous pouvez développer un point de restauration pour afficher les volumes protégés.

Liens connexes

[Affichage des points de restauration d'une machine](#)

Comprendre les indicateurs d'état des points de restauration

Lorsqu'un point de restauration est créé pour un serveur Exchange ou SQL protégé, l'application affiche un indicateur d'état correspondant dans la grille des points de restauration. La grille apparaît dans le volet **Points de restauration** pendant l'affichage des points de restauration d'une machine spécifique. La couleur qui s'affiche se base sur les paramètres de vérification de la machine protégée et sur la réussite ou l'échec de ces vérifications, comme indiqué dans les tableaux suivants.

REMARQUE : pour en savoir plus sur l'affichage des points de restauration, voir [Affichage de la page des points de restauration d'une machine protégée](#).

Couleurs d'état des points de restauration des bases de données Exchange

Le tableau suivant répertorie les indicateurs de statut qui s'affichent pour les bases de données Exchange.

Tableau 149. Indicateurs d'état des bases de données Exchange

Couleur d'état	Description
Blanc	Indique qu'aucune base de données Exchange n'est détectée dans le point de restauration, volume ou groupe de volumes.
Jaune	Indique que les vérifications de montabilité de la base de données Exchange n'ont pas encore été exécutées.
Rouge	Indique que les vérifications de montabilité ou les vérifications de la somme de contrôle ont échoué au moins sur une base de données.
Vert	Indique que le point de restauration contient une ou plusieurs bases de données, que les vérifications de montabilité sont activées, et que la vérification de montabilité ou la vérification de somme de contrôle a réussi.

Couleurs des états des points de restauration des bases de données SQL

Le tableau suivant répertorie les indicateurs d'état qui s'affichent pour les bases de données SQL.

Tableau 150. Indicateurs d'état des bases de données SQL

Couleur d'état	Description
Blanc	Indique qu'aucune base de données SQL n'est détectée dans le point de restauration, volume ou groupe de volumes.
Jaune	La base de données SQL étant hors ligne, les vérifications de la capacité d'attachement n'ont pas pu être effectuées.
Rouge	Indique que la vérification de la capacité d'attachement a échoué, ou que la base de données SQL est hors ligne.
Vert	Indique que la vérification de la capacité d'attachement a été exécutée correctement.

REMARQUE : les points de restauration n'étant pas associés à une base de données Exchange ou SQL auront un indicateur d'état blanc. Si les bases de données Exchange et SQL existent toutes les deux dans le point de restauration, l'indicateur de statut le plus grave s'affiche pour le point de restauration.

Monter un point de restauration

Dans Rapid Recovery, vous pouvez monter un point de restauration pour une machine Windows afin d'accéder aux données stockées via un système de fichiers local.

① **REMARQUE :** pour monter un point de restauration Linux avec l'utilitaire `local_mount`, voir [Monter un volume d'un point de restauration sur une machine Linux](#).

① **REMARQUE :** lorsque vous montez des points de restauration à partir de données restaurées depuis une machine pour laquelle la déduplication de données a été activée, vous devez vérifier que la déduplication est également activée sur le serveur Core.

- 1 Dans la console Core Rapid Recovery, accédez à la machine à monter dans un système de fichiers local.
La page **Synthèse** de la machine protégée sélectionnée s'affiche.
- 2 Cliquez sur le menu **Points de restauration**.
La page **Points de restauration** de la machine sélectionnée s'affiche.
- 3 Si vous le souhaitez, dans la liste des points de restauration du volet **Points de restauration**, vous pouvez cliquer sur la flèche droite ► pour développer les détails concernant le point de restauration et afficher les volumes qu'il contient.
- 4 Dans la ligne du point de restauration à monter, cliquez sur  et dans le menu déroulant, sélectionnez **Monter**.
L'**Assistant de montage** s'affiche et ouvre la page **Volumes**.
- 5 Sur la page **Volumes**, sélectionnez chaque volume du point de restauration à monter, puis cliquez sur **Suivant**.
La page **Options de montage** de l'Assistant s'affiche.
- 6 Sur la page **Options de montage**, modifiez les paramètres de montage d'un point de restauration, comme indiqué dans le tableau suivant.

Tableau 151. Paramètres Options de montage

Option	Description
Dossier local	Indiquez le chemin d'accès au point de restauration monté. Par exemple, sélectionnez <code>C:\ProgramData\AppRecovery\MountPoints\MountPoint1</code> .
Type de montage	Spécifiez le mode d'accès au point de restauration monté : • Lecture seule • Lecture seule avec écritures préalables • Accessible en écriture
Créer un partage Windows pour ce montage	Éventuellement, vous pouvez cocher cette case pour indiquer si le point de restauration monté peut être partagé, puis définissez les droits d'accès à celui-ci, notamment le nom de partage et les groupes autorisés.

- 7 Cliquez sur **Terminer** pour monter le point de restauration.

① **REMARQUE :** si vous voulez copier des répertoires ou des fichiers depuis un point de restauration monté sur une autre machine Windows, vous pouvez utiliser l'explorateur Windows pour les copier avec les autorisations par défaut ou les autorisations d'accès des fichiers d'origine. Pour de plus amples informations, voir [Restauration d'un répertoire ou d'un fichier à l'aide de l'Explorateur Windows](#) jusqu'à [Restaurer un répertoire ou un fichier en conservant les autorisations avec l'Explorateur Windows](#).

- 8 Éventuellement, lorsque la tâche est en cours d'exécution, vous pouvez afficher son avancement dans le menu déroulant **Tâches en cours** de la console Core, ou afficher des informations détaillées sur la page **Événements**. Pour plus d'informations sur la surveillance des événements Rapid Recovery, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Démonter des points de restauration

Suivez cette procédure pour démonter des points de restauration montés sur le Core.

 **REMARQUE :** le démontage d'un point de restauration monté à distance est désigné en tant que *déconnexion*.

- 1 Dans la barre d'icônes de la console Core Rapid Recovery, cliquez sur  (Plus), puis sélectionnez  **Montages**.
La page **Montages** s'affiche. Il existe un volet pour les Montages locaux (points de restauration montés depuis le Core) et un autre pour les montages distants (points de restauration montés en utilisant l'utilitaire Local Mount Utility). Dans chaque volet, les points de restauration montés correspondants figurent dans une liste.
- 2 Pour démonter des montages locaux, dans le volet **Montages locaux**, procédez comme suit :
 - a Sélectionnez le ou les points de montage locaux que vous souhaitez démonter.
 - Pour démonter tous les points de restauration, cliquez sur la case à cocher dans la barre de titre du tableau Montages locaux pour sélectionner tous les points de montage.
 - Pour démonter un ou plusieurs points de restauration, dans la première colonne, cochez la case de chaque ligne désignant le point de montage à déconnecter.
 - b Cliquez sur  **Démonter**.
Une boîte de dialogue de confirmation s'affiche.
 - c Cliquez pour confirmer que vous souhaitez démonter les points de restauration sélectionnés.
Les points de restauration locaux sont démontés.

 **REMARQUE :** si les alertes Toast sont activées, vous pourrez voir une alerte indiquant que les points de montage sont en cours de démontage.

- 3 Pour déconnecter les points de restauration montés à distance, dans le volet **Montages distants**, procédez comme suit :
 - a Sélectionnez le ou les points de montage distants à déconnecter.
 - Pour déconnecter tous les points de restauration, dans la barre de titre du tableau Montages distants, cochez la case permettant de sélectionner tous les points de montage.
 - Pour déconnecter un ou plusieurs points de restauration, dans la première colonne, cochez la case de chaque ligne désignant le point de montage à déconnecter.
 - b Cliquez sur  **Déconnecter**.
Une boîte de dialogue de confirmation s'affiche.
 - c Cliquez pour confirmer que vous souhaitez déconnecter les points de restauration sélectionnés.
Les points de restauration locaux sont déconnectés.

 **REMARQUE :** si les alertes Toast sont activées, vous pourrez voir une alerte indiquant que les points de montage sont en cours de déconnexion.

- 4 Vérifiez que les points de restauration montés précédemment ne figurent plus dans la liste Montages locaux ou Montages distants, selon le cas.

Utiliser des points de restauration Linux

Le moyen conseillé et pris en charge de monter et démonter des points de restauration à partir d'une machine Linux protégée consiste à utiliser l'utilitaire `local_mount`.

Les procédures énumérées ci-dessous expliquent de manière spécifique l'utilisation de l'utilitaire `local_mount` pour monter et démonter des points de restauration Linux.

REMARQUE : pour gérer des points de restauration Linux d'une autre façon, voir [Gérer les instantanés et les points de restauration](#), ainsi que les autres façons de les gérer depuis la console Core.

Monter un volume d'un point de restauration sur une machine Linux

En utilisant l'utilitaire `local_mount` dans Rapid Recovery, vous pouvez monter à distance un volume à partir d'un point de restauration sous la forme d'un volume local sur une machine Linux.

REMARQUE : Lorsque vous effectuez cette procédure, n'essayez pas de monter les points de restauration dans le dossier `/tmp`, qui contient les fichiers `aavdisk`.

- 1 Créez un nouveau répertoire pour monter le point de restauration (par exemple, vous pouvez utiliser la commande `mkdir`).
- 2 Vérifiez que le répertoire existe (par exemple, en utilisant la commande `ls`).
- 3 Exécutez l'utilitaire `local_mount` Rapid Recovery en tant qu'utilisateur `root`, ou super utilisateur, par exemple :

```
sudo local_mount
```
- 4 À l'invite de montage Rapid Recovery, entrez la commande suivante pour répertorier les machines protégées.

```
lm
```
- 5 Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte de votre serveur Core Rapid Recovery.
- 6 Entrez les données d'identification de connexion du serveur Core, c'est-à-dire le nom d'utilisateur et le mot de passe.
La liste des machines protégées par le serveur Rapid Recovery va s'afficher. Chaque machine est identifiée par les éléments suivants : numéro de ligne, adresse IP/nom d'hôte et un numéro d'identification pour la machine.

Par exemple : 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

- 7 Entrez la commande suivante pour répertorier les points de restauration disponibles pour une machine spécifiée :

```
lr <line_number_of_machine>
```

REMARQUE : Notez que vous pouvez également entrer le numéro d'identification de la machine dans cette commande au lieu du numéro de ligne.

Une liste s'affiche indiquant les points de restauration de base et incrémentiels de cette machine. La liste comprend le numéro de ligne, l'horodatage, l'emplacement du volume, la taille du point de restauration et le numéro d'identification du volume, comprenant un numéro de séquence à la fin qui sert à identifier le point de restauration.

Par exemple, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

- 8 Entrez la commande suivante pour sélectionner et monter le point de restauration spécifié sur le point de montage/dans le chemin spécifié.

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

L'indicateur « flag » dans la commande détermine la manière de monter le point de restauration. Vous pouvez utiliser l'une des options suivantes :

- `[r]` - montage en lecture seule (par défaut). Cet indicateur vous permet de monter un point de restauration, mais ne vous permet pas d'y apporter des modifications.
- `[w]` - montage accessible en écriture. Cet indicateur vous permet de monter un point de restauration, et vous permet d'y apporter des modifications.
- `[v]` - monter avec les écritures précédentes. L'indicateur « v » vous permet de monter le point de restauration et d'y inclure tout changement qui a été apporté lors des montages accessibles en écriture précédents, mais qui ne sont pas présents dans le point de restauration.
- `[n]` - ne pas monter le nbd sur `<path>`. Un nbd (Network Block Device) établit une connexion socket entre le Core et la machine protégée lorsque vous effectuez un montage local. Cet indicateur vous permet de monter le point de restauration sans monter le nbd, ce qui est utile si vous souhaitez vérifier manuellement le système de fichiers du point de restauration.

❶ **REMARQUE :** Pour identifier le point de restauration, vous pouvez également spécifier un numéro de ligne dans la commande au lieu du numéro d'identification du point de restauration. Dans ce cas, vous allez utiliser le numéro de ligne de la machine (de la sortie `lm`), suivi du numéro de ligne du point de restauration et de la lettre du volume, suivi du chemin d'accès, par exemple, `m <numéro_ligne_machine> <numéro_ligne_point_restoration> <lettre_volume> <chemin>`. Par exemple, si la sortie `lm` répertorie trois machines protégées, et que vous entrez la commande `lr` pour le numéro 2 et que vous montez le point de restauration 23, volume b sur `/tmp/mount_dir`, la commande sera alors `m 2 23 b /tmp/mount_dir`

❶ **REMARQUE :** Si vous montez un volume BTRFS à partir d'un système d'exploitation compatible (voir la rubrique « Tableau d'installation et de compatibilité des systèmes d'exploitation avec Rapid Recovery version 6.1 » dans le *Dell Data Protection | Rapid Recovery Installation and Upgrade Guide* (Guide d'installation et de mise à jour de Dell Data Protection | Rapid Recovery)), vous devez inclure le paramètre suivant :

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9 Pour vérifier que le montage est réussi, entrez la commande suivante, qui devrait répertorier le volume distant attaché :

```
l
```

Démonter un point de restauration sur une machine Linux

Suivez les étapes de cette procédure pour démonter un point de restauration d'une machine Linux.

1 Exécutez l'utilitaire `local_mount` Rapid Recovery en tant qu'utilisateur root, ou super utilisateur, par exemple :

```
sudo local_mount
```

2 À l'invite de montage Rapid Recovery, entrez la commande suivante pour répertorier les machines protégées.

```
lm
```

3 Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte de votre serveur Core Rapid Recovery.

4 Entrez les données d'identification de connexion (le nom d'utilisateur et le mot de passe) de ce serveur.

La liste des machines protégées par le serveur Rapid Recovery va s'afficher.

5 Entrez la commande suivante pour répertorier les points de restauration disponibles pour une machine spécifiée :

```
lr <line_number_of_machine>
```

❶ **REMARQUE :** notez que vous pouvez également entrer le numéro d'identification de la machine dans cette commande au lieu du numéro de ligne.

Une liste des points de restauration de base et incrémentiels de la machine va s'afficher et comporter les éléments suivants. La liste comprend le numéro de ligne, l'horodatage, l'emplacement du volume, la taille du point de restauration et le numéro d'identification du volume, comprenant un numéro de séquence à la fin qui sert à identifier le point de restauration.

Par exemple : 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6 Exécutez la commande `l or list` pour obtenir la liste des dispositifs Network Block Device (NBD) montés. Si vous montez n'importe quel point de restauration, vous allez obtenir un chemin vers le dispositif NBD après avoir exécuté la commande `l or list`.

7 Entrez la commande suivante pour démonter un point de restauration.

```
umount <path_of_nbd-device>
```

8 Exécutez la commande `l or list` pour vérifier que le démontage du point de restauration s'est bien déroulé.

Forcer un instantané

Forcer un instantané permet de forcer un transfert de données pour la machine protégée actuelle. Lorsque vous forcez un instantané, le transfert est soit lancé immédiatement, soit ajouté à la file d'attente lorsque d'autres tâches sont en cours d'exécution.

Vous avez le choix entre deux types d'instantané.

Si vous sélectionnez un instantané incrémentiel et qu'il n'existe aucun point de restauration antérieur, une image de base est réalisée. Le fait de forcer un instantané ne modifie pas le moment choisi pour les instantanés de planifications.

REMARQUE : Rapid Recovery est compatible avec Windows 8, Windows 8.1, Windows Server 2012 et Windows Server 2012 R2 pour les transferts de base et incrémentiels.

- Une image de base est un instantané de toutes les données des volumes sélectionnés de la machine.
 - Un instantané incrémentiel enregistre toutes les données modifiées depuis le dernier instantané.
- 1 Dans la console Core Rapid Recovery, accédez à la machine ou au cluster possédant le point de restauration pour lequel vous souhaitez forcer un instantané.
 - 2 Sur le volet Synthèse de la page éponyme, cliquez sur **Forcer l'instantané**.
La boîte de dialogue Forcer l'instantané s'affiche.
 - 3 Dans la boîte de dialogue Forcer l'instantané, dans la case à cocher, cliquez sur un ou plusieurs volumes ou groupes de protection.
 - 4 Cliquez sur **Forcer l'instantané** ou Forcer l'image de base, le cas échéant.
 - 5 Si vous avez sélectionné une image de base, cliquez pour confirmer votre sélection.
La création d'une image de base peut prendre beaucoup de temps, selon la quantité de données que contiennent les volumes à sauvegarder.

L'instantané sélectionné est mis en file d'attente et démarre une fois les autres tâches terminées.

Supprimer des points de restauration

Vous pouvez facilement supprimer des points de restauration d'une machine de la logithèque. Lorsque vous supprimez des points de restauration dans Rapid Recovery, vous pouvez spécifier l'une des options suivantes.

- **Supprimer tous les points de restauration.** Supprime tous les points de restauration de la logithèque pour la machine protégée sélectionnée.
- **Supprimer une plage de points de restauration.** Supprime tous les points de restauration d'une plage spécifiée avant le point de restauration actuel jusqu'à l'image de base (inclusive), c'est-à-dire toutes les données de la machine, ainsi que tous les points de restauration après le point de restauration actuel jusqu'à la prochaine image de base.

REMARQUE : vous ne pouvez pas récupérer les points de restauration que vous avez supprimés. Si vous avez besoin des données stockées dans les points de restauration, pensez à effectuer l'archivage de ces données en premier lieu.

- 1 Dans la console Core Rapid Recovery, sous **Machines protégées**, cliquez sur le nom ou l'adresse IP de la machine dont vous souhaitez afficher et supprimer les points de restauration.
La vue Synthèse de la machine protégée sélectionnée s'affiche.
- 2 En regard du nom de la machine ou de son adresse IP, cliquez sur le menu **Points de restauration**.
La page **Points de restauration** de la machine sélectionnée s'affiche.
- 3 Faites défiler vers le bas jusqu'au volet **Points de restauration**.
Des options s'affichent sous le titre du volet, notamment Actualiser, Supprimer la plage et Supprimer tout.
- 4 Pour supprimer tous les points de restauration actuellement stockés, sous le titre du volet Points de restauration, cliquez sur **Supprimer tout**, puis dans la boîte de dialogue de confirmation, cliquez pour confirmer la suppression.
- 5 Pour supprimer un ensemble de points de restauration dans une plage de données spécifique, procédez comme suit :
 - a Sous le titre du volet Points de restauration, cliquez sur **Supprimer la plage**.
La boîte de dialogue **Supprimer les points de restauration dans la plage** s'affiche.
 - b Dans la boîte de dialogue **Supprimer les points de restauration dans la plage**, accédez au champ **De**, puis sélectionnez la date et l'heure à partir desquelles vous souhaitez supprimer les points de restauration.
 - c Dans le champ **À**, sélectionnez la date et l'heure définissant le dernier point de restauration à supprimer.
 - d Cliquez sur **Supprimer**.
 - e Dans la boîte de dialogue de confirmation, cliquez pour confirmer la suppression.

Supprimer une chaîne de points de restauration orphelins

Un point de restauration orphelin est un instantané incrémentiel qui n'est pas associé à une image de base. Les instantanés suivants continuent de reposer sur ce point de restauration. Cependant, sans l'image de base, les points de restauration qui en résultent sont incomplets et ne contiendront vraisemblablement pas les données nécessaires à l'exécution d'une restauration. Ces points de restauration sont considérés comme faisant partie d'une chaîne de points de restauration orphelins. Dans ce cas, la meilleure solution est de supprimer la chaîne et de créer une image de base.

Pour plus d'informations sur le forçage d'une image de base, voir [Forcer un instantané](#).

- 1 Dans la Rapid Recovery Core Console, accédez à la machine protégée pour laquelle vous souhaitez supprimer la chaîne de points de restauration orphelins.
- 2 Dans le menu situé en haut de la page, cliquez sur **Points de restauration**.
- 3 Dans le volet Points de restauration, développez le point de restauration orphelin.
Ce point de restauration s'appelle « Incrémentiel, orphelin » dans la colonne Type.
- 4 En regard de l'option Actions, cliquez sur **Supprimer**.
La fenêtre Supprimer les points de restauration s'affiche.
- 5 Dans la fenêtre Supprimer les points de restauration, cliquez sur **Oui**.

⚠ PRÉCAUTION : La suppression du point de restauration supprime la chaîne complète de points de restauration, y compris les éventuels points de restauration incrémentiels apparus avant ou après la suppression, jusqu'à la prochaine image de base. Cette opération ne peut pas être annulée.

La chaîne de points de restauration orphelins est supprimée.

Migration de points de restauration vers une logithèque différente

Si vous voulez supprimer d'une logithèque les points de restauration d'une machine protégée sans les supprimer pour autant, vous pouvez les migrer manuellement vers une autre logithèque en suivant cette procédure. Ce processus implique l'archivage des points de restauration à partir de la logithèque source, puis l'importation de l'archive dans la logithèque cible.

Par exemple, vous pouvez effectuer cette procédure si votre logithèque existante est pleine ou si vos besoins changent et que vous souhaitez protéger une machine à l'aide d'un Core et d'une logithèque différents.

⚠ PRÉCAUTION : Si votre logithèque a été précédemment mise à jour à partir d'AppAssure 5.3 ou 5.4 et a utilisé une réplique, Dell vous recommande d'effectuer la tâche de vérification de logithèque sur chaque logithèque de ce Core cible avant la migration. L'exécution de cette tâche évitera la copie des irrégularités des données sur la nouvelle logithèque de destination. La tâche de vérification de logithèque est uniquement disponible dans l'interface utilisateur si elle s'applique à votre Core et son exécution peut prendre beaucoup de temps. Pour en savoir plus sur cette tâche, voir [À propos de la vérification de l'intégrité des référentiels DVM](#). Pour en savoir plus sur l'exécution de cette tâche, voir [Exécution de la tâche de vérification de logithèque sur une logithèque DVM](#).

- 1 Dans la Rapid Recovery Core Console, suspendez la protection pour la machine ou les machines protégées dont vous souhaitez migrer les points de restauration. Pour plus d'informations, voir [Suspendre et reprendre la protection](#).
- 2 Annulez toutes les opérations actives pour la ou les machines protégées dont vous souhaitez migrer les points de restauration ou attendez la fin de ces opérations.
- 3 Archivez les points de restauration de la ou des machines que vous avez suspendues. Pour plus d'informations, voir [Création d'une archive](#).
- 4 Après l'archivage et la vérification de l'archive, retirez les points de restauration existants de la machine protégée que vous souhaitez migrer. Pour plus d'informations, voir [Supprimer des points de restauration](#).

REMARQUE : Si vous ne supprimez pas les points de récupération existants, vous ne pouvez pas changer les logithèques pour une machine protégée.

- 5 Créez une nouvelle logithèque pour les points de restauration migrés ou assurez-vous qu'une nouvelle logithèque de destination existe. Pour en savoir plus, voir [Créer un référentiel DVM](#).
 - Si vous voulez utiliser une logithèque existante, passez à l'[Étape 6](#).
- 6 Modifiez la logithèque de chaque machine que vous avez suspendue en procédant comme suit :
 - a Sur Core Console, cliquez sur la machine protégée dans l'arborescence.
 - b Sur la page **Résumé** de la machine protégée, cliquez sur **Paramètres**.
 - c Sur la page **Paramètres**, dans le volet **Général**, cliquez sur la liste déroulante **Logithèque**, puis sélectionnez le nom de la logithèque que vous avez créée à l'[Étape 4](#).
 - Si vous voulez utiliser une logithèque existante, sélectionnez le nom d'une logithèque existante.
 - d Cliquez sur **OK**.
- 7 Reprenez la protection de la ou des machines dont vous aviez suspendu la protection. Pour plus d'informations, voir [Suspendre et reprendre la protection](#).
- 8 Prendre une nouvelle image de base pour chacune des machines protégées que vous avez déplacées. Pour plus d'informations, voir [Forcer un instantané](#) et utilisez l'option Forcer l'image de base.
- 9 Importez les données archivées des machines que vous voulez migrer. Pour en savoir plus, voir [Importer une archive](#).

REMARQUE : Lorsque vous migrez des points de restauration vers une logithèque existante, assurez-vous que la logithèque existante dispose de suffisamment d'espace libre pour accueillir les points de restauration migrés.

Restaurer des données

Cette section décrit comment restaurer les données sauvegardées.

À propos de la restauration de données avec Rapid Recovery

Le Core Rapid Recovery peut restaurer les données ou restaurer immédiatement les machines vers des machines physiques ou virtuelles à partir des points de restauration. Les points de restauration contiennent les instantanés des volumes des agents, capturés au niveau des blocs. Ces instantanés tiennent compte de l'état et du fonctionnement des applications, ce qui implique que toutes les transactions ouvertes et les journaux de transactions en cours sont terminés et les caches sont vidés sur disque avant la création d'instantanés. L'utilisation de snapshots prenant en compte les applications en conjonction avec Verified Recovery permet au Core d'effectuer plusieurs types de restaurations, notamment :

- Restauration de fichiers et de dossiers
- Restauration de volumes de données à l'aide de Live Recovery
- Restauration de volumes de données pour Microsoft Exchange Server et Microsoft SQL Server à l'aide de Live Recovery
- Restauration sans système d'exploitation à l'aide d'Universal Recovery
- Restauration sans système d'exploitation sur un matériel différent à l'aide d'Universal Recovery
- Exportation ponctuelle et exportation continue sur des machines virtuelles

REMARQUE : lorsque vous restaurez des données ou effectuez une exportation virtuelle, le point de restauration utilisé doit faire partie d'une chaîne de points de restauration complète. Pour plus d'informations sur les chaînes de points de restauration, voir la rubrique [Points de restauration en chaîne et orphelins](#).

Compréhension des Live Recovery

Live Recovery est une fonction de restauration des données dans le Core Rapid Recovery. Si votre machine protégée subit l'échec de données d'un volume Windows non système, vous pouvez restaurer les données à partir d'un point de restauration sur le Core Rapid Recovery. La sélection de Live Recovery dans l'Assistant Restauration permet aux utilisateurs de continuer immédiatement leurs activités

commerciales, quasiment sans temps d'arrêt. Au cours de la restauration, Live Recovery vous permet d'accéder directement aux données, même pendant que Rapid Recovery continue à restaurer les données en arrière-plan. Cette fonction offre un temps de récupération quasi nul, même si la restauration concerne des téraoctets de données.

Le Core Rapid Recovery utilise une technologie unique de sauvegarde et de récupération, basée sur des blocs, qui permet aux utilisateurs d'accéder entièrement aux serveurs cible au cours du processus de récupération. Les blocs demandés sont restaurés à la demande pour une récupération transparente.

Live Recovery s'applique aux machines physiques et virtuelles protégées par le Core Rapid Recovery, avec les exclusions suivantes :

- Live Recovery est accessible aux volumes Windows non système. Le lecteur C:\ et la partition réservée au système ne peuvent pas être restaurés à l'aide de Live Recovery.
- Live Recovery est accessible pour les volumes basés sur Windows à l'aide de l'agent Rapid Recovery. Les volumes sans agent ou sous Linux ne peuvent pas bénéficier de Live Recovery.

Live Recovery vous permet de restaurer immédiatement des serveurs physiques ou virtuels directement à partir du fichier de sauvegarde. Lorsqu'un volume non système est en cours de restauration, Rapid Recovery présente instantanément les métadonnées de volume pour le système d'exploitation, rendant ces données disponibles sur demande. Par exemple, si le volume de base de données de Microsoft Exchange est corrompu, Live Recovery peut restaurer le volume, la base de données et les services Exchange en quelques minutes.

Cette fonctionnalité constitue la méthode de récupération la plus rapide pour de grandes quantités de données avec un temps d'arrêt minimal. Les utilisateurs peuvent immédiatement poursuivre leurs activités commerciales.

Une fois Live Recovery lancé, le volume restauré et son contenu deviennent instantanément disponibles. Le Core Rapid Recovery continue de restaurer les données en arrière-plan, même si le volume, ses données, les applications et les services sont déjà à nouveau en production. Si des données spécifiques sont demandées, le processus en arrière-plan donne la priorité à la restauration immédiate de ces données. Cette fonctionnalité performante permet de respecter les contrats de niveau de service les plus exigeants.

Lorsque vous démarrez Live Recovery, les métadonnées (structure de répertoire, descripteurs de sécurité, attributs de fichiers NTFS, carte d'espace libre, etc.) du volume cible sont restaurées rapidement sur la machine protégée. Ensuite, le volume et son contenu deviennent disponibles pour le système. L'agent Rapid Recovery commence à restaurer les blocs de données du serveur Core Rapid Recovery, en écrivant les blocs sur le volume cible.

Les demandes de données qui n'ont pas encore été restaurées reçoivent immédiatement une réponse, le programme ou système demandeur ne détectant pas que les blocs viennent d'être restaurés.

Restaurer des données à partir de points de restauration

Rapid Recovery protège vos données sur les machines Windows et Linux. Les sauvegardes des machines agent protégées sont enregistrées sur le Core Rapid Recovery sous la forme de points de restauration. À partir de ces points de restauration, vous avez le choix entre trois méthodes pour restaurer vos données.

Dans la Rapid Recovery Core Console, vous pouvez restaurer des volumes entiers à partir d'un point de restauration d'un volume non système, en remplaçant les volumes sur la machine de destination. Cela s'applique uniquement aux machines Windows. Pour plus d'informations, voir [À propos de la restauration de volumes à partir d'un point de restauration](#).

Vous ne pouvez pas restaurer un volume qui contient le système d'exploitation directement à partir d'un point de restauration, car la machine sur laquelle vous effectuez la restauration utilise le système d'exploitation et les pilotes associés dans le processus de restauration. Si vous voulez restaurer à partir d'un point de restauration sur un volume système (par exemple, le disque C de la machine agent, vous devez effectuer une restauration BMR (Bare Metal Restore). Cette opération crée une image amorçable du point de restauration, qui inclut le système d'exploitation et les fichiers de configuration, ainsi que les données, et démarrer la machine cible à partir de cette image amorçable pour effectuer la restauration. L'image d'amorçage est différente selon que la machine à restaurer utilise un système d'exploitation Windows ou Linux. Si vous souhaitez effectuer une restauration à partir d'un point de restauration vers un volume système sur une machine Windows, voir [Exécution d'une restauration complète sur des machines Windows](#). Si vous souhaitez effectuer une restauration à partir d'un point de restauration d'un volume système sur une machine Linux, voir [Exécution d'une restauration complète sur des machines Linux](#).

Enfin, par opposition à la restauration de volumes entiers, vous pouvez monter un point de restauration à partir d'une machine Windows, et naviguer dans les dossiers et fichiers pour ne restaurer qu'un ensemble de fichiers spécifiques. Pour plus d'informations, voir [Restauration d'un répertoire ou d'un fichier à l'aide de l'Explorateur Windows](#). Si vous souhaitez procéder ainsi tout en préservant les autorisations des fichiers d'origine (par exemple, lorsque vous restaurez le dossier d'un utilisateur sur un serveur de fichiers), voir [Restaurer un répertoire ou un fichier en conservant les autorisations avec l'Explorateur Windows](#).

Les rubriques de cette section contiennent des informations sur la restauration des données sur les machines physiques. Pour en savoir plus sur l'exportation des données protégées des machines Windows vers des machines virtuelles, voir [VM export \(Exportation NFS\)](#).

REMARQUE : lorsque vous récupérez des données sur des machines Windows, si la déduplication des données Windows est activée sur le volume que vous restaurez, vous devez vérifier que la déduplication est également activée sur le serveur Core. Rapid Recovery est compatible avec Windows 8, Windows 8.1, Windows 10, Windows Server 2012 et Windows Server 2012 R2 pour les transferts normaux (de base et incrémentiels), ainsi que pour les restaurations de données, les restaurations BMR et les exportations virtuelles. Pour en savoir plus sur les types de volumes pris en charge et non pris en charge pour la sauvegarde et la restauration, voir [Prise en charge des volumes dynamiques et des volumes de base](#).

À propos de la restauration de volumes à partir d'un point de restauration

Vous pouvez restaurer les volumes d'une machine protégée à partir des points de récupération conservés dans le Noyau de la Rapid Recovery.

REMARQUE : dans les versions précédentes, ce processus était appelé une Restauration.

REMARQUE : la Rapid Recovery prend en charge la protection et la récupération des machines configurées avec des partitions EISA. L'assistance est en outre étendue aux machines sous Windows 8, Windows 8.1, Windows Server 2012 et Windows Server 2012 R2 utilisant l'environnement de récupération de Windows (Windows RE).

Vous pouvez entamer une restauration depuis n'importe quel emplacement sur la console du Noyau de la Rapid Recovery en cliquant sur l'icône Restauration dans la barre des boutons de la Rapid Recovery. Lorsque vous démarrez un processus de restauration de cette manière, vous devez préciser la ou les machines protégées sur le Noyau que vous souhaitez restaurer, puis le volume à restaurer.

Vous pouvez également vous rendre sur la page Points de récupération d'une machine particulière, cliquer sur un point de récupération spécifique dans le menu déroulant, puis sélectionner **Restauration**. Si vous démarrez un processus de restauration de cette manière, suivez alors cette procédure en commençant par l'[étape 5](#).

Si vous souhaitez restaurer depuis un point de récupération vers un volume système, ou restaurer depuis un point de récupération à l'aide d'un CD de démarrage, vous devez effectuer une restauration complète. Pour plus d'informations sur les restaurations complètes, veuillez consulter [Comprendre la restauration Bare Metal Restore pour les machines Windows](#). Pour des informations préliminaires au sujet des systèmes d'exploitation Windows ou Linux, veuillez consulter [Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows](#) et [Prérequis pour l'exécution d'une restauration BMR pour une machine Linux](#), respectivement. Vous pouvez accéder aux fonctions de restauration complète depuis la console du Noyau, comme il est décrit dans la feuille de route de chaque système d'exploitation. Vous pouvez également procéder à une restauration complète depuis l'assistant Restauration de machines. Ceci vous amènera jusqu'au point approprié dans l'assistant de la procédure [Exécution d'une restauration BMR avec l'Assistant Restaurer une machine](#).

Restaurer des volumes à partir d'un point de restauration

Le logiciel Agent doit être installé sur la machine protégée et doit aussi avoir des points de restauration depuis lesquels vous pouvez effectuer l'opération de restauration.

Suivez la procédure suivante pour restaurer des volumes à partir d'un point de restauration.

- 1 Pour restaurer un volume sur une machine protégée depuis l'icône Restaurer, accédez à la Core Console, puis cliquez sur **Restaurer** dans la barre des boutons Rapid Recovery.

L'assistant Restaurer une machine s'affiche.

- 2 Depuis la page Machines protégées, sélectionnez la machine protégée dont vous voulez restaurer les données, puis cliquez sur **Suivant**.
La page points de restauration s'affiche.
 - 3 Depuis la liste de points de restauration, recherchez l'instantané à restaurer sur la machine agent.
 - Si nécessaire, utilisez les boutons dans le bas de la page pour afficher d'autres pages de points de restauration.
 - Si vous voulez limiter le nombre de points de restauration qui s'affichent sur la page Points de restauration de l'Assistant, vous pouvez filtrer par volumes (s'ils sont définis) ou par date de création de point de restauration.
 - 4 Cliquez sur un point de restauration pour le sélectionner, puis sur **Suivant**.
La page Destination s'affiche.
 - 5 Sur la page Destination, sélectionnez la machine à partir de laquelle vous souhaitez restaurer les données, comme suit :
 - si vous voulez restaurer des données depuis le point de restauration sélectionné sur la même machine et que les volumes que vous voulez restaurer ne contiennent pas le volume système, sélectionnez **Restaurer sur une machine protégée (seulement les volumes hors volume système)**, vérifiez que la machine de destination est sélectionnée, puis cliquez sur **Suivant**.
La page Adressage des volumes s'affiche. Passez à l'étape 9.
 - Pour restaurer des données depuis le point de restauration sélectionné sur une machine protégée différente (par exemple, pour remplacer le contenu de Machine2 par les données de Machine1), sélectionnez **Restaurer sur une machine protégée (seulement les volumes hors volume système)** et la machine de destination dans la liste, puis cliquez sur **Suivant**.
La page Adressage des volumes s'affiche. Passez à l'étape 9.
 - Si vous voulez effectuer une restauration depuis le point de restauration sélectionné vers la même machine ou une machine différente en utilisant un CD d'amorçage, il s'agit alors d'une restauration BMR (Bare Metal Restore). Pour plus d'informations sur la restauration BMR, voir [Comprendre la restauration Bare Metal Restore pour les machines Windows](#).
- REMARQUE :** l'exécution d'une restauration BMR répond à des conditions spécifiques, en fonction du système d'exploitation de la machine agent à restaurer. Pour connaître ces conditions, voir respectivement [Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows](#) et [Prérequis pour l'exécution d'une restauration BMR pour une machine Linux](#).

Si les volumes à restaurer incluent le volume système, sélectionnez **Restaurer sur n'importe quelle machine cible à l'aide d'un CD d'amorçage**. Cette option demande de créer un CD d'amorçage.

 - Pour continuer et créer le CD d'amorçage avec les informations du point de restauration sélectionné en utilisant l'assistant de restauration de machine, cliquez sur **Suivant**, et reportez-vous à [Exécution d'une restauration complète sur des machines Windows](#).
 - Si vous avez déjà créé le CD d'amorçage et que la machine cible a été démarrée avec le CD, passez à l'étape 8 de la rubrique [Exécution d'une restauration complète sur des machines Windows](#).
- Si vous voulez effectuer une restauration depuis un point de restauration vers un volume système (par exemple, le disque C de la machine agent Machine1), il s'agit également d'une restauration BMR (Bare Metal Restore). Sélectionnez **Restaurer sur n'importe quelle machine cible avec un CD d'amorçage**. Cette option demande de créer un CD d'amorçage.
 - Pour continuer et créer le CD d'amorçage avec les informations du point de restauration sélectionné en utilisant l'assistant de restauration de machine, cliquez sur **Suivant**, et reportez-vous à [Exécution d'une restauration complète sur des machines Windows](#).
 - Si vous avez déjà créé le CD d'amorçage, passez à l'étape 6.
 - 6 Démarrez la machine cible de la restauration en utilisant le CD d'amorçage. Pour plus d'informations, pour la restauration BMR sur une machine Windows, voir [Chargement du CD d'amorçage et démarrage de la machine cible](#) et pour davantage d'informations sur la restauration BMR sur une machine Linux, voir [Chargement du DVD Live et démarrage de la machine cible](#).
 - 7 Sur le serveur Core, sur la page Destination de l'Assistant de restauration de machine, sélectionnez **J'ai déjà un CD d'amorçage exécuté sur la machine cible** et saisissez les informations relatives à la machine à laquelle vous voulez vous connecter, comme indiqué dans le tableau suivant.

Tableau 152. Informations sur la machine

Zone de texte	Description
Adresse IP	Adresse IP de la machine à restaurer. Celle-ci est identique à l'adresse IP affichée dans l'URC.
Clé d'authentification	Mot de passe pour se connecter au serveur sélectionné. Celui-ci est identique à la clé d'authentification affichée dans l'URC.

8 Cliquez sur **Suivant**.

Si les informations de connexion que vous avez saisies correspondent à celles de l'URC et que le Core et le serveur cible peuvent s'identifier correctement mutuellement sur le réseau, les volumes du point de restauration sélectionné sont chargés. La page Adressage des disques s'affiche.

Pour exécuter la restauration BMR depuis l'Assistant Restaurer une machine, passez à l'étape 9 de la rubrique [Exécution d'une restauration complète sur des machines Windows](#).

REMARQUE : Rapid Recovery prend en charge les partitions FAT32 et ReFS. Seules la restauration complète et la restauration BMR sont prises en charge en cas de limitation de pilote avec ReFS. La restauration est mise en œuvre en mode utilisateur, dans l'exportation de machine virtuelle, etc. Si un Core protège au moins un volume agent qui contient le système de fichiers ReFS, il doit être installé sur une machine Windows 8/2012 qui fournit le support natif de ReFS. À défaut, la fonctionnalité est limitée, et les opérations impliquant le montage d'une image de volume ne fonctionnent pas. La Rapid Recovery Core Console affiche alors les messages d'erreur applicables en de telles circonstances.

La restauration BMR de la configuration des disques d'espace de stockage (une fonctionnalité de Windows 8.1) n'est pas prise en charge dans cette version. Pour plus d'informations, voir le Guide d'installation et de mise à niveau de Rapid Recovery.

9 Sur la page Adressage des volumes, pour chacun des volumes du point de restauration à restaurer, choisissez le volume de destination approprié. S'il existe un volume que vous ne voulez pas restaurer, sélectionnez **Ne pas restaurer** dans la colonne Volumes de destination.

10 Cliquez sur **Afficher les options avancées** et procédez comme suit :

- Pour restaurer sur des machines Windows, si vous voulez utiliser Live Recovery, cliquez sur **Live Recovery**.
En utilisant la technologie de restauration instantanée Live Recovery de Rapid Recovery, vous pouvez récupérer ou restaurer des données instantanément sur des machines physiques ou virtuelles à partir de points de restauration de machines Windows, y compris les espaces de stockage Microsoft Windows. Live Recovery n'est pas disponible pour les machines Linux ou les machines virtuelles employant une protection sans agent.
- Si vous souhaitez forcer le démontage des volumes sélectionnés avant de démarrer la restauration, sélectionnez **Forcer le démontage**.

PRÉCAUTION : Si vous ne forcez pas le démontage avant de restaurer les données, la restauration risque d'échouer avec une erreur indiquant que le volume est en cours d'utilisation.

11 Cliquez sur **Suivant**.

12 Si les volumes à restaurer contiennent des bases de données SQL ou Microsoft Exchange, vous êtes invité à les démonter sur la page Démonter les bases de données.

Si vous voulez remonter ces bases de données à la fin de la restauration, sélectionnez **Remonter automatiquement toutes les bases de données après la restauration du point de restauration**.

13 Cliquez sur **Suivant**.

La page Avertissement peut s'afficher pour vous inviter à fermer tous les programmes sur les volumes à restaurer. Si tel est le cas, cliquez de nouveau sur **Suivant**.

14 Sur la page Récapitulatif, sélectionnez l'option **IMPORTANT ! Je comprends que cette opération remplacera les volumes sélectionnés par les données du point de restauration sélectionné** pour confirmer que vous comprenez les conséquences de restauration d'un volume.

AVERTISSEMENT : Cette option souligne le fait que toutes les données qui ont été enregistrées sur le volume sélectionné après la date et l'heure du point de restauration sélectionné seront perdues lors de la restauration.

Restauration d'un répertoire ou d'un fichier à l'aide de l'Explorateur Windows

Vous pouvez utiliser l'Explorateur Windows pour copier et coller des répertoires et des fichiers depuis un point de restauration vers n'importe quelle machine Windows. Cela peut s'avérer utile lorsque vous souhaitez ne distribuer qu'une partie d'un point de restauration aux utilisateurs.

Lorsque vous copiez des répertoires et des fichiers, les autorisations d'accès de l'utilisateur qui effectue l'opération de copie sont utilisées et appliquées aux répertoires et aux fichiers collés. Pour restaurer des répertoires et des fichiers pour les utilisateurs tout en préservant les autorisations des fichiers d'origine (par exemple, lorsque vous restaurez le dossier d'un utilisateur sur un serveur de fichiers), voir [Restaurer un répertoire ou un fichier en conservant les autorisations avec l'Explorateur Windows](#).

- 1 Montez le point de restauration qui contient les données à restaurer. Pour de plus amples informations, voir [Monter un point de restauration](#).
- 2 Dans l'Explorateur Windows, accédez au point de restauration monté et sélectionnez les répertoires et les fichiers à restaurer. Faites un clic droit et sélectionnez **Copier**.
- 3 Dans l'Explorateur Windows, accédez à l'emplacement de la machine où vous souhaitez restaurer les données. Faites un clic droit et sélectionnez **Coller**.

Restaurer un répertoire ou un fichier en conservant les autorisations avec l'Explorateur Windows

Vous pouvez utiliser l'Explorateur Windows pour copier et coller des répertoires et des fichiers depuis un point de restauration vers n'importe quelle machine Windows tout en conservant les autorisations d'accès aux fichiers.

Par exemple, si vous devez restaurer un dossier accessible uniquement par des utilisateurs spécifiques sur un serveur de fichiers, vous pouvez utiliser les commandes Copier et Coller avec les autorisations pour que les fichiers restaurés conservent les autorisations restreignant l'accès. De cette façon, vous pouvez éviter d'avoir à appliquer manuellement les autorisations aux répertoires et aux fichiers restaurés.

REMARQUE : La commande **Coller avec les autorisations** est installée avec les logiciels **Agent** et **Core Rapid Recovery**. Elle n'est pas disponible dans l'utilitaire **Local Mount Utility**.

- 1 Montez le point de restauration qui contient les données à restaurer. Pour de plus amples informations, voir [Monter un point de restauration](#).
- 2 Dans l'Explorateur Windows, accédez au point de restauration monté et sélectionnez les répertoires et les fichiers à restaurer. Faites un clic droit et sélectionnez **Copier**.
- 3 Dans l'Explorateur Windows, accédez à l'emplacement de la machine où vous souhaitez restaurer les données. Faites un clic droit et sélectionnez **Coller avec les autorisations**.

REMARQUE : Dans cette étape, si la commande **Coller avec les autorisations** est désactivée dans le menu contextuel (clic droit), cela implique que l'Explorateur Windows n'a pas connaissance des fichiers à copier. Répétez l'étape 2 pour activer la commande **Copier avec les autorisations** dans le menu contextuel (clic droit).

Restauration de clusters et de nœuds de cluster

La restauration est le processus consistant à restaurer les volumes d'une machine à partir de points de récupération. Pour un cluster de serveurs, la restauration s'effectue au niveau d'un nœud ou d'une machine. Cette section présente les consignes permettant de restaurer des volumes d'un cluster.

Restauration pour des clusters CCR et DAG (Exchange)

Suivez les étapes décrites dans cette procédure afin d'effectuer une restauration pour des clusters CCR et DAG (Exchange).

- 1 Désactivez tous les nœuds sauf un.
- 2 Effectuez une restauration à l'aide de la procédure de Rapid Recovery standard pour la machine, comme il est décrit dans [À propos de la restauration de volumes à partir d'un point de restauration](#) et [Restaurer les volumes d'une machine Linux à l'aide de la ligne de commande](#).
- 3 Lorsque la restauration est terminée, montez toutes les bases de données pour les volumes du cluster.
- 4 Activez tous les autres nœuds.
- 5 Pour Exchange, accédez à la console de gestion Exchange, puis, pour chaque base de données, procédez à la mise à jour de la copie de la base de données.

Restauration pour des clusters SCC (Exchange, SQL)

Suivez les étapes décrites dans cette procédure afin d'effectuer une restauration pour des clusters SCC (Exchange, SQL).

- 1 Désactivez tous les nœuds sauf un.
- 2 Effectuez une restauration à l'aide de la procédure de Rapid Recovery standard pour la machine, comme il est décrit dans [À propos de la restauration de volumes à partir d'un point de restauration](#) et [Restaurer les volumes d'une machine Linux à l'aide de la ligne de commande](#).
- 3 Lorsque la restauration est terminée, montez toutes les bases de données depuis les volumes du cluster.
- 4 Activez tous les nœuds un par un.

REMARQUE : vous n'avez pas à effectuer une restauration automatique du disque de quorum. Celui-ci peut être régénéré automatiquement ou en utilisant la fonctionnalité du service de cluster.

Restauration depuis une archive attachée

Il y a deux façons de restaurer des données depuis une archive. Vous pouvez utiliser une archive comme base d'une restauration complète ; ou vous pouvez attacher une archive, monter un point de récupération depuis cette archive, puis restaurer les données archivées.

Lorsque vous attachez une archive, elle apparaît sous Archives attachées de la page Archives de la console du Noyau, tandis que son contenu est accessible depuis la zone de navigation gauche. Le contenu apparaît sous le nom de l'archive. Les machines archivées apparaissent en tant que machines avec points de récupération. De cette façon, vous pouvez accéder aux points de récupération de la même manière que pour une machine actuellement protégée : en montant un point de récupération, en identifiant l'élément que vous souhaitez récupérer et en utilisant l'explorateur Windows pour copier et coller l'élément jusqu'à votre destination.

Il y a des avantages à procéder à une restauration depuis une archive attachée plutôt que d'importer une archive dans une logithèque.

- Restaurer depuis une archive attachée vous permet d'économiser le temps que vous auriez passé à importer une archive entière dans une logithèque.
 - En outre, lorsque vous importez une archive, les points de récupération archivés sont ajoutés à la logithèque. À cause du fait que ces points de récupération archivés sont certainement les éléments les plus anciens présents dans la logithèque, ils peuvent faire l'objet d'un cumul, selon votre stratégie de conservation, lors de la prochaine tâche nocturne (bien que cette action ne les supprime pas de l'archive, vous pouvez les importer à nouveau le jour suivant).
 - Enfin, le Noyau mémorise l'association d'attache à une archive, même après l'avoir détachée. Une archive est ainsi plus simple et plus rapide à attacher ultérieurement.
- Vous pouvez supprimer l'association en retirant l'attache.

Pour restaurer les données d'une archive attachée, suivez les étapes ci-dessous, en vous reportant aux liens fournis :

REMARQUE : la procédure de restauration depuis une archive attachée suppose que vous disposiez déjà d'une archive constituée de points de récupération cumulés.

- 1 Attachez l'archive.
- 2 Montez le point de récupération contenant les données que vous souhaitez récupérer.
- 3 Restaurez les données en utilisant l'une des méthodes suivantes :
 - Restauration de données, comme un fichier ou un dossier, depuis un point de récupération.
 - Restauration d'un point de récupération complet.
 - Exportation d'un point de récupération vers une machine virtuelle.

Liens connexes

[Attachement d'une archive](#)
[Monter un point de restauration](#)
[Restauration d'un répertoire ou d'un fichier à l'aide de l'Explorateur Windows](#)
[À propos de l'exportation vers des machines virtuelles avec Rapid Recovery](#)
[Sauvegarde Windows](#)
[Description des archives](#)
[Importer une archive](#)
[Exécution d'une restauration BMR à partir d'une archive](#)

Comprendre la restauration Bare Metal Restore pour les machines Windows

Cette section décrit comment faire une restauration BMR d'une machine Windows protégée à partir de machines identiques ou différentes.

Restauration BMR (Bare Metal Restore) pour les machines Windows

Les serveurs, lorsqu'ils fonctionnent comme prévu, effectuent les tâches pour lesquelles ils sont configurés. Ce n'est que lorsqu'ils tombent en panne que les choses changent. Lorsqu'un événement catastrophique survient, rendant le serveur inutilisable, il est nécessaire de prendre des mesures immédiates pour rétablir l'état de fonctionnement complet du serveur.

Rapid Recovery offre la possibilité d'effectuer une restauration BMR des machines Windows ou Linux. La restauration BMR est un processus qui restaure la configuration logicielle complète d'un système. Le terme « bare metal » (sans système d'exploitation) est utilisé parce que l'opération de restauration ne récupère pas uniquement les données du serveur, mais reformate également le disque dur et réinstalle le système d'exploitation et toutes les applications logicielles. Pour exécuter une restauration BMR, vous spécifiez un point de restauration depuis une machine protégée, puis effectuez une restauration vers la machine physique ou virtuelle désignée. Si vous effectuez une restauration vers un volume système, il s'agit d'une restauration BMR. Si vous effectuez une restauration et nécessitez un CD d'amorçage, il s'agit aussi d'une restauration BMR. Les cas pour lesquels vous pouvez choisir une restauration BMR incluent la mise à niveau matérielle ou le remplacement de serveur. Dans les deux cas, vous exécutez une restauration depuis un point de restauration vers le matériel mis à niveau ou remplacé.

Rapid Recovery prend en charge les systèmes d'exploitation Windows 8, 8.1, Windows Server 2012 et 2012 R2 amorcés à partir des partitions FAT32 EFI, ainsi que les volumes Resilient File System (ReFS). Ils sont donc disponibles pour la protection et la restauration.

REMARQUE : la restauration BMR de la configuration des disques d'espace de stockage (une fonctionnalité de Windows 8.1) n'est pas prise en charge dans cette version. Actuellement, seules la restauration complète et la restauration BMR sont prises en charge, car une limitation de pilote existe avec ReFS, la restauration est donc effectuée en mode utilisateur, exportation de VM, etc. Si un Core protège au moins un volume agent qui contient le système de fichiers ReFS, il doit être installé sur une machine Windows 8, Windows 8.1, Windows Server 2012 ou Windows Server 2012 R2, car ces systèmes d'exploitation fournissent le support natif de ReFS. Autrement, la fonctionnalité est limitée, et les opérations qui impliquent le montage d'une image de volume ne fonctionnent pas. La console Core Rapid Recovery affiche des messages d'erreur correspondants dans ces cas-là.

Seuls les systèmes d'exploitation Linux pris en charge sont disponibles pour la protection ou la restauration. Il s'agit de : Ubuntu®, Red Hat® Enterprise Linux®, CentOS™ et SUSE® Linux Enterprise Server (SLES®). Pour plus d'informations, voir le *Dell Data Protection | Rapid Recovery*.

L'exécution d'une restauration BMR est possible pour les machines physiques ou virtuelles. Un autre avantage de Rapid Recovery est la possibilité d'effectuer une restauration BMR que le matériel soit similaire ou non. L'exécution d'une restauration BMR sur Rapid Recovery sépare le système d'exploitation d'une plate-forme spécifique, ce qui permet d'offrir la portabilité.

Le remplacement du disque dur du système existant ou du serveur en panne par une machine identique est un exemple de restauration BMR pour des matériels similaires.

La restauration d'un système en panne avec un serveur d'un autre fabricant différent ou configuré différemment sont des exemples de restauration BRM pour des matériels différents. Ce processus consiste à créer une image CD d'amorçage, à graver l'image sur un disque, à démarrer le serveur cible à partir de l'image d'amorçage, à se connecter à l'instance de la console de restauration, à adresser les volumes, à lancer la restauration et à surveiller l'exécution du processus. Une fois la restauration BMR terminée, vous pouvez poursuivre la tâche de chargement du système d'exploitation et des applications logicielles sur le serveur restauré, puis définir les paramètres uniques nécessaires à votre configuration.

La restauration BMR est utilisée dans les scénarios de restauration après sinistre, mais également pour migrer des données lors d'une mise à niveau ou d'un remplacement de serveurs.

Exécution d'une restauration complète sur des machines Windows

Pour exécuter une restauration complète sur des machines Windows, suivez les étapes ci-dessous.

- Création d'une image de démarrage Windows. Cette image ISO du CD de démarrage est utilisée pour démarrer le disque de destination, à partir duquel vous pouvez accéder à la console de récupération universelle pour communiquer avec les sauvegardes situées sur le Noyau. Veuillez consulter [Comprendre la création du CD d'amorçage pour les machines Windows](#).
- Si vous avez besoin d'un support physique pour démarrer la machine de destination, vous devrez alors transférer l'image ISO du CD de démarrage sur un support. Veuillez consulter [Transfert de l'image ISO sur CD d'amorçage vers un support](#).
- Dans tous les cas, vous devez charger l'image de démarrage dans le serveur de destination et démarrer le serveur depuis cette image de démarrage. Veuillez consulter [Chargement du CD d'amorçage et démarrage de la machine cible](#).

REMARQUE : cette procédure explique comment utiliser une image de CD de démarrage depuis la boîte de dialogue **Créer un CD de démarrage**. Vous pouvez également effectuer ces étapes depuis l'assistant **Restaurer des machines** sur la page **CD de démarrage**. Vous accédez à cette page lorsque vous spécifiez **Restaurer** pour une machine cible quelconque utilisant un CD de démarrage, sur la page **Destination** de l'assistant. Pour des instructions étape par étape sur la façon d'utiliser une image de démarrage Windows depuis l'assistant **Restaurer des machines** dans le cadre d'une restauration complète, veuillez consulter [À propos de la restauration BMR effectuée à l'aide de l'Assistant Restaurer une machine](#).

- Exécution d'une restauration complète pour Windows. Une fois la machine de destination démarrée depuis le CD de démarrage, vous pouvez lancer la procédure de restauration complète. Veuillez consulter [Utilisation de l'Universal Recovery Console pour une restauration BMR](#). Elle comprend les opérations suivantes :
 - L'initialisation d'une restauration depuis un point de récupération situé sur le Noyau. Veuillez consulter [Sélection d'un point de restauration et lancement d'une restauration BMR](#).
 - L'établissement de la topologie des volumes. Veuillez consulter [À propos de l'adressage des volumes pour une restauration BMR \(Bare Metal Restore\)](#).
 - Si vous restaurez sur un matériel différent et que les pilotes réseau et stockage nécessaires ne sont pas présents sur le CD de démarrage, vous aurez peut-être besoin de charger les pilotes depuis un appareil multimédia portable. Pour plus d'informations, veuillez consulter [Chargement des pilotes à l'aide de Universal Recovery Console](#).

- Exécution d'une restauration complète depuis l'assistant Restauration de machines. Les procédures nécessaires à l'utilisation d'une image de démarrage Windows et au lancement de la restauration complète, y compris l'ensemble des sous-opérations, peuvent également être effectuées depuis l'assistant Restauration de machines. Pour plus d'informations sur la façon de lancer l'assistant, veuillez vous reporter aux étapes 1 à 5 de [À propos de la restauration de volumes à partir d'un point de restauration](#), puis consulter [À propos de la restauration BMR effectuée à l'aide de l'Assistant Restaurer une machine](#).
- Vérification d'une restauration complète. Après avoir lancé la procédure de restauration complète, vous pouvez vérifier et surveiller sa progression. Veuillez consulter [Vérification d'une restauration bare metal restore](#).
 - Vous pouvez surveiller la progression de votre restauration. Veuillez consulter [Affichage de l'avancement de la restauration](#).
 - Une fois la procédure terminée, vous pouvez démarrer le serveur restauré. Veuillez consulter [Démarrage d'un serveur cible restauré](#)
 - Dépannage de la procédure de restauration complète. Veuillez consulter [Résolution des problèmes de connexion à Universal Recovery Console](#) et [Réparation des problèmes d'amorçage](#).

Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows

Pour pouvoir démarrer une restauration BMR pour une machine Windows, vous devez vérifier que les conditions et critères suivants existent et sont respectés :

- Unité de traitement (CPU) de 64 bits. Le CD de démarrage de Rapid Recovery inclut le système d'exploitation Win PE 5.1. Les restaurations BMR Rapid Recovery ne sont pas compatibles avec les unités de traitement x86. Une restauration BMR peut uniquement être exécutée sur une unité de traitement 64 bits.

❗ REMARQUE : cette exigence est une nouveauté de la version 6.0 .

- Sauvegardes de la machine que vous souhaitez restaurer. Vous devez disposer d'un Core Rapid Recovery en état de fonctionnement et contenant les points de restauration du serveur protégé à restaurer.
- Matériel à restaurer (nouveau ou ancien, similaire ou non) La machine cible doit satisfaire aux exigences d'installation d'un agent. Pour obtenir de plus amples informations, voir le guide d'installation et de mise à niveau de *Dell Data Protection | Rapid Recovery*.
- Support de l'image et logiciel. Vous devez disposer d'un CD ou d'un DVD vierge, ainsi que d'un logiciel de gravure de disque ou d'un logiciel permettant de créer une image ISO. Si vous gérez les machines à distance à l'aide d'un logiciel de gestion de réseau virtuel tel que UltraVNC, vous devez disposer de VNC Viewer.
- Pilotes de stockage et pilotes de carte réseau compatibles. Si vous effectuez la restauration sur un matériel différent, vous devez disposer des pilotes de stockage et des pilotes de carte réseau compatibles (pilotes RAID, AHCI et de jeu de puces du système d'exploitation cible, selon les cas).
- Espace de stockage et partitions, selon les cas. Assurez-vous de disposer de suffisamment d'espace sur le disque dur pour créer des partitions de destination sur la machine cible devant contenir les volumes source. Toute partition de destination doit être au minimum aussi grande que la partition source d'origine.
- Partitions compatibles. Les systèmes d'exploitation Windows 8, Windows 8.1, Windows 10, Windows Server 2012 et Windows Server 2012 R2 démarrés à partir de partitions FAT32 EFI sont disponibles pour la protection ou la restauration, ainsi que les volumes ReFS (Resilient File System). Les partitions UEFI sont traitées comme simples volumes FAT32. Les transferts incrémentiels sont entièrement pris en charge et protégés. Rapid Recovery prend en charge les systèmes UEFI pour la restauration BMR, incluant des disques à partitionnement automatique GPT.

À propos de la restauration BMR effectuée à l'aide de l'Assistant Restaurer une machine

La gestion d'une image d'amorçage Windows via l'Assistant comprend les opérations suivantes :

- Lancement de la création du CD d'amorçage.
- Définition du chemin de l'image du Core.
- Sélection de l'environnement de restauration adapté au matériel sur lequel vous souhaitez effectuer la restauration.
- Si vous le souhaitez, définition des paramètres de connexion de l'agent restauré pour utiliser le réseau ou UltraVNC.
- Si vous le souhaitez, injection des pilotes de matériel à restaurer.
- Si vous le souhaitez, transfert de l'image d'amorçage vers le média physique.
- Amorçage de la machine pour laquelle vous souhaitez restaurer les données depuis le CD d'amorçage.
- Connexion à l'Universal Recovery Console.
- Adressage de volumes.

- Initiation de la restauration BMR (Bare Metal Restore) à partir du point de restauration sélectionné sur le Core.

REMARQUE : ce processus explique comment gérer une image de CD d'amorçage depuis l'Assistant Restaurer une machine dans le cadre du processus d'exécution d'une restauration BMR à l'aide de l'Assistant. Vous pouvez également gérer une image d'amorçage depuis la boîte de dialogue Créer un CD d'amorçage. Pour plus d'informations sur la gestion d'une image de CD d'amorçage en dehors de l'assistant de restauration de machine, voir [Comprendre la création du CD d'amorçage pour les machines Windows](#).

Exécution d'une restauration BMR avec l'Assistant Restaurer une machine

Vous pouvez utiliser l'Assistant Restauration pour créer un CD d'amorçage et effectuer une restauration BMR.

Avant d'effectuer une restauration BMR, voir [Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows](#) ou [Prérequis pour l'exécution d'une restauration BMR pour une machine Linux](#), selon le cas. Si vous démarrez votre BMR pour une machine Windows depuis la console Core, voir [Exécution d'une restauration complète sur des machines Windows](#).

Le logiciel Agent doit être installé sur la machine protégée et doit aussi avoir des points de restauration depuis lesquels vous pouvez effectuer l'opération de restauration.

- Pour restaurer un volume sur une machine protégée, naviguez jusqu'à la console Core, puis cliquez sur **Restaurer** dans la barre des boutons Rapid Recovery.
L'assistant Restaurer une machine s'affiche.
- Sur la page Machines, sélectionnez la machine protégée à restaurer, puis cliquez sur **Suivant**.
La page points de restauration s'affiche.
- Sélectionnez le point de restauration que vous voulez utiliser pour restaurer la machine.
 - De plus, si vous souhaitez limiter le nombre de points de restauration qui s'affichent, filtrez les résultats par volumes (s'ils sont définis) ou par date de création de point de restauration. Vous pouvez également rechercher un point de restauration spécifique.
- Cliquez sur **Suivant**.
- Sur la page Destination, sélectionnez **Restaurer sur n'importe quelle machine cible à l'aide d'un CD d'amorçage**.
 - Si vous n'avez pas encore chargé un CD d'amorçage sur la machine à restaurer, cliquez sur **Suivant**, puis passez à l'étape 6.
 - Si vous avez déjà chargé un CD d'amorçage sur la machine cible de la BMR, sélectionnez **J'ai déjà un CD d'amorçage en cours d'exécution sur la machine cible**, cliquez sur **Suivant**, puis passez à l'étape 16.
- Sur la page CD d'amorçage, dans la zone de texte Chemin de sortie, entrez le chemin où doit être stockée l'image ISO du CD d'amorçage.

REMARQUE : si le disque partagé sur lequel vous souhaitez stocker l'image possède un espace disque insuffisant, vous pouvez créer un disque dans le chemin ; par exemple, F:\filename.iso.

REMARQUE : l'extension du fichier doit être .iso. Lorsque vous spécifiez le chemin, n'utilisez que des caractéristiques alphanumériques, des tirets, des barres obliques inverses (uniquement pour séparer les composantes du chemin), ou des points (uniquement pour séparer les noms d'hôte et les domaines). Les lettres a à z sont sensibles à la casse. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.

- Si vous le désirez, pour configurer les paramètres réseau de la machine cible, ou pour ajouter des fonctions UltraVNC, vous pouvez choisir **Afficher les options avancées** et effectuer les étapes suivantes :
 - Pour établir une connexion réseau avec la cible de la BMR, sélectionnez **Utiliser l'adresse IP suivante**, puis entrez les informations décrites dans le tableau suivant.

Tableau 153. Options de connexion réseau

Option	Description
adresse IP	L'adresse IP de la machine restaurée.
Masque de sous-réseau	Le masque de sous-réseau de la machine restaurée.
Passerelle par défaut	Spécifiez la passerelle par défaut de la machine restaurée.
Serveur DNS	Spécifiez le serveur de nom de domaine de la machine restaurée.

- Si vous avez un compte UltraVNC et souhaitez l'utiliser pour terminer la BMR, sélectionnez **Ajouter UltraVNC**, puis saisissez les informations décrites dans le tableau suivant.

Tableau 154. Identifiants de connexion UltraVNC

Option	Description
Mot de passe	Le mot de passe de votre compte UltraVNC.
Port	Le port que vous souhaitez utiliser pour vous connecter à la cible de la BMR. Le port par défaut est 5900.

8 Cliquez sur **Suivant**.

- 9
- Pour établir une connexion réseau pour la machine restaurée, sélectionnez **Utiliser l'adresse IP suivante** comme il est décrit dans le tableau suivant.
 - Pour définir les informations UltraVNC, sélectionnez **Ajouter UltraVNC** de la manière décrite dans le tableau suivant.
- Utilisez cette option si vous avez besoin d'un accès à distance à la console de restauration. Vous ne pouvez pas vous connecter à l'aide de Microsoft Terminal Services pendant l'utilisation du CD d'amorçage.

Tableau 155. Connexion UltraVNC

Option	Description
Mot de passe	Spécifiez le mot de passe de cette connexion UltraVNC.
Port	Spécifiez le port de cette connexion UltraVNC. Le port par défaut est 5900.

10 Une fois les sélections effectuées sur la page CD d'amorçage, cliquez sur **Suivant**.

- 11 Sur la page Injection de pilote, si vous envisagez de restaurer sur un matériel différent, injectez les contrôleurs de stockage et autres pilotes appropriés pour votre système cible en procédant comme suit :
- Téléchargez les pilotes depuis le site Web du fabricant, puis décompressez-les.
 - Compressez chacun des pilotes dans un fichier .zip en utilisant un utilitaire de compression approprié (par exemple, WinZip).
 - Sur la page Injection de pilote de l'Assistant Restaurer une machine, cliquez sur **Ajouter une archive de pilotes**.
 - Naviguez dans le système de classement des fichiers pour localiser le fichier du pilote compressé, sélectionnez le fichier, puis cliquez sur **Ouvrir**.
 - Répétez l'étape c et l'étape d selon le cas, jusqu'à ce que vous ayez injecté tous les pilotes nécessaires.
- Pour plus d'informations sur l'injection de pilotes, voir [Comprendre l'injection de pilotes dans le CD d'amorçage](#).

REMARQUE : certaines versions de Windows ne sont pas compatibles avec l'injection de pilotes automatique. Si votre système d'exploitation n'est pas compatible, enregistrez manuellement les pilotes sous C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

Rapid Recovery crée l'image ISO du CD d'amorçage.

12 Cliquez sur **Suivant**.

13 Démarrez la machine cible de la BMR, puis effectuez l'une des opérations suivantes :

- Si vous pouvez démarrer la machine cible à partir de l'image ISO du CD d'amorçage, faites-le.
- Si vous ne pouvez pas démarrer la machine cible, copiez l'image ISO sur le support physique (un CD ou un DVD), chargez le disque dans la machine cible, configurez la machine pour qu'elle se charge à partir du CD d'amorçage et redémarrez à partir du CD d'amorçage.

REMARQUE : il peut être nécessaire de modifier les paramètres du BIOS de la machine cible pour que le volume qui se charge en premier soit le CD d'amorçage.

La machine cible, lorsqu'elle est démarrée à partir du CD d'amorçage, affiche l'interface de la console URC (Universal Recovery Console). Cet environnement est utilisé pour restaurer le disque système ou les volumes sélectionnés directement depuis le Core Rapid Recovery. Notez l'adresse IP et les données d'identification de la clé d'authentification dans la console URC, qui s'actualisent chaque fois que vous effectuez un démarrage à partir du CD d'amorçage.

14 Dans la page Connexion de l'Assistant Restaurer une machine de la console Core, entrez les informations d'authentification depuis l'instance URC de la machine à restaurer comme suit :

Tableau 156. Options d'authentification

Option	Description
Adresse IP	L'adresse IP fournie dans l'URC de la machine cible.
Clé d'authentification	La clé d'authentification fournie dans l'URC de la machine cible.

15 Cliquez sur **Suivant**.

16 Dans la page Adressage des disques, si vous souhaitez adresser les volumes manuellement, passez à l'étape 10. Si vous souhaitez adresser les volumes automatiquement, effectuez les étapes suivantes :

- Dans le menu déroulant Mappage des volumes, sélectionnez **Automatique**.
- Dans la liste des volumes, assurez-vous que les volumes à restaurer sont sélectionnés. Tous les volumes sont sélectionnés par défaut.

Si vous ne souhaitez pas restaurer un volume apparaissant dans la liste, désélectionnez l'option.

REMARQUE : vous devez sélectionner au moins un volume pour effectuer la restauration.

- Sur le côté droit, sélectionnez le disque de destination de la restauration.
- Cliquez sur **Suivant**.
- Sur la page reprenant l'adressage des disques, vérifiez les paramètres des actions de restauration que vous avez sélectionnées.
- Accédez à l'étape 18.

17 Pour adresser des volumes manuellement, dans la page Adressage des disques, effectuez les étapes suivantes :

- Dans le menu déroulant Mappage des volumes, sélectionnez **Manuel**.
- Dans la colonne Destination, sélectionnez un volume de destination que vous souhaitez restaurer. Si vous ne souhaitez pas restaurer un volume apparaissant dans la liste, vous pouvez également désélectionner l'option.

REMARQUE : vous devez sélectionner au moins un volume pour effectuer la restauration.

18 Cliquez sur **Terminer**.

PRÉCAUTION : toutes les partitions et données existantes du lecteur cible seront définitivement supprimées, puis remplacées par le contenu du point de restauration sélectionné, c'est-à-dire le système d'exploitation et toutes les données.

19 Si les volumes à restaurer contiennent des bases de données SQL ou Microsoft Exchange et que vous exécutez une restauration Live, sur la page Démontez les bases de données, un message demande de les démonter. Si vous voulez remonter ces bases de données après la fin de la restauration, vous pouvez également sélectionner **Remonter automatiquement toutes les bases de données après la restauration du point de restauration**.

20 Cliquez sur **Restaurer**.

21 Dans le message d'état, cliquez sur **OK** pour confirmer que le processus de restauration a commencé.

La restauration démarre. Vous pouvez surveiller l'avancement dans la page Événements. Pour plus d'informations, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Comprendre la création du CD d'amorçage pour les machines Windows

Une restauration BMR nécessite une image d'amorçage, communément appelée CD d'amorçage, que vous créez en en définissant les paramètres dans la console Core Rapid Recovery. Cette image est adaptée à vos besoins spécifiques. Vous allez utiliser l'image pour démarrer la machine Windows de destination. En fonction des caractéristiques de l'environnement, il peut être nécessaire de transférer l'image vers un support physique, comme un CD ou un DVD. Vous devez ensuite charger virtuellement ou physiquement l'image d'amorçage, et démarrer le serveur Windows à partir de celle-ci.

La première étape d'une restauration BMR pour une machine Windows consiste à créer le fichier du CD d'amorçage dans la console Core Rapid Recovery. Il s'agit d'une image ISO amorçable qui contient l'interface de l'Universal Recovery Console (URC) Rapid Recovery, un environnement utilisé pour restaurer le disque système ou le serveur dans son intégralité directement depuis le Core Rapid Recovery.

L'image ISO sur CD d'amorçage qui est créée est personnalisée pour la machine en cours de restauration ; elle contient donc les pilotes de réseau et de stockage de masse correspondants. Si vous pensez effectuer la restauration sur un matériel différent de celui de la machine sur laquelle le point de restauration a été généré, vous devez inclure le contrôleur de stockage et les autres pilotes dans le CD d'amorçage. Pour plus d'informations sur l'injection de ces pilotes dans le CD d'amorçage, voir [Comprendre l'injection de pilotes dans un CD d'amorçage](#).

Comprendre l'injection de pilotes dans un CD d'amorçage

L'image du CD d'amorçage nécessite des pilotes de stockage qui reconnaissent les disques du serveur, et des pilotes de carte réseau capables de communiquer avec le Core Rapid Recovery en utilisant le réseau.

Un ensemble générique comportant des pilotes de carte réseau et un contrôleur de stockage Windows 8.1 x64 est inclus automatiquement lorsque vous générez un CD d'amorçage pour Windows. Cela satisfait les exigences des nouveaux systèmes Dell. Les systèmes d'autres fabricants ou d'anciens systèmes Dell peuvent nécessiter d'injecter un contrôleur de stockage ou des pilotes de carte réseau lors de la création du CD d'amorçage. Si vous constatez que le CD d'amorçage que vous avez créé ne contient pas les pilotes nécessaires pour effectuer la restauration, vous pouvez également charger les pilotes sur la machine cible à l'aide de la console URC. Pour plus d'informations, voir [Chargement des pilotes à l'aide de Universal Recovery Console](#).

Lorsque vous créez le CD d'amorçage, l'injection de pilotes est utilisée pour faciliter les opérations entre la console de restauration, la carte réseau et le stockage sur le serveur cible.

Les données restaurées à partir du point de restauration comprennent les pilotes du matériel préalablement installé. Si vous effectuez une restauration BMR sur du matériel différent, vous devez injecter les pilotes de contrôle du stockage dans le système d'exploitation à restaurer à l'aide de la console URC après que les données ont été restaurées sur le disque. Cela permet au système d'exploitation restauré de s'amorcer en utilisant le nouveau matériel. Après que le système d'exploitation a été amorcé après la restauration, vous pouvez télécharger et installer tous les pilotes manquants dont a besoin le système d'exploitation pour interagir avec le nouveau matériel.

Création d'une image ISO sur CD d'amorçage

Un CD d'amorçage est le terme utilisé par Rapid Recovery pour désigner l'emplacement de stockage portable de l'image ISO image réservé pour l'exécution d'une restauration bare metal restore (BMR). L'image comprend l'Universal Recovery Console (URC) Rapid Recovery.

Pour effectuer une restauration BMR sur une machine, vous devez démarrer la machine sur le CD d'amorçage, cette opération lance la console URC. La console URC rend possible la connexion de la cible de la BMR à l'emplacement du point de restauration à utiliser pour terminer la restauration.

- 1 À partir de la Rapid Recovery Core Console où le serveur à restaurer est protégé, dans la barre d'icônes, cliquez sur le menu Plus, puis cliquez sur **CD d'amorçage**.
- 2 Sur la page CD d'amorçage, cliquez sur **Créer un CD d'amorçage**.
La boîte de dialogue Créer un CD d'amorçage s'affiche.
- 3 Dans la boîte de dialogue Créer un CD d'amorçage, dans la zone de texte **Chemin de sortie**, entrez l'emplacement où vous souhaitez stocker l'image ISO du CD d'amorçage.

REMARQUE : l'extension du fichier doit être **.iso**. Lorsque vous spécifiez le chemin, n'utilisez que des caractéristiques alphanumériques, des tirets, des barres obliques inverses (uniquement pour séparer les composantes du chemin), ou des points (uniquement pour séparer les noms d'hôte et les domaines). Les lettres a à z ne sont pas sensibles à la casse. N'utilisez pas d'espaces. Aucun autre symbole ou caractère de ponctuation n'est autorisé.

- 4 Sous Options de connexion, effectuez l'une des opérations suivantes :
 - pour obtenir l'adresse IP de façon dynamique en utilisant Dynamic Host Configuration Protocol (DHCP), sélectionnez **Obtenir une adresse IP automatiquement**.
 - Pour spécifier une adresse IP statique pour la console URC, sélectionnez **Utiliser l'adresse IP suivante**, puis entrez les informations suivantes :
 - adresse IP
 - Masque de sous-réseau

- Passerelle par défaut
- Serveur DNS

REMARQUE : vous devez impérativement renseigner ces champs.

- 5 Si vous avez besoin d'un accès distant à la recovery console, et que vous avez installé UltraVNC, sous Options UltraVNC, procédez comme suit :

REMARQUE : UltraVNC vous permet de gérer la console URC à distance lorsqu'elle est en cours d'utilisation. Vous ne pouvez pas vous connecter à l'aide de Microsoft Terminal Services pendant l'utilisation du CD d'amorçage.

- Sélectionnez **Ajouter UltraVNC**.
- Entrez votre **mot de passe UltraVNC**.
- Entrez le **port UltraVNC**. Le port par défaut est 5900.

REMARQUE : les options UltraVNC sont disponibles uniquement si vous avez déjà installé UltraVNC. Pour que ces options deviennent disponibles, accédez à <http://www.uvnc.com/downloads/ultravnc/> pour télécharger UltraVNC version 1.0.9.1 ou ultérieure pour l'architecture x64. Installez-le et enregistrez le fichier winvnc.exe dans C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\.

- 6 Si vous envisagez de restaurer sur un matériel différent, injectez le contrôleur de stockage et autres pilotes appropriés pour votre système cible en procédant comme suit :

REMARQUE : certaines versions de Windows ne sont pas compatibles avec l'injection de pilotes automatique. Si votre système d'exploitation n'est pas compatible, enregistrez manuellement les pilotes sous C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

- Téléchargez les pilotes depuis le site Web du fabricant, puis décompressez-les.
- Compressez chacun des pilotes dans un fichier .zip en utilisant un utilitaire de compression approprié (par exemple, WinZip).
- Dans la boîte de dialogue Créer un CD d'amorçage, dans la section Pilotes, cliquez sur **Ajouter une archive de pilotes**.
- Naviguez dans le système de classement des fichiers pour localiser le fichier du pilote compressé, sélectionnez le fichier, puis cliquez sur **Ouvrir**.
Le fichier de pilote s'affiche dans le volet Pilotes de la boîte de dialogue Créer un CD d'amorçage.
- Répétez l'étape c et l'étape d selon le cas, jusqu'à ce que vous ayez ajouté tous les pilotes nécessaires.
- Dans le volet Pilotes, sélectionnez les pilotes à injecter.

Pour plus d'informations sur l'injection de pilotes, voir [Comprendre l'injection de pilotes dans un CD d'amorçage](#).

- 7 Cliquez sur **Créer un CD d'amorçage**.

Rapid Recovery crée le CD d'amorçage et l'enregistre en utilisant le nom du fichier que vous avez fourni.

- 8 Pour surveiller l'avancement de cette tâche, accédez à la barre d'icônes et cliquez sur l'icône Événements.

Pour plus d'informations sur la surveillance des événements Rapid Recovery, voir [Affichage des événements à l'aide des tâches, des alertes et du journal](#).

Lorsque la création de l'image ISO est terminée, un enregistrement de l'image s'affiche dans la page des CD d'amorçage, vous pouvez y accéder à partir du menu Plus de la barre d'icônes.

Pour accéder à l'image ISO, vous pouvez naviguer jusqu'au chemin de sortie que vous avez indiqué ou cliquez sur le lien de la page CD d'amorçage pour enregistrer l'image dans un emplacement à partir duquel vous pourrez ensuite la charger sur le nouveau système, par exemple, un lecteur de réseau.

Transfert de l'image ISO sur CD d'amorçage vers un support

Lorsque vous créez le fichier du CD d'amorçage, celui-ci est stocké en tant qu'image ISO dans le chemin que vous indiquez. Vous devez être capable de monter cette image comme lecteur sur le serveur sur lequel vous effectuez la restauration BMR.

Vous pouvez graver l'image ISO d'amorçage sur un CD (disque compact) ou un DVD (disque vidéo numérique), accessible lors du démarrage du système.

Lorsque vous démarrez la machine depuis le CD d'amorçage, la console URC (Universal Recovery Console) démarre automatiquement.

Si vous effectuez une restauration BMR sur une machine virtuelle, cette étape n'est pas nécessaire. Il suffit de charger l'image ISO sur un disque et de modifier les paramètres de la VM pour qu'elle démarre depuis ce disque.

Chargement du CD d'amorçage et démarrage de la machine cible

Après avoir créé l'image d'amorçage, vous devez amorcer le serveur cible avec le CD d'amorçage nouvellement créé.

Pour vous connecter à la console Core Rapid Recovery ou télécharger d'autres pilotes à l'aide de Chromium, vous devez d'abord charger un contrôleur Ethernet et une carte réseau. Pour en savoir plus, voir [Chargement des pilotes à l'aide de Universal Recovery Console](#).

❗ REMARQUE : si vous avez créé le CD d'amorçage à l'aide de DHCP, vous devez entrer l'adresse IP et le mot de passe.

- 1 Sur le nouveau serveur, chargez l'image du CD d'amorçage depuis l'emplacement approprié, puis démarrez le serveur à partir de l'image du CD d'amorçage pour charger le logiciel Agent Rapid Recovery et Win PE 5.1.
La machine cible affiche un écran Dell bleu avec trois boutons d'icônes dans la partie supérieure.
- 2 Pour ouvrir l'interface utilisateur de l'Universal Recovery Console (URC) Rapid Recovery, cliquez avec le bouton droit sur l'icône Dell en haut de l'écran.
L'adresse IP et mot de passe de la machine s'affichent sous le menu Authentification.

❗ REMARQUE : un nouveau mot de passe temporaire est généré chaque fois que la machine est démarrée avec le CD d'amorçage. Notez l'adresse IP qui s'affiche dans le volet Paramètres des cartes réseau et le mot de passe qui s'affiche dans le volet Authentification. Vous aurez besoin de ces informations ultérieurement au cours du processus de restauration des données pour vous reconnecter à la console.

❗ REMARQUE : si aucune adresse IP n'est indiquée, chargez le contrôleur Ethernet et la carte réseau.

- 3 Si vous souhaitez modifier l'adresse IP, sélectionnez-la et cliquez sur **Modifier**.

❗ REMARQUE : si vous avez spécifié une adresse IP dans la boîte de dialogue Créer un CD d'amorçage, l'Universal Recovery Console l'utilise et l'affiche dans l'écran Paramètres de carte réseau.

La machine est prête à se connecter au Core. Sélectionnez un point de restauration et poursuivez le processus de restauration BMR.

Utilisation de l'Universal Recovery Console pour une restauration BMR

Avant de lancer une restauration BMR pour une machine Windows, les conditions suivantes doivent être remplies :

- Pour restaurer un point de restauration enregistré sur le Core, vous devez disposer du matériel approprié. Pour plus d'informations, voir [Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows](#).
- La machine Windows de destination pour la restauration BMR doit être démarrée à l'aide de l'image d'amorçage (CD d'amorçage). Pour plus d'informations, voir [Comprendre la création du CD d'amorçage pour les machines Windows](#).

Une restauration BMR démarre une machine à l'aide du point de restauration que vous sélectionnez. Le point de restauration comprend les pilotes du matériel précédent. Si vous effectuez une restauration sur du matériel différent, vous devez injecter les pilotes de contrôle du stockage dans le système d'exploitation en cours de restauration à l'aide de la console URC après que les données ont été restaurées sur le disque. Cela permet au système d'exploitation restauré de démarrer en utilisant le nouveau matériel. Une fois le système d'exploitation démarré, vous pouvez télécharger et installer d'autres pilotes requis par le système d'exploitation pour interagir avec le nouveau matériel.

Pour lancer une restauration BMR depuis la Rapid Recovery Core Console, effectuez les tâches suivantes.

- [Sélection d'un point de restauration et lancement d'une restauration BMR](#)
- [À propos de l'adressage des volumes pour une restauration BMR \(Bare Metal Restore\)](#)
- [Chargement des pilotes à l'aide de Universal Recovery Console](#)

Cette tâche est une étape de la [Exécution d'une restauration complète sur des machines Windows](#).

À propos des outils de la console URC

La console URC (Universal Recovery Console) inclut l'accès à des outils qui peuvent vous aider à effectuer une restauration BMR.

Pour trouver les outils suivants, cliquez sur l'icône du milieu en haut de l'écran de démarrage Dell sur une cible BMR démarrée dans la console URC :

- **Far Manager.** Cet outil est semblable à l'Explorateur Windows. Il permet de rechercher des fichiers sur le serveur jusqu'à ce que vous ayez terminé la restauration BMR et d'installer un système d'exploitation doté de sa propre fonction de navigation, comme l'Explorateur Windows.
- **Chromium.** Ce navigateur est la base Open source de Google Chrome™. Il permet de naviguer sur Internet sur un serveur doté d'un contrôleur réseau chargé via la console URC.
- **PuTTY.** Cet outil est un émulateur de terminal Open source. Dans le contexte d'une restauration BMR Rapid Recovery, il vous permet de vous connecter à un périphérique de stockage NAS qui n'inclut aucune interface utilisateur. Cette fonctionnalité peut être nécessaire si vous souhaitez effectuer une restauration à partir d'une archive se trouvant sur un périphérique NAS.
- **Bloc-notes.** Comme dans un système d'exploitation Windows, cet outil permet de saisir des notes non formatées et d'afficher les fichiers journaux.
- **Gestionnaire des tâches.** Comme dans un système d'exploitation Windows, cet outil permet de gérer les processus et de surveiller les performances du serveur lorsque la restauration est en cours.
- **Éditeur du registre.** Comme dans un système d'exploitation Windows, cet outil permet de modifier le registre système de la cible BMR.
- **Invite de commande.** Cet outil vous permet d'exécuter des commandes sur la cible BMR en dehors de la console URC jusqu'à ce que vous installiez une interface utilisateur.

Chargement des pilotes à l'aide de Universal Recovery Console

Cette fonctionnalité permet d'ajouter tous les pilotes non inclus dans l'image ISO, mais qui sont nécessaires à une restauration BMR.

Cette tâche est une étape de la rubrique [Exécution d'une restauration complète sur des machines Windows](#). Elle fait partie du processus [Utilisation de l'Universal Recovery Console pour une restauration BMR](#).

Lorsque vous créez un CD d'amorçage, vous pouvez ajouter les pilotes nécessaires à l'image ISO. Après avoir amorcé la machine cible, vous pouvez également charger les pilotes réseau ou de stockage depuis Universal Recovery Console (URC).

Si vous effectuez la restauration sur un matériel différent, vous devez injecter les pilotes du contrôleur de stockage, RAID, AHCI, de jeux de puces et les autres pilotes s'ils ne sont pas déjà sur le CD d'amorçage. Ces pilotes permettent au système d'exploitation de faire fonctionner correctement tous les périphériques sur le serveur cible après avoir redémarré le système en suivant le processus de restauration.

Suivre une des procédures ci-dessous permet de charger des pilotes en utilisant l'utilitaire URC :

- [Chargement de pilotes dans l'Universal Recovery Console à l'aide d'un média portable](#)
- [Chargement d'un pilote dans la console URC à l'aide de Chromium](#)

Chargement de pilotes dans l'Universal Recovery Console à l'aide d'un média portable

Les tâches suivantes sont les pré-requis de cette procédure.

- [Création d'une image ISO sur CD d'amorçage](#)
- [Transfert de l'image ISO sur CD d'amorçage vers un support](#)
- [Chargement du CD d'amorçage et démarrage de la machine cible](#)

Suivez la procédure suivante pour utiliser un appareil média mobile pour charger les pilotes dans l'Universal Recovery Console (URC).

- 1 Sur une machine connectée à Internet, téléchargez les pilotes pour le serveur depuis le site Web du fabricant, puis décompressez-les.
- 2 Comprimez chacun des pilotes dans un fichier .zip en utilisant un utilitaire de compression approprié (par exemple, WinZip).

- 3 Copiez et enregistrez le fichier .zip des pilotes sur un appareil média mobile, tel qu'un lecteur USB.
- 4 Retirez le support de la machine connectée et insérez-le dans le serveur d'amorçage cible.
- 5 Sur le serveur cible, chargez le CD d'amorçage, puis démarrez la machine.
L'écran d'accueil Dell s'affiche.
- 6 Pour démarrer l'URC, cliquez sur **l'icône Dell**.
La console URC ouvre l'onglet du gestionnaire de pilotes du CD d'amorçage.
- 7 Développez la liste **Autres périphériques**.
Cette liste affiche les pilotes qui sont nécessaires pour le matériel, mais qui ne sont pas inclus sur le CD d'amorçage.
- 8 Faites un clic droit sur un périphérique de la liste, puis cliquez sur **Charger le pilote**.
- 9 Dans la fenêtre du mode Sélectionner le mode de chargement du pilote, sélectionnez l'une des options suivantes :
 - Charger un package de pilote unique (le pilote sera chargé sans vérifier le support du périphérique)
 - Rechercher les paquets de pilote dans un dossier (les pilotes du périphérique sélectionné sont recherchés dans le dossier sélectionné)
- 10 Développez le disque de l'appareil média mobile, sélectionnez le pilote (avec l'extension de fichier .inf), puis cliquez sur **OK**.
Le pilote se charge sur le système d'exploitation sélectionné.
- 11 Dans la fenêtre Infos, cliquez sur **OK** pour confirmer que le pilote est correctement chargé.
- 12 Répétez cette procédure autant de fois que nécessaire pour chaque pilote à charger.

Chargement d'un pilote dans la console URC à l'aide de Chromium

Les tâches suivantes sont les pré-requis de cette procédure.

- [Création d'une image ISO sur CD d'amorçage](#)
- [Transfert de l'image ISO sur CD d'amorçage vers un support](#)
- [Chargement du CD d'amorçage et démarrage de la machine cible](#)

Suivez la procédure suivante pour utiliser le navigateur Chromium, installé sur le CD d'amorçage, pour charger les pilotes lorsque vous êtes sur la console URC.

- 1 Sur le serveur cible, chargez le CD d'amorçage, puis démarrez la machine.
L'écran d'accueil Dell s'affiche.
- 2 Pour démarrer l'URC, cliquez sur **l'icône Dell**.
La console URC ouvre l'onglet du gestionnaire de pilotes du CD d'amorçage.
- 3 Sur la cible BMR, cliquez sur les outils (icône du milieu) situés en haut de l'écran, puis cliquez sur **Chromium**.
- 4 Dans le navigateur Chromium, naviguez jusqu'à un site Web à partir duquel vous pouvez télécharger le pilote nécessaire.
- 5 Téléchargez le ou les pilotes vers l'emplacement de votre choix, comme un dossier local ou un partage de fichiers réseau.
- 6 Développez la liste **Autres périphériques**.
Cette liste affiche les pilotes qui sont nécessaires pour le matériel, mais qui ne sont pas inclus sur le CD d'amorçage.
- 7 Faites un clic droit sur un périphérique de la liste, puis cliquez sur **Charger le pilote**.
- 8 Dans la fenêtre du mode Sélectionner le mode de chargement du pilote, sélectionnez l'une des options suivantes :
 - Charger un package de pilote unique (le pilote est chargé sans vérification du support du périphérique)
 - Rechercher les paquets de pilotes dans un dossier (les pilotes du périphérique sélectionné sont recherchés dans le dossier sélectionné)
- 9 Naviguez jusqu'à l'emplacement où vous avez enregistré le pilote, sélectionnez le pilote, puis cliquez sur **OK**.
Le pilote se charge sur le système d'exploitation sélectionné.
- 10 Dans la fenêtre Infos, cliquez sur **OK** pour confirmer que le pilote est correctement chargé.
- 11 Répétez cette procédure autant de fois que nécessaire pour chaque pilote à charger.

Sélection d'un point de restauration et lancement d'une restauration BMR

Une fois la console URC (Universal Recovery Console) accessible sur la machine cible de la restauration BMR, vous devez sélectionner le point de restauration à restaurer.

Accédez à la console Core pour choisir le point de restauration à charger, et désigner la console de restauration en tant que destination des données restaurées.

REMARQUE : cette étape est obligatoire pour effectuer la restauration BMR sur toutes les machines Windows et facultative pour effectuer la restauration BMR sur les machines Linux.

Cette tâche est une étape de la rubrique [Exécution d'une restauration complète sur des machines Windows](#). Elle fait partie du processus [Utilisation de l'Universal Recovery Console pour une restauration BMR](#).

Si vous effectuez une restauration BMR sur une machine Linux depuis la console Core, cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#).

- 1 Dans la liste des machines protégées de la console Core Rapid Recovery, cliquez sur le nom de la machine protégée à restaurer. La page Synthèse de la machine sélectionnée s'affiche.
- 2 Cliquez sur **Points de restauration**.
- 3 Cliquez sur le menu déroulant en regard du point de restauration à utiliser pour la restauration BMR, puis sur **Restaurer**. L'Assistant Restaurer une machine s'affiche.
- 4 Sélectionnez **Restaurer sur n'importe quelle machine cible avec un CD d'amorçage**.
- 5 Cliquez sur **J'ai déjà un CD d'amorçage en cours d'exécution sur la machine cible**. Les zones de texte d'authentification s'affichent.
- 6 Saisissez les informations concernant la machine à restaurer, tel que décrit dans le tableau suivant.

Tableau 157. Informations sur la machine cible

Boîte de texte	Description
Adresse IP	Adresse IP de la machine à restaurer. Celle-ci est identique à l'adresse IP affichée dans l'URC.
Clé d'authentification	Mot de passe pour se connecter au serveur sélectionné. Celui-ci est identique à la clé d'authentification affichée dans l'URC.

- 7 Cliquez sur **Suivant**.
Si les informations de connexion que vous avez entrées correspondent à celles de l'URC et que le Core et le serveur cible peuvent s'identifier correctement mutuellement sur le réseau, les volumes du point de restauration sélectionné sont chargés, et la page Adressage des disques apparaît. Dans ce cas, la prochaine étape consiste à adresser les volumes.
- 8 Passez à la section [À propos de l'adressage des volumes pour une restauration BMR \(Bare Metal Restore\)](#) pour en savoir plus sur les options d'adressage du disque.

À propos de l'adressage des volumes pour une restauration BMR (Bare Metal Restore)

Une fois connecté à Universal Recovery Console, vous devez adresser les volumes, entre ceux répertoriés dans le point de restauration et ceux existant sur le matériel cible.

Rapid Recovery essaie d'adresser automatiquement les volumes. Si vous acceptez l'adressage par défaut, le disque présent sur la machine de destination est nettoyé et repartitionné, et toutes les données existantes sont supprimées. L'alignement est effectué dans l'ordre selon lequel les volumes sont répertoriés dans le point de restauration, et les volumes sont alloués de façon appropriée aux disques selon leur taille, etc. En supposant que l'espace est suffisamment sur le disque cible, aucun partitionnement n'est nécessaire lorsque l'alignement des disques se fait automatiquement. Un disque peut être utilisé par plusieurs volumes. Si vous adressez manuellement les disques, vous ne pouvez pas utiliser le même disque deux fois.

Pour l'adressage manuel, la nouvelle machine doit être formatée correctement préalablement à la restauration. La machine de destination doit disposer d'une partition distincte pour chacun des volumes du point de restauration, y compris le volume réservé au système. Pour plus d'informations, voir [Utilisation de l'Universal Recovery Console pour une restauration BMR](#).

Suivez la procédure de l'une des options d'adressage de disque ci-après :

- [Adressage automatique des disques pour une restauration BMR](#)
- [Adressage manuel des disques pour une restauration BMR](#)

⚠ PRÉCAUTION : bien que Rapid Recovery prenne en charge les partitions FAT32 et ReFS, actuellement, seules la restauration complète et la restauration BMR sont prises en charge, car une limitation de pilote existe pour ReFS. La restauration est donc effectuée en mode utilisateur, exportation de VM, etc. Si un Core protège au moins un volume agent contenant le système de fichiers ReFS, il doit être installé sur une machine Windows 8, Windows 8.1, Windows 10, Windows Server 2012 ou Windows Server 2012 R2 intégrant le support natif de ReFS. À défaut, la fonctionnalité est limitée, et les opérations impliquant le montage d'une image de volume ne fonctionnent pas. La console Core Rapid Recovery affiche alors les messages d'erreur applicables en de telles circonstances.

⚠ PRÉCAUTION : La restauration BMR de la configuration des disques d'espaces de stockage (fonctionnalité de Windows 8.1) n'est pas prise en charge. Pour obtenir de plus amples informations, voir le guide d'installation et de mise à niveau *Dell Data Protection | Rapid Recovery*.

Cette tâche est une étape de la [Exécution d'une restauration complète sur des machines Windows](#). Elle fait partie du processus [Utilisation de l'Universal Recovery Console pour une restauration BMR](#).

Si vous effectuez une restauration BMR pour une machine Linux depuis la console Core, cette tâche constitue également une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Lancement d'une restauration Bare Metal Restore pour Linux](#).

Adressage automatique des disques pour une restauration BMR

Cette procédure permet d'adresser automatiquement des disques au cours d'une restauration BMR à l'aide de l'Assistant Restauration d'une machine.

Suivez les étapes de la procédure suivante pour sélectionner automatiquement les volumes à récupérer et leur emplacement de restauration.

- 1 Sur la page Adressage des disques de l'Assistant Restauration d'une machine, en regard de Mappage des volumes, sélectionnez **Automatique** dans le menu déroulant.
- 2 Dans le tableau de gauche, vérifiez que les volumes appropriés sont répertoriés et sélectionnés.

❗ REMARQUE : D'une manière générale, pour une restauration BMR, vous devez restaurer, au minimum, le volume réservé au système et le volume système (généralement, mais pas toujours, le volume C:\). Vous devez sélectionner au moins un volume pour effectuer une restauration BMR.

- 3 Dans le tableau de droite, sélectionnez le ou les disques auxquels vous souhaitez adresser les volumes sur la machine cible.
- 4 Cliquez sur **Suivant**.
- 5 Sur la page Aperçu de l'adressage de disques, vérifiez l'adressage des volumes de point de récupération et le volume de destination pour la restauration.
- 6 Pour commencer la restauration, cliquez sur **Terminer**.

 **PRÉCAUTION :** Si vous sélectionnez Démarrer la restauration, toutes les partitions et données existantes du lecteur cible sont définitivement supprimées, puis remplacées par le contenu du point de restauration sélectionné, y compris le système d'exploitation et toutes les données.

Adressage manuel des disques pour une restauration BMR

Cette procédure explique comment désigner l'emplacement de stockage des disques dans la machine restaurée.

Pour manuellement adresser les disques, vous devez d'abord utiliser DiskPart sur la ligne de commande de la machine cible de la BMR pour créer et formater les volumes cibles. Pour plus d'informations, voir [Options de ligne de commande de DiskPart \(Standard 7 SP1\)](#) sur le Microsoft Developer Network.

Suivez les étapes de la procédure suivante pour sélectionner manuellement les volumes à récupérer et leur emplacement de restauration.

- 1 Dans la page Adressage des disques de l'Assistant Restaurer une machine, près de Mappage des volumes, sélectionnez **Manuel** dans le menu déroulant.

 **REMARQUE :** Si aucun volume n'existe sur le disque de la machine sur laquelle vous exécutez une restauration bare metal restore (BMR), vous ne pouvez pas voir cette option ni adresser manuellement les volumes.

- 2 Dans la zone Adressage des volumes, vérifiez que le volume source est sélectionné et que les volumes appropriés sont répertoriés sous celui-ci et qu'ils sont sélectionnés.
- 3 Dans Destination, dans le menu déroulant, sélectionnez la destination appropriée, c'est-à-dire le volume cible sur lequel la restauration BMR du point de restauration doit être effectuée, puis cliquez sur **Restaurer**.
- 4 Dans la boîte de dialogue de confirmation, vérifiez l'adressage de la source du point de restauration et du volume de destination à utiliser pour la restauration.
- 5 Pour commencer la restauration, cliquez sur **Commencer la restauration**.

 **PRÉCAUTION :** si vous sélectionnez Commencer la restauration, toutes les partitions et données existantes sur le disque cible sont supprimées définitivement et remplacées par le contenu du point de restauration sélectionné, c'est-à-dire le système d'exploitation et toutes les données.

Exécution d'une restauration BMR à partir d'une archive

Rapid Recovery permet de restaurer une machine sans système d'exploitation à l'aide d'un point de restauration archivé.

Les tâches suivantes sont les pré-requis de cette procédure.

- [Création d'une image ISO sur CD d'amorçage](#)
- [Chargement du CD d'amorçage et démarrage de la machine cible](#)

À partir de la console URC (Universal Recovery Console), vous pouvez accéder au Core Rapid Recovery et récupérer un point de restauration pour une restauration. Vous pouvez également opter pour restaurer votre machine sans système d'exploitation à partir d'un point de restauration stocké dans une archive. La console URC vous permet d'atteindre cette archive, qu'elle se trouve sur un lecteur local, un partage réseau ou un compte cloud.

- 1 Dans la console URC, cliquez sur l'onglet **Restauration à partir d'une archive**.
- 2 Dans la liste déroulante **Type d'emplacement**, sélectionnez l'emplacement de votre archive. Vous pouvez choisir parmi les options ci-dessous.
 - Local
 - Réseau
 - Cloud
- 3 Saisissez les informations d'identification décrites dans le tableau suivant, selon le type d'emplacement que vous avez choisi.

Tableau 158. Options concernant les informations d'identification selon le type d'emplacement

Type d'emplacement	Option	Description
Local	Chemin local	Emplacement actuel de l'archive.
Réseau	Chemin réseau	Emplacement actuel de l'archive.
	Utilisateur	Nom d'utilisateur pour accéder au partage réseau.
	Mot de passe	Mot de passe pour accéder au partage réseau.
Cloud	Type de cloud	Fournisseur de votre emplacement de stockage cloud. Sélectionnez l'une des options suivantes : • Microsoft Azure • Amazon™ S3 • OpenStack • Fichiers Rackspace® Cloud

- 4 Si vous avez sélectionné un type de cloud, fournissez les informations d'identification qui s'appliquent à votre fournisseur cloud.
 - Pour Microsoft Azure, procédez comme suit :
 - 1 Saisissez les informations d'identification suivantes :
 - Nom du compte de stockage
 - Clé d'accès
 - 2 Pour le nom du conteneur, sélectionnez un conteneur dans la liste déroulante.
 - 3 Pour le chemin cloud, sélectionnez le chemin vers l'archive dans la liste déroulante.
 - Pour Amazon™ S3, suivez les étapes ci-dessous.
 - 1 Saisissez les informations d'identification suivantes :
 - Clé d'accès
 - Clé secrète
 - 2 Pour le nom du conteneur, sélectionnez un conteneur dans la liste déroulante.
 - 3 Pour le chemin cloud, sélectionnez le chemin vers l'archive dans la liste déroulante.
 - Pour les comptes optimisés par OpenStack ou Rackspace Cloud Files, procédez comme suit :
 - 1 Saisissez les informations suivantes :
 - Région
 - Utilisateur
 - 2 Sélectionnez l'une des options suivantes :
 - Mot de passe
 - Clé API
 - 3 Dans la zone de texte, saisissez les informations en fonction de votre sélection à l'étape C.
 - 4 Saisissez les informations suivantes :
 - ID du propriétaire
 - URL d'authentification
 - Nom du conteneur
 - Chemin vers le cloud
- 5 Cliquez sur **Suivant**.
 - 6 Sur la page **Machines**, sélectionnez la machine que vous souhaitez restaurer, puis cliquez sur **Suivant**.
 - 7 Sur la page **Points de restauration**, sélectionnez le point de restauration que vous souhaitez utiliser pour restaurer la machine, puis cliquez sur **Suivant**.
 - 8 Sur la page **Mappage**, sélectionnez l'une des options suivantes, puis suivez les étapes correspondantes :

- Dans la liste déroulante **Mappage des volumes**, sélectionnez **Automatique**.

1 Dans le tableau de gauche, vérifiez que les volumes appropriés sont répertoriés et sélectionnés.

REMARQUE : D'une manière générale, pour une restauration BMR, vous devez restaurer, au minimum, le volume réservé au système et le volume système (généralement, mais pas toujours, le volume C:\). Vous devez sélectionner au moins un volume pour effectuer une restauration BMR.

2 Dans le tableau de droite, sélectionnez le ou les disques auxquels vous souhaitez adresser les volumes sur la machine cible.

- Dans la liste déroulante **Mappage des volumes**, sélectionnez **Manuel**.

REMARQUE : Pour adresser des disques manuellement, vous devez d'abord utiliser DiskPart sur la ligne de commande pour créer et formater les volumes cibles. Pour plus d'informations, voir [Options de ligne de commande de DiskPart \(Standard 7 SP1\)](#) sur le Microsoft Developer Network.

REMARQUE : Si aucun volume n'existe sur le disque de la machine sur laquelle vous exécutez une restauration bare metal restore (BMR), vous ne pouvez pas voir cette option ni adresser manuellement les volumes.

- Sous **Volumes de destination**, dans le menu déroulant, sélectionnez le volume cible approprié pour chaque volume dans le point de restauration.

9 Dans la zone de texte **Chemin de mappage de montage**, saisissez une destination pour le stockage temporaire des fichiers de mappage.

L'emplacement par défaut est le suivant : X:\ProgramData\AppRecovery\IndexEntriesMaps.

REMARQUE : Pour vous assurer que votre destination dispose d'un espace libre suffisant, divisez la capacité totale du volume de montage par 1,024. Par exemple, à l'aide de la formule (Mount volume total capacity) / 1024 = Free space, puis 1 TB / 1024 = 1 GB.

10 Cliquez sur **Restaurer**.

La console URC mappe les volumes vers le ou les nouveaux disques.

11 Cliquez sur **Restaurer**.

La console URC restaure les données sur la machine cible. Vous pouvez suivre l'avancement dans l'onglet **Progression de la restauration**.

12 Une fois la restauration terminée, retirez le CD d'amorçage.

13 Pour amorcer la machine cible BMR dans Windows, redémarrez la machine.

Chargement de pilotes sur le système d'exploitation

Cette procédure explique comment charger les pilotes sur le système d'exploitation de la cible de la bare metal restore (BMR).

Pour injecter des pilotes sur le système d'exploitation, vous avez déjà terminé les tâches suivantes :

- Vous avez créé un CD d'amorçage à l'aide de Boot CD Builder dans la console Core Rapid Recovery. Pour plus d'informations, voir [Création d'une image ISO sur CD d'amorçage](#).
- Vous avez chargé le CD d'amorçage dans la cible de la BMR. Pour plus d'informations, voir [Chargement du CD d'amorçage et démarrage de la machine cible](#).
- Vous avez chargé les pilotes nécessaires ou les contrôleurs de stockage et de mise en réseau. Pour plus d'informations, voir [Chargement des pilotes à l'aide de Universal Recovery Console](#).
- Vous avez effectué une restauration à l'aide de l'Assistant Restaurer une machine de la console Core Rapid Recovery ou une archive de la console Universal Recovery Console (URC). Pour plus d'informations, voir [Exécution d'une restauration BMR avec l'Assistant Restaurer une machine](#) et [Exécution d'une restauration BMR à partir d'une archive](#).

Une fois avoir effectué une restauration, le processus n'est pas terminé jusqu'à ce que vous injectiez les pilotes pour le système d'exploitation de la cible de la restauration BMR. Cette tâche s'ajoute au chargement de pilotes dans la console URC.

1 Après avoir cliqué sur Restaurer dans la procédure BMR de votre choix (voir prérequis), cliquez sur l'onglet **Gestion des pilotes Windows**.

2 Dans la liste déroulante, sélectionnez un système d'exploitation.

La console URC recherche les pilotes disponibles.

- 3 Pour charger des pilotes supplémentaires, cliquez sur **Forcer le chargement**.
- 4 Naviguez dans le système de classement des fichiers pour localiser le fichier du pilote compressé, puis sélectionnez le fichier.
- 5 Cliquez sur **OK**.
La console URC charge le pilote dans le système d'exploitation que vous avez sélectionné.
- 6 Répétez les **étapes 3 à 5** pour chaque pilote supplémentaire à charger.
- 7 Redémarrez la machine cible de la BMR.
La BMR est terminée. Si vous rencontrez un problème lors du redémarrage, voir [Réparation des problèmes d'amorçage](#).

Effectuer une restauration Bare Metal Restore de machines Linux

Dans Rapid Recovery, vous pouvez effectuer une restauration BMR pour une machine Linux, y compris une restauration du volume système. Lorsque vous restaurez une machine Linux, vous restaurez sur le point de restauration du volume d'amorçage. La fonctionnalité de restauration BMR est prise en charge à l'aide de l'utilitaire `local_mount` de ligne de commande et depuis l'interface utilisateur de la console Core.

⚠ PRÉCAUTION : Avant de commencer le processus de restauration BMR, assurez-vous que la ou les machines Linux que vous souhaitez restaurer n'incluent pas de partition d'amorçage ext2. Lorsque la restauration BMR est effectuée sur une machine dont le type de partition est ext2, le processus va empêcher le démarrage de la machine, en règle générale. Si tel est le cas, pour effectuer une restauration BMR, vous allez devoir d'abord convertir toutes les éventuelles partitions ext2 en partition ext3, ext4 ou XFS avant de commencer la protection et la sauvegarde de la machine.

⚠ PRÉCAUTION : Lorsque vous amorcez une machine Linux restaurée pour la première fois après une restauration BMR, Rapid Recovery crée une image de base de la machine restaurée. Selon la quantité de données sur la machine, ce processus prend plus de temps que de prendre un instantané incrémentiel. Pour plus d'informations sur les images de base et les snapshots incrémentiels, voir [Comprendre la planification de la protection](#).

Pour effectuer une restauration BMR pour des machines Linux, effectuez les tâches suivantes.

- Gérer une image d'amorçage Linux. L'image ISO d'amorçage Live DVD de Linux sera utilisée pour démarrer le disque de destination, à partir duquel vous allez pouvoir accéder à la console Universal Recovery Console pour communiquer avec les sauvegardes présentes sur le Core. Voir [Gestion d'une image d'amorçage Linux](#).
 - Pour obtenir l'image de démarrage de la restauration BMR, vous devez d'abord identifier l'image dont vous avez besoin, puis la charger dans le Portail des licences. Voir [À propos de l'image d'amorçage ISO pour Linux](#) puis [Télécharger une image ISO d'amorçage pour Linux](#).
 - Si vous avez besoin d'un support physique pour démarrer la machine de destination Linux, vous devez transférer l'image ISO vers le support. Voir [Enregistrement de l'image ISO de DVD Live vers un support](#).
 - Dans tous les cas, vous devez charger l'image d'amorçage dans le serveur de destination et démarrer le serveur à partir de l'image d'amorçage. Voir [Chargement du DVD Live et démarrage de la machine cible](#).
 - Une fois le média chargé, vous devez connecter la machine Linux au Core Rapid Recovery. Voir [Connexion à la cible de la BMR à partir du Core Rapid Recovery](#).
- Gérer les partitions. Il peut être nécessaire de créer ou de monter des partitions avant d'effectuer une restauration BMR sur une machine Linux. Voir [Gestion des partitions Linux](#).
 - Le système Linux sur lequel vous effectuez une restauration BMR doit avoir les mêmes partitions que les volumes source du point de restauration. Il peut être nécessaire de créer des partitions supplémentaires sur le système cible, si nécessaire. Voir [Création de partitions sur le disque de destination](#).
 - Si vous effectuez une restauration BMR manuelle, vous devez d'abord monter les partitions. Voir [Montage de partitions à partir de la ligne de commande](#). Les étapes pour monter les partitions sont incluses dans le processus d'exécution d'une restauration BMR à partir de la ligne de commande. Voir [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#).
Si vous utilisez le partitionnement automatique pour la restauration BMR dans Core Console, vous n'avez pas besoin de monter les partitions. Rapid Recovery va restaurer les mêmes partitions que celles incluses dans le ou les points de restauration en cours de restauration.
- Lancer une restauration Bare Metal Restore pour Linux. Une fois la machine de destination démarrée à partir de l'image d'amorçage Live DVD, vous pouvez lancer la restauration BMR. Les tâches à accomplir varient selon que vous effectuez cette opération depuis

l'interface utilisateur Rapid Recovery ou depuis la ligne de commande à l'aide de l'utilitaire local_mount. Voir [Lancement d'une restauration Bare Metal Restore pour Linux](#).

- Si vous utilisez la Core Console, vous devez lancer une restauration à partir d'un point de restauration présent sur le Core. Voir [Sélection d'un point de restauration et lancement d'une restauration BMR](#).
- Si vous utilisez la Core Console, vous devez adresser les volumes depuis l'interface utilisateur. Voir [À propos de l'adressage des volumes pour une restauration BMR \(Bare Metal Restore\)](#).
- Facultativement, si vous effectuez une restauration depuis la ligne de commande, vous pouvez utiliser l'utilitaire de l'écran pour améliorer le défilement ou l'affichage des commandes dans la console du terminal. Cet utilitaire s'ouvre par défaut. Si vous le fermez, vous pouvez toujours le relancer. Pour plus d'informations, voir [Démarrage de l'utilitaire d'écran](#).
- Si vous utilisez local_mount, toutes les tâches seront effectuées sur la ligne de commande. Pour plus d'informations, voir [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#).
- Vérification d'une restauration Bare Metal Restore. Après avoir démarré la restauration BMR, vous pouvez vérifier et surveiller son avancement. Voir [Vérification de la restauration BMR à partir de la ligne de commande](#).
 - Vous pouvez surveiller l'avancement de la restauration. Voir [Affichage de l'avancement de la restauration](#).
 - Une fois la restauration terminée, vous pouvez démarrer le serveur restauré. Voir [Démarrage d'un serveur cible restauré](#).
 - Résolution des problèmes liés au processus de restauration BMR. Voir [Résolution des problèmes de connexion à Universal Recovery Console](#) et [Réparation des problèmes d'amorçage](#).

Prérequis pour l'exécution d'une restauration BMR pour une machine Linux

Pour pouvoir démarrer une restauration BMR pour une machine Linux, vous devez vérifier que les conditions et critères suivants sont respectés :

- Sauvegardes de la machine que vous souhaitez restaurer. Vous devez disposer d'un Core Rapid Recovery en état de fonctionnement et contenant les points de restauration du serveur protégé à restaurer.
- Matériel à restaurer (nouveau ou ancien, similaire ou on) La machine cible doit satisfaire aux exigences d'installation d'un agent ; pour plus de détails, reportez-vous au Rapid Recovery.
- Image d'amorçage Live DVD. Récupérez l'image ISO Live DVD de Linux, qui comprend une version amorçable de Linux. Téléchargez-le à partir du Portail des licences Dell Data Protection | Rapid Recovery à l'adresse <https://licenseportal.com>. Si vous rencontrez des problèmes lors du téléchargement du DVD Live, contactez le Support Dell Rapid Recovery.
- Support de l'image et logiciel. Si vous utilisez un support physique, vous devez disposer d'un CD ou d'un DVD vierge et d'un logiciel de gravure de disque ou d'un logiciel permettant de créer une image ISO.
- Pilotes de stockage et pilotes de carte réseau compatibles. Si vous effectuez la restauration sur un matériel différent, vous devez disposer des pilotes de stockage et des pilotes de carte réseau compatibles pour la machine cible (pilotes RAID, AHCI et de jeu de puces du système d'exploitation cible, selon les cas).
- Espace de stockage et partitions, selon les cas. Assurez-vous de disposer de suffisamment d'espace sur le disque dur pour créer des partitions de destination sur la machine cible devant contenir les volumes source. Toute partition de destination doit être au minimum aussi grande que la partition source d'origine.
- Chemin de restauration. Identifiez le chemin de la restauration, c'est-à-dire le chemin correspondant au descripteur de fichier de l'appareil. Pour identifier le chemin correspondant au descripteur de fichier du périphérique, utilisez la commande `fdisk` depuis une fenêtre de terminal.

Gestion d'une image d'amorçage Linux

Une restauration BMR pour Linux nécessite une image d'amorçage Live DVD, que vous pouvez télécharger depuis le Portail des licences Dell Data Protection | Rapid Recovery. Vous allez utiliser cette image pour démarrer la machine Linux de destination. En fonction des caractéristiques de l'environnement, il peut être nécessaire de transférer l'image vers un support physique, comme un CD ou un DVD. Vous devez ensuite charger virtuellement ou physiquement l'image d'amorçage et démarrer le serveur Linux à partir de celle-ci.

REMARQUE : le DVD Live s'appelait auparavant CD Live.

La gestion d'une image d'amorçage Linux est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#).

Vous pouvez effectuer les tâches suivantes :

À propos de l'image d'amorçage ISO pour Linux

La première étape d'une restauration BMR pour une machine Linux consiste à télécharger l'image ISO du DVD Linux Live depuis le Portail des licences Dell Data Protection | Rapid Recovery. Le DVD Live fonctionne avec tous les systèmes de fichiers Linux pris en charge par Rapid Recovery, et comporte une version amorçable de Linux, un utilitaire d'écran et l'interface Universal Recovery Console (URC) Rapid Recovery. L'Universal Recovery Console Rapid Recovery est un environnement utilisé pour restaurer le disque système ou tout le serveur directement depuis le Core Rapid Recovery.

REMARQUE : L'Organisation internationale de normalisation (ISO) est un organisme international composé de représentants de diverses organisations nationales qui définissent les normes des systèmes de fichiers. ISO 9660 est une norme de système de fichiers utilisée dans les supports de disques optiques au cours de l'échange de données. Elle prend en charge divers systèmes d'exploitation. Une image ISO est le fichier archive ou l'image disque qui contient les données de chaque secteur du disque, ainsi que le système de fichiers du disque.

Télécharger une image ISO d'amorçage pour Linux

Vous devez télécharger l'image ISO du DVD Live qui correspond à votre version de Rapid Recovery. La version actuelle du DVD Live est disponible à partir du Portail des licences Dell Data Protection | Rapid Recovery sur <https://licenseportal.com>. Si vous avez besoin d'une version différente, contactez le Support Dell Rapid Recovery.

REMARQUE : Pour plus d'informations sur le Portail des licences Dell Data Protection | Rapid Recovery, voir le guide d'utilisation du Portail des licences Dell Data Protection | Rapid Recovery.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Gestion d'une image d'amorçage Linux](#).

Effectuez cette procédure pour télécharger l'image ISO du DVD Live.

- 1 Connectez-vous au Portail des licences Dell Data Protection | Rapid Recovery sur <https://licenseportal.com>.
- 2 Accédez à la zone Téléchargements.
- 3 Accédez à Applications Linux et, dans la section Live DVD Linux, cliquez sur **Télécharger**.
- 4 Enregistrez l'image ISO DVD Live. Si vous effectuez la restauration d'une machine virtuelle, vous pouvez l'enregistrer sur un emplacement réseau, et paramétrer la machine virtuelle pour qu'elle démarre à partir d'un disque CD ou DVD associé à l'image ISO.
- 5 Si vous effectuez la restauration d'une machine physique, gravez l'image ISO d'amorçage sur un disque compact (CD) ou un disque vidéo numérique (DVD) à partir duquel la machine cible peut être démarrée. Pour plus d'informations, voir [Enregistrement de l'image ISO de DVD Live vers un support](#).

Enregistrement de l'image ISO de DVD Live vers un support

Lorsque vous téléchargez le fichier Live DVD de Linux, celui-ci est stocké en tant qu'image ISO dans le chemin que vous indiquez. Vous devez pouvoir amorcer la machine Linux cible à partir de l'image de DVD Live.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Gestion d'une image d'amorçage Linux](#).

Gravez l'image ISO d'amorçage sur un CD (disque compact) ou un DVD (disque vidéo numérique).

Si vous effectuez une restauration BMR sur une machine virtuelle, cette étape n'est pas nécessaire. Il suffit de charger l'image ISO sur un disque et de modifier les paramètres de machine pour cette machine virtuelle pour qu'elle démarre depuis ce disque. Vous pouvez également utiliser l'exportation virtuelle pour restaurer une machine virtuelle Linux. Pour plus d'informations, voir [VM export \(Exportation NFS\)](#).

Chargement du DVD Live et démarrage de la machine cible

Après avoir récupéré l'image ISO Live DVD, vous devez démarrer la machine Linux à partir du DVD Live qui vient d'être créé.

Cette tâche est une étape de la rubrique [Effectuer une restauration BMR de machines Linux](#). Elle fait partie du processus [Gestion d'une image d'amorçage Linux](#).

- 1 Accédez au nouveau serveur et chargez l'image de DVD Live depuis l'emplacement approprié. Spécifiez que le serveur va démarrer à partir de l'image DVD Live.
- 2 Démarrez la machine.
Une page d'attente Rapid Recovery apparaît et une fenêtre s'ouvre, affichant l'adresse IP et le mot de passe d'authentification de la machine.

REMARQUE : un nouveau mot de passe temporaire est généré chaque fois que la machine est démarrée avec l'image Live DVD.

- 3 Notez l'adresse IP et le mot de passe d'authentification affichés sur l'écran d'introduction. Vous aurez besoin de ces informations ultérieurement au cours du processus de restauration des données pour vous reconnecter à la console.

Connexion à la cible de la BMR à partir du Core Rapid Recovery

Une fois avoir démarré la machine Linux cible avec le DVD Live, cette machine est prête pour une connexion depuis le Core et au démarrage du processus de restauration BMR. Vous pouvez effectuer ce processus en utilisant l'une des deux méthodes suivantes :

- Lancement d'une restauration depuis la console Core Rapid Recovery. Pour plus d'informations, voir [Lancement d'une restauration Bare Metal Restore pour Linux](#).
- Lancer une restauration depuis la ligne de commande en utilisant l'utilitaire aamount. Pour plus d'informations, voir [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#).

Gestion des partitions Linux

Lorsque vous effectuez une restauration BMR, le disque de destination sur lequel vous allez restaurer les données doit avoir les mêmes partitions que celles du point de restauration que vous restaurez. Il peut être nécessaire de créer des partitions qui répondent à cette exigence.

Vous pouvez lancer la restauration depuis la ligne de commande en utilisant l'utilitaire aamount, ou depuis la console Core Rapid Recovery. Si vous restaurez en utilisant l'interface utilisateur, vous devez d'abord monter les partitions.

La gestion des partitions Linux est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#).

Vous pouvez effectuer les tâches suivantes :

Liens connexes

- [Création de partitions sur le disque de destination](#)
- [Formater des partitions sur le disque de destination](#)
- [Montage de partitions à partir de la ligne de commande](#)

Création de partitions sur le disque de destination

Généralement, lorsque vous effectuez une restauration BMR, le lecteur de destination est un nouveau volume susceptible de ne contenir qu'une seule partition. Le lecteur de la machine de destination doit avoir le même tableau de partitions que celui du point de restauration, y compris en ce qui concerne la taille des volumes. Si le disque de destination ne contient pas les mêmes partitions, vous devez les créer avant d'effectuer la restauration BMR. Utilisez l'utilitaire fdisk pour créer des partitions sur le disque de destination qui soient identiques aux partitions présentes sur le disque source.

PRÉCAUTION : la procédure ci-dessous est donnée à titre d'exemple. Les environnements des clients présentent des différences. Nous vous conseillons d'adapter les commandes utilisées aux particularités de votre environnement.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Gestion des partitions Linux](#).

- 1 Vous pouvez également utiliser l'utilitaire d'écran. Cet utilitaire démarre par défaut et reste actif jusqu'au redémarrage de la machine.

REMARQUE : si vous le fermez explicitement et souhaitez le rouvrir, voir [Démarrage de l'utilitaire d'écran](#).

- 2 Depuis la ligne de commande, saisissez la commande suivante, puis appuyez sur **Entrée** pour modifier les privilèges pour exécuter en tant qu'administrateur avant de répertorier les partitions du disque :

```
sudo fdisk -l
```

La liste de tous les volumes apparaît.

Cet exemple suppose que le volume que vous voulez partitionner est /dev/sda. Si le volume est différent (par exemple, pour les disques plus anciens, il est possible que vous voyiez /dev/hda), modifiez les commandes en conséquence.

- 3 Pour créer une partition d'amorçage, entrez la commande suivante, puis appuyez sur **Entrée** :

```
sudo fdisk /dev/sda
```

- 4 Pour créer une partition d'amorçage, entrez la commande suivante, puis appuyez sur **Entrée** :

```
n
```

- 5 Pour créer une partition principale, entrez la commande suivante, puis appuyez sur **Entrée** :

```
p
```

- 6 Pour spécifier un numéro de partition, entrez le numéro de partition, puis appuyez sur **Entrée**. Par exemple, pour spécifier la partition 1, entrez 1, puis appuyez sur **Entrée**.

- 7 Pour utiliser le premier secteur, 2 048, appuyez sur **Entrée**.

- 8 Affectez une quantité appropriée à la partition d'amorçage en entrant le signe + suivi de la quantité allouée, puis appuyez sur **Entrée**. Par exemple, pour affecter 500 M à la partition d'amorçage, entrez la commande suivante puis appuyez sur **Entrée** :

```
+512000K
```

- 9 Pour utiliser un indicateur d'amorçage pour la partition d'amorçage (pour rendre la partition amorçable), entrez la commande suivante puis appuyez sur **Entrée** :

```
a
```

- 10 Pour affecter un indicateur d'amorçage à la partition appropriée, entrez le numéro de la partition, puis appuyez sur **Entrée**. Par exemple, pour affecter un indicateur d'amorçage à la partition 1, entrez 1 puis appuyez sur **Entrée**.

- 11 Continuer de partitionner votre disque si nécessaire.

- 12 Pour enregistrer toutes les modifications dans l'utilitaire fdisk, saisissez la commande suivante puis appuyez sur **Entrée** :

```
w
```

Formater des partitions sur le disque de destination

Après la création de partitions sur un nouveau volume sur le lecteur de destination pour effectuer une restauration BMR, si vous n'utilisez pas l'option de partition automatique, vous devez formater les partitions avant de pouvoir les monter. Si cette situation s'applique à vous, suivez cette procédure pour formater les partitions dans le format ext3, ext4 ou XFS.

Pour tous les autres scénarios, vous n'avez pas besoin de formater les partitions en suivant la procédure décrite dans cette rubrique.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Gestion des partitions Linux](#).

- 1 Facultativement, vous pouvez utiliser l'utilitaire d'écran. Cet utilitaire démarre par défaut et reste actif jusqu'au redémarrage de la machine.

REMARQUE : Si vous l'avez explicitement fermé et que vous souhaitez le rouvrir, voir [Démarrage de l'utilitaire d'écran](#).

- 2 Depuis la ligne de commande, saisissez la commande suivante, puis appuyez sur **Entrée** pour modifier les privilèges pour exécuter en tant qu'administrateur avant de répertorier les partitions du disque :

```
sudo fdisk -l
```

La liste de tous les volumes apparaît.

Cet exemple suppose que la partition à formater est /dev/sda1. Si le volume est différent (par exemple, pour les disques plus anciens, il est possible que vous voyiez /dev/hda), modifiez les commandes en conséquence.

- 3 Sélectionnez l'une des commandes suivantes en fonction du format à utiliser pour la partition de destination :

- Pour formater la partition dans le format ext3, entrez la commande suivante, puis appuyez sur **Entrée** :

```
sudo mkfs.ext3 /dev/sda1
```

- Pour formater la partition dans le format ext4, entrez la commande suivante, puis appuyez sur **Entrée** :

```
sudo mkfs.ext4 /dev/sda1
```

- Pour formater la partition au format XFS, entrez la commande suivante, puis appuyez sur **Entrée** :

```
sudo mkfs.xfs /dev/sda1
```

La partition sélectionnée est formatée de manière appropriée.

- 4 Répétez éventuellement cette procédure si vous devez formater d'autres partitions.

Montage de partitions à partir de la ligne de commande

Si vous effectuez une restauration BMR à l'aide de la console Core Rapid Recovery, vous devez d'abord monter les partitions appropriées sur la machine de destination. Effectuez cela à partir de la ligne de commande dans Universal Recovery Console.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Gestion des partitions Linux](#).

Suivez cette procédure pour monter les partitions sur la machine Linux avant d'effectuer une restauration.

- 1 Depuis la ligne de commande, saisissez la commande suivante, puis appuyez sur **Entrée** pour modifier les privilèges pour exécuter en tant qu'administrateur avant de répertorier les partitions du disque :

```
sudo fdisk -l
```

La liste de tous les volumes apparaît.

- 2 Formatez toutes les partitions dont vous avez besoin pour effectuer la restauration BMR dans le répertoire de montage. Celles-ci doivent correspondre aux volumes qui sont dans le point de restauration. Par exemple, si le volume à monter s'appelle sda1, et que le répertoire de montage est mnt, tapez la commande suivante, puis appuyez sur **Entrée** :

- 3 Montez toutes les partitions dont vous avez besoin pour effectuer la restauration BMR dans le répertoire de montage. Celles-ci doivent correspondre aux volumes qui sont dans le point de restauration. Par exemple, si le volume à monter s'appelle sda1, et que le répertoire de montage est mnt, tapez la commande suivante, puis appuyez sur **Entrée** :

```
mount /dev/sda1 /mnt
```

- 4 Répétez l'étape 3 autant de fois que nécessaire jusqu'à ce que vous ayez monté tous les volumes requis.

Lorsque les volumes sont montés, vous pouvez effectuer une restauration sur la machine de destination Linux à partir de la console Core Rapid Recovery. Voir [Lancement d'une restauration Bare Metal Restore pour Linux](#).

Lancement d'une restauration Bare Metal Restore pour Linux

Avant de lancer une restauration BMR pour une machine Linux, certaines conditions doivent être remplies.

- Pour restaurer un point de restauration enregistré sur le Core, vous devez disposer du matériel approprié. Pour plus d'informations, voir [Prérequis pour l'exécution d'une restauration BMR pour une machine Linux](#).
- La machine Linux de destination pour la restauration BMR doit être démarrée à l'aide de l'image d'amorçage (Live DVD). Pour plus d'informations, voir [Gestion d'une image d'amorçage Linux](#).
- Le nombre de volumes sur la machine Linux à restaurer doit correspondre au nombre de volumes dans le point de restauration. Vous devez également décider si vous souhaitez restaurer à partir de la console Core Rapid Recovery, ou à partir de la ligne de commande en utilisant local_mount. Pour plus d'informations, voir [Gestion des partitions Linux](#).
- Si vous restaurez depuis l'interface utilisateur Core Console, la première étape d'une restauration BMR consiste à sélectionner le point de restauration approprié, puis à lancer la restauration sur le matériel en spécifiant l'adresse IP et le mot de passe temporaire que vous avez obtenus de Universal Recovery Console. Vous devez ensuite adresser les disques et démarrer la restauration.

Cette tâche est une étape de la [Effectuer une restauration Bare Metal Restore de machines Linux](#).

Pour lancer une restauration BMR depuis la console Core Rapid Recovery, effectuez les tâches suivantes.

- [Sélection d'un point de restauration et lancement d'une restauration BMR](#)
- [À propos de l'adressage des volumes pour une restauration BMR \(Bare Metal Restore\)](#)

Si vous restaurez à partir de la ligne de commande en utilisant l'utilitaire `local_mount`, vous devez tout d'abord définir les privilèges appropriés, monter les volumes, exécuter `local_mount`, récupérer les informations sur le Core à partir de la liste des machines, effectuer la connexion au Core, récupérer la liste des points de restauration, sélectionner le point de restauration à restaurer sur la machine bare metal et lancer la restauration.

De manière optionnelle, vous pouvez démarrer l'utilitaire Screen.

Pour lancer une restauration BMR depuis la ligne de commande, effectuez les tâches suivantes.

- [Démarrage de l'utilitaire d'écran](#)
- [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#)

Démarrage de l'utilitaire d'écran

Le DVD Live comprend Screen, un utilitaire qui est disponible lorsque vous démarrez à partir du DVD Live dans la Universal Recovery Console. Screen permet aux utilisateurs de gérer plusieurs shells simultanément par le biais d'une seule session Secure Shell (SSH) ou fenêtre de console. Cela permet d'effectuer une tâche dans la fenêtre de terminal (par exemple, vérifier les volumes montés) et, pendant que cette tâche est en cours d'exécution, d'ouvrir ou de basculer sur une autre instance de Shell afin d'y effectuer une autre tâche (par exemple, exécuter l'utilitaire `local_mount`).

L'utilitaire Screen dispose également de sa propre mémoire tampon de défilement, ce qui permet de faire défiler l'écran pour afficher de plus grandes quantités de données, telles qu'une liste des points de restauration.

❗ REMARQUE : Cet utilitaire est fourni à des fins pratiques, mais son utilisation est facultative.

L'utilitaire Screen démarre sur la machine amorcée avec le DVD Live par défaut. Cependant, si vous avez fermé cette application, vous devez démarrer l'utilitaire Screen depuis le DVD Live en procédant comme suit.

Si la machine a été amorcée depuis le DVD Live, dans la fenêtre de terminal, saisissez « screen » et appuyez sur **Entrée**.

L'utilitaire Screen démarre.

Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande

Lorsque l'image ISO Live DVD est accessible sur la machine sur laquelle vous souhaitez effectuer une restauration BMR et que le nombre et la taille des volumes de la machine cible correspondent à ceux du point de restauration à restaurer à l'état bare metal, vous pouvez lancer une restauration depuis la ligne de commande à l'aide de l'utilitaire `local_mount`.

❗ REMARQUE : ce composant était auparavant appelé `aamount`.

Pour effectuer une restauration BMR à l'aide de l'interface utilisateur de la console Core Rapid Recovery, voir [Sélection d'un point de restauration et lancement d'une restauration BMR](#).

❗ REMARQUE : lorsque vous effectuez cette procédure, n'essayez pas de monter les points de restauration dans le dossier `/tmp`, qui contient les fichiers `rapidrecovery-vdisk` (anciennement `aavdisk`).

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Lancement d'une restauration BMR sur une machine Linux à l'aide de la ligne de commande](#).

Suivez la procédure suivante pour choisir un point de restauration sur le Core à restaurer sur la machine cible BMR physique ou virtuelle.

- 1 Pour exécuter l'utilitaire `local_mount` de Rapid Recovery en tant qu'utilisateur `root`, saisissez la commande suivante, puis appuyez sur **Entrée** :

```
sudo local_mount
```

- 2 Pour afficher la liste des machines protégées, saisissez la commande suivante, puis appuyez sur **Entrée** :

```
lm
```

- 3 Lorsque vous y êtes invité, entrez les informations de connexion du Core Rapid Recovery, tel que décrit dans le tableau suivant, en appuyant sur Entrée après chaque commande demandée :

Tableau 159. Informations de connexion du Core Rapid Recovery

Boîte de texte	Description	Obligatoire
adresse IP ou nom d'hôte du Core Rapid Recovery	adresse IP ou nom d'hôte du Core Rapid Recovery.	Oui
Domaine	Domaine du Core Rapid Recovery. Ce champ est facultatif.	Non
Utilisateur	Nom d'utilisateur correspondant à un utilisateur administratif sur le Core.	Oui
Mot de passe	Mot de passe utilisé pour connecter l'utilisateur administratif au Core.	Oui

Une liste s'affiche, indiquant les machines protégées par le Core Rapid Recovery. Elle répertorie les machines détectées par numéro de ligne, l'adresse IP ou le nom d'affichage de l'hôte et un numéro d'identification correspondant à la machine.

- 4 Pour afficher la liste des points de restauration de la machine à restaurer, entrez la commande Répertorier les points de restauration en utilisant la syntaxe suivante, puis appuyez sur **Entrée** :

```
lr <machine_line_item_number>
```

REMARQUE : vous pouvez également entrer le numéro d'identification de la machine dans cette commande au lieu du numéro de ligne.

Une liste s'affiche indiquant les points de restauration de base et incrémentiels de cette machine. Cette liste comprend :

- Un numéro de ligne
- Un horodatage
- La liste des lettres des volumes dans le point de restauration
- L'emplacement du volume
- La taille du point de restauration
- Un numéro d'identification du volume comprenant un numéro de séquence final qui identifie le point de restauration

- 5 Pour choisir le point de restauration à restaurer, entrez la commande suivante, puis appuyez sur **Entrée** :

```
r <recovery_point_ID_number> <path>
```

PRÉCAUTION : vous devez vous assurer que le volume système n'est pas monté.

REMARQUE : si vous avez démarré la machine à partir du Live DVD, le volume système n'est pas monté.

Cette commande restaure l'image de volume spécifiée par le numéro d'identification du Core au chemin spécifié. Le chemin utilisé pour la restauration correspond au chemin du descripteur de fichiers du périphérique et n'est pas le répertoire sur lequel il est monté.

❶ **REMARQUE :** pour identifier le point de restauration, vous pouvez également indiquer le numéro de ligne dans la commande au lieu du numéro d'identification du point de restauration. Dans ce cas, utilisez le numéro de ligne de la machine ou de l'agent (à partir de la sortie `lm`), suivi du numéro de ligne du point de restauration et de la lettre de volume (à partir de la liste des lettres de volumes du point de restauration), suivi du chemin. Par exemple :

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

Par exemple, saisissez :

```
r 1 24 a /dev/sda1
```

Dans cette commande, `<path>` est le descripteur de fichier du volume réel en question.

- 6 Lorsque vous êtes invité à poursuivre, saisissez `y` pour Yes (Oui), puis appuyez sur **Entrée**.
Une fois la restauration lancée, une série de messages s'affiche pour vous informer de l'état d'avancement du processus de restauration.

❶ **REMARQUE :** si vous recevez un message d'exception, les détails correspondants se trouvent dans le fichier `local_mount.log`. Le fichier `local_mount.log` se situe dans `/var/log/apprecovery`.

- 7 Une fois la restauration achevée, quittez `local_mount` en saisissant `exit`, puis appuyez sur **Entrée**.
8 L'étape suivante consiste à vérifier la restauration. Pour plus d'informations, voir [Vérification de la restauration BMR à partir de la ligne de commande](#).

Restaurer les volumes d'une machine Linux à l'aide de la ligne de commande

Dans Rapid Recovery, vous pouvez restaurer des volumes sur les machines protégées Linux à l'aide de l'utilitaire de ligne de commande `local_mount`.

❶ **REMARQUE :** ce processus s'appelait auparavant *Rollback*. Lorsque vous effectuez cette procédure, n'essayez pas de monter les points de restauration dans le dossier `/tmp`, qui contient les fichiers `rapidrecovery-vdisk` (anciennement `aavdisk`). La restauration de volumes est également prise en charge pour les machines protégées dans la Rapid Recovery Core Console. Voir [À propos de la restauration de volumes à partir d'un point de restauration](#) pour plus d'informations.

⚠ **PRÉCAUTION :** pour restaurer le système ou la partition racine (`/`), ou le système d'exploitation tout entier, voir [Effectuer une restauration Bare Metal Restore de machines Linux](#).

- 1 Exécutez l'utilitaire de Rapid Recovery `local_mount` en tant que racine, par exemple :

```
sudo local_mount
```
- 2 À l'invite de montage Rapid Recovery, entrez la commande suivante pour répertorier les machines protégées.

```
lm
```
- 3 Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte de votre serveur Core Rapid Recovery.
- 4 Entrez les données d'identification de connexion, c'est-à-dire le nom d'utilisateur et le mot de passe de ce serveur.
Une liste s'affiche, indiquant les machines protégées par ce serveur Rapid Recovery. Elle répertorie les machines protégées et trouvées par le numéro de ligne, l'adresse IP/le nom d'hôte et l'identifiant de machine (par exemple : `7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2`).
- 5 Entrez la commande suivante pour répertorier les points de restauration actuellement montés pour la machine spécifiée :

```
lr <machine_line_item_number>
```

❶ **REMARQUE :** notez que vous pouvez également entrer le numéro d'identification de la machine dans cette commande au lieu du numéro de ligne.

Une liste s'affiche, indiquant les points de restauration de base et incrémentiels de cette machine. Cette liste comprend le numéro de ligne, l'horodatage, l'emplacement du volume, la taille du point de restauration et le numéro d'identification du volume, comprenant un numéro de séquence à la fin (par exemple, "293cc667-44b4-48ab-91d8-44bc74252a4f:2"), qui identifie le point de restauration.

- 6 Entrez la commande suivante pour sélectionner un point de restauration à restaurer :

```
r <volume_recovery_point_ID_number> <device_path>
```

Cette commande restaure l'image de volume spécifiée par le numéro d'identification du Core au chemin spécifié. Le chemin utilisé pour la restauration correspond au chemin du descripteur de fichiers du périphérique, et non au répertoire sur lequel il est monté.

- Pour identifier le point de restauration, vous pouvez également spécifier un numéro de ligne dans la commande au lieu du numéro d'identification du point de restauration. Dans ce cas, vous utilisez le numéro de ligne de la machine protégée (à partir de la sortie `lm`), suivi du numéro de ligne du point de restauration et de la lettre du volume, suivi du chemin d'accès, par exemple, `r <numéro_élément_ligne_machine> <numéro_ligne_point_restoration> <lettre_volume> <chemin>`. Dans cette commande, `<path>` est le descripteur de fichier du volume réel en question.

Par exemple, si le résultat de `lm` répertorie trois machines protégées, que vous saisissez la commande `lr` pour le numéro de machine protégée 2, et que vous souhaitez restaurer le volume 23 du point de restauration `b` qui a été monté sur le répertoire `/dev/sda5`, la commande serait :

```
r2 23 b /dev/sda5
```

REMARQUE : il est possible de restaurer vers / si nécessaire. Si vous exécutez une restauration Bare Metal Restore à l'aide d'un DVD Live, il est supposé que vous souhaitez restaurer vers une machine différente. Pour plus d'informations, voir [Lancement d'une restauration Bare Metal Restore pour Linux](#).

- 7 Lorsque vous êtes invité à continuer, saisissez `y` pour Oui.

Au cours de la restauration, une série de messages s'affiche pour vous informer de l'état.

- 8 Si la récupération aboutit, l'utilitaire `local_mount` monte et attache de nouveau automatiquement le module noyau au volume restauré si la cible a été préalablement protégée et montée. Dans le cas contraire, vous allez devoir monter le volume restauré sur le disque local, puis vérifier que les fichiers sont restaurés (par exemple, vous pouvez utiliser la commande `sudo mount` suivie de la commande `ls`).

Vérification d'une restauration bare metal restore

Après avoir effectué une restauration bare metal restore (BMR), vous pouvez vérifier la progression de cette restauration. Une fois l'opération terminée sans erreur, vous pouvez démarrer le serveur restauré. Certaines étapes de dépannage sont incluses en cas de problèmes de connexion à l'Universal Recovery Console pour effectuer la restauration, et pour résoudre les problèmes de démarrage rencontrés avec la machine restaurée.

Vous pouvez effectuer les tâches suivantes :

Liens connexes

- [Affichage de l'avancement de la restauration](#)
- [Démarrage d'un serveur cible restauré](#)
- [Résolution des problèmes de connexion à Universal Recovery Console](#)
- [Réparation des problèmes d'amorçage](#)

Affichage de l'avancement de la restauration

Suivez les étapes de cette procédure pour afficher l'avancement d'une restauration de données à partir d'un point de restauration (y compris bare metal restore) lancée depuis la Rapid Recovery Core Console.

- 1 Après avoir lancé le processus de restauration des données à partir d'un point de restauration, lorsque la tâche est en cours d'exécution, vous pouvez afficher son avancement dans le menu déroulant Tâche en cours d'exécution sur la Core Console.
- 2 Vous pouvez également consulter des informations détaillées sur la page Événements. Pour en savoir plus sur la surveillance des événements Rapid Recovery, voir [Affichage des tâches, alertes et événements](#).

Démarrage d'un serveur cible restauré

Effectuez cette procédure pour démarrer le serveur cible restauré.

❶ **REMARQUE :** avant de démarrer le serveur cible, vous devez vérifier que la restauration s'est effectuée correctement. Pour plus d'informations, voir [Affichage de l'avancement de la restauration](#).

Cette tâche est une étape de la rubrique [Exécution d'une restauration complète sur des machines Windows](#). Elle fait partie du processus [Vérification d'une restauration bare metal restore](#).

- 1 Sur le serveur cible, vérifiez que l'Universal Recovery Console Rapid Recovery est active.
- 2 Éjectez le CD d'amorçage (ou déconnectez le support physique comportant l'image d'amorçage) du serveur restauré.
- 3 Dans l'Universal Recovery Console, cliquez sur l'icône du menu Alimentation située en haut de l'écran, puis cliquez sur **Redémarrer**.
- 4 Indiquez que vous voulez démarrer le système d'exploitation normalement.
- 5 Connectez-vous à la machine. Le système doit être restauré dans l'état qui était le sien dans le point de restauration.

Résolution des problèmes de connexion à Universal Recovery Console

Les étapes suivantes permettent de résoudre les problèmes de connexion à l'image du CD d'amorçage dans le cadre du processus [Sélection d'un point de restauration et lancement d'une restauration BMR](#).

Si une erreur s'affiche indiquant que le Core n'a pas pu se connecter au serveur distant, plusieurs causes sont possibles.

- Vérifiez que l'adresse IP et le mot de passe actuel affichés dans la console URC sont identiques aux informations que vous avez saisies dans la boîte de dialogue Instance Recovery Console.
- Pour accéder au serveur sur lequel vous voulez restaurer les données, le Core doit pouvoir identifier le serveur dans le réseau. Pour déterminer si cela est possible, vous pouvez ouvrir une invite de commande sur le Core et envoyer un ping à l'adresse IP du serveur cible BMR. Vous pouvez également ouvrir une invite de commande sur le serveur cible et envoyer un ping à l'adresse IP du Core Rapid Recovery.
- Vérifiez que les paramètres de la carte réseau sont compatibles entre le Core et le serveur cible BMR.

Réparation des problèmes d'amorçage

Les tâches suivantes sont les pré-requis de cette procédure.

- [Création d'une image ISO sur CD d'amorçage](#)
- [Chargement du CD d'amorçage et démarrage de la machine cible](#)
- [Chargement des pilotes à l'aide de Universal Recovery Console](#)

Suivez cette procédure pour résoudre les problèmes de démarrage. Notez que si vous avez effectué la restauration sur un matériel différent, vous devez avoir injecté les pilotes du contrôleur de stockage, RAID, AHCI, de jeu de puces et les autres pilotes s'ils ne sont pas déjà sur le CD d'amorçage. Ces pilotes permettent au système d'exploitation de faire fonctionner correctement tous les périphériques sur le serveur cible. Pour en savoir plus, voir [Chargement des pilotes à l'aide de Universal Recovery Console](#). Procédez comme suit pour résoudre les problèmes de démarrage sur le serveur cible.

- 1 Dans l'Universal Recovery Console, cliquez sur l'onglet **Gestionnaire de pilotes Windows existant**.
- 2 Cliquez sur **Réparer les problèmes d'amorçage**.
Les paramètres de démarrage du disque d'amorçage du serveur cible sont automatiquement réparés.

Vérification de la restauration BMR à partir de la ligne de commande

Dell recommande d'effectuer les étapes suivantes pour vérifier une restauration BMR effectuée à partir de la ligne de commande.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#).

Liens connexes

[Exécution d'une vérification du système de fichiers sur le volume restauré](#)

[Utilisation de la ligne de commande pour rendre une machine Linux restaurée amorçable](#)

Exécution d'une vérification du système de fichiers sur le volume restauré

Après avoir exécuté une restauration BMR à partir de la ligne de commande, vous devez vérifier le système de fichiers dans le volume restauré pour vous assurer que les données restaurées du point de restauration ne sont pas endommagées.

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Vérification de la restauration BMR à partir de la ligne de commande](#).

Effectuez la tâche ci-dessous pour vérifier le système de fichiers dans le volume restauré.

- 1 Depuis la ligne de commande dans Universal Recovery Console de la machine Linux que vous avez restaurée, pour vérifier si les partitions ont correctement été montées, entrez la commande suivante, puis appuyez sur **Entrée** qui:

```
df
```
- 2 Si le volume restauré n'est pas monté, passez à l'[étape 3](#). si le volume restauré est monté, démontez-le en entrant la commande suivante, puis en appuyant sur Entrée :

```
umount <mount point>
```
- 3 Vérifiez le système de fichiers dans les volumes restaurés en entrant la commande suivante, puis en appuyant sur Entrée :

```
fsck -f <volume>
```

Si la commande fsck ne renvoie pas d'erreur, le système de fichiers est vérifié.
- 4 Remontez les volumes appropriés en entrant la commande suivante dans le format `mount <volume> <folder>`, puis appuyez sur **Entrée**.
Par exemple, si le volume à monter s'appelle prod/sda1 et que le dossier à monter est mnt, tapez la commande suivante, puis appuyez sur **Entrée** :

```
mount /dev/sda1 /mnt
```

Utilisation de la ligne de commande pour rendre une machine Linux restaurée amorçable

Après avoir vérifié le système de fichiers dans le volume restauré, vous devez créer des partitions amorçables.

GRUB (GNU Grand Unified Bootloader) est un chargeur de démarrage qui permet aux administrateurs de configurer le système d'exploitation ou la configuration de noyau à utiliser pour démarrer le système. Après une restauration BMR, le fichier de configuration GRUB doit être modifié de sorte que la machine utilise l'identifiant universel unique approprié (UUID) du volume racine. Avant cette étape, vous devez monter les volumes d'amorçage et racine et vérifier les identifiants UUID de chacun afin de pouvoir démarrer depuis la partition.

❗ REMARQUE : cette procédure s'applique aux machines Linux utilisant GRUB1 ou GRUB2. Lorsque vous utilisez cette procédure, assurez-vous que la partition d'amorçage est en bonne santé et qu'elle est protégée.

GRUB ou GRUB2 est généralement installé sur les systèmes d'exploitation Linux. Vous pouvez effectuer cette procédure en utilisant la version fournie avec votre distribution Linux. Si aucune version de GRUB n'est installée, vous devrez réinstaller la version par défaut correspondant à votre distribution Linux.

⚠ PRÉCAUTION : lorsque vous amorcez une machine Linux restaurée pour la première fois après une restauration BMR, Rapid Recovery crée une image de base de la machine restaurée. Selon la quantité de données stockées sur la machine, ce processus prend plus de temps que la création d'un snapshot incrémentiel. Pour en savoir plus sur les images de base et les snapshots incrémentiels, voir [Comprendre la planification de la protection](#).

Cette tâche est une étape de la rubrique [Effectuer une restauration Bare Metal Restore de machines Linux](#). Elle fait partie du processus [Vérification de la restauration BMR à partir de la ligne de commande](#).

Effectuez la tâche ci-dessous pour créer des partitions amorçables en utilisant la ligne de commande.

- 1 Vous devez monter le volume racine, puis le volume d'amorçage. Montez chacun des volumes restaurés à l'aide des commandes suivantes :

- a Pour monter le volume racine, saisissez la commande suivante, puis appuyez sur **Entrée** :

```
mount /<restored volume[root]> /mnt
```

Par exemple, si /dev/sda2 est le volume racine, saisissez `mount /dev/sda2 /mnt`, puis appuyez sur **Entrée**.

- b Pour monter le volume d'amorçage, entrez la commande suivante, puis appuyez sur **Entrée** :

```
mount /<restored volume[boot]> /mnt/boot
```

Par exemple, si /dev/sda1 est le volume d'amorçage, saisissez `mount /dev/sda1 /mnt/boot`, puis appuyez sur **Entrée**.

❗ REMARQUE : certaines configurations système peuvent inclure le répertoire d'amorçage dans le volume racine.

- 2 Si la taille du volume augmente, c'est-à-dire, si le volume de destination sur la nouvelle machine Linux est plus grand que le volume qui était dans le point de restauration, vous devez supprimer tous les fichiers de données bitmap existants.
- 3 Récupérez l'identifiant unique universel (UUID) des nouveaux volumes en utilisant la commande `blkid` . Entrez la commande suivante, puis appuyez sur **Entrée** :

```
blkid [volume]
```

❗ REMARQUE : vous pouvez également utiliser la commande `ls -l /dev/disk/by-uuid` .

- 4 Si vous effectuez une restauration BMR sur un tout nouveau disque de la machine de destination, entrez un commentaire pour la partition SWAP de fstab dans le volume racine.
- 5 La modification des chemins fstab et mtab doit se produire sur le volume restauré et non pas sur le DVD Live. Il est inutile de modifier les chemins sur le DVD Live. Préparez l'installation de Grand Unified Bootloader (GRUB) en entrant les commandes suivantes. Après chaque commande, appuyez sur **Entrée** :

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

```
mount --bind /sys /mnt/sys
```

- 6 Modifiez le répertoire racine en entrant la commande suivante, puis appuyez sur **Entrée** :

```
chroot /mnt /bin/bash
```

- 7 Récupérez l'ancien UUID de la ou des partitions à partir du fichier des points de restauration `montés/etc/fstab` et comparez-le aux UUID des volumes racine (pour Ubuntu et CentOS) et d'amorçage (pour CentOS et RHEL) ou aux partitions de données en saisissant la commande suivante, puis en appuyant sur **Entrée** :

```
less /mnt/etc/fstab
```

- 8 Récupérez l'ancien UUID de la ou des partitions à partir du fichier des points de restauration `montés/etc/mtab` et comparez-le aux UUID des volumes racine (pour Ubuntu et CentOS) et d'amorçage (pour CentOS et RHEL), ainsi qu'aux partitions de données en saisissant la commande suivante, puis en appuyant sur **Entrée** :

```
less /mnt/etc/mtab
```

- 9 Si vous utilisez SLES 11, installez GRUB en tapant les commandes suivantes, puis en appuyant sur **Entrée** :

```
grub-install --recheck /dev/sda
```

```
grub-install /dev/sda
```

- 10 Si vous utilisez Ubuntu, CentOS 6.x, RHEL 6.x, ou Oracle Linux 6.x, installez GRUB en saisissant la commande suivante, puis en appuyant sur **Entrée** :

```
grub-install /dev/sda
```

- 11 Si vous utilisez SLES 12, CentOS 7, RHEL 7, ou Oracle 7, installez GRUB2 en saisissant la commande suivante, puis en appuyant sur **Entrée** :

```
grub2-install /dev/sda
```

- 12 Après avoir terminé l'installation, exécutez l'une des mises à jour suivantes :

- Pour SLES :

```
grub-install.unsupported --recheck /dev/sda
```

```
grub-install.unsupported /dev/sda
```

```
update-grub
```

❗ **REMARQUE :** si la commande `update-grub` n'existe pas dans votre distribution Linux, ignorez cette option.

- Pour les autres distributions :
`grub-install /dev/sda`
`update-grub`

❗ **REMARQUE :** si la commande `update-grub` n'existe pas dans votre distribution Linux, ignorez cette option.

- 13 Retirez le disque DVD Live du lecteur de CD-ROM ou de DVD et redémarrez la machine Linux.

Générer et afficher des rapports

Cette section fournit une présentation de la création de rapports disponible dans le Core Rapid Recovery, et dans la Central Management Console Rapid Recovery.

Sujets :

- [À propos des rapports Rapid Recovery](#)
- [Central Management Console](#)

À propos des rapports Rapid Recovery

Vous pouvez générer des rapports à partir de la console Core Rapid Recovery. Certains de ces rapports sont également disponibles dans la Central Management Console.

Les rapports disponibles sont décrits dans le tableau suivant.

Tableau 160. Rapports Rapid Recovery

Type de rapport	Description
Rapport de tâche	Établit un rapport sur l'état des tâches réussies, les tâches qui ont échoué, ainsi que les tâches comportant des erreurs. Les tâches qui ont échoué peuvent encore être affichées dans un rapport sur les défaillances. Ce type de tâche peut être exécuté à partir de la console Core et à partir de la Central Management Console. • Lorsque vous l'exécutez depuis le Core, ce rapport peut spécifier les détails pour un ou plusieurs Cores. Par défaut, cet ensemble d'informations comprend les tâches pour toutes les machines : chaque machine protégée, machine répliquée et machine comportant uniquement des points de restauration dans les Cores spécifiés. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure des machines. Vous pouvez également sélectionner ou exclure des tâches qui sont indépendantes de la machine, auquel cas le rapport indique uniquement l'état des tâches du Core. • Lorsque vous l'exécutez depuis la perspective d'une machine protégée dans la console Core, le rapport obtenu affiche l'état des tâches pour cette machine protégée. • Lorsque exécuté depuis la Central Management Console, ce rapport peut spécifier les détails de n'importe quelle combinaison de Cores ou de groupes de Cores configurés dans la console. Les seuls paramètres configurables sont le type de rapport et la plage de dates. Pour plus d'informations sur ce type de rapport, voir Comprendre le rapport de tâche.
Rapport d'échec	Fournit des informations sur les tâches de Core ayant échoué avec les critères définis. Ce type de tâche peut être exécuté à partir de la console Core et à partir de la Central Management Console. • Lorsque vous l'exécutez à partir du Core, ce rapport peut inclure ou exclure les détails de la machine protégée. Tout comme le rapport de tâche, ce rapport peut également être exécuté uniquement à partir d'une machine protégée sélectionnée dans le Core. Le rapport obtenu affiche des informations sur les tâches qui ont échoué pour la machine protégée sélectionnée uniquement. • Lorsque exécuté depuis la Central Management Console, ce rapport peut spécifier les événements d'échec de n'importe quelle combinaison de Cores ou de groupes de Cores configurés dans la console. Les seuls paramètres configurables sont le type de rapport et la plage de dates.

Type de rapport	Description
	Pour plus d'informations sur ce type de rapport, voir Comprendre le rapport des échecs .
Rapport récapitulatif	Fournit des informations récapitulatives. Par défaut, cet ensemble d'informations comprend les tâches pour toutes les machines : chaque machine protégée, machine répliquée et machine comportant uniquement des points de restauration dans les Cores spécifiés. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure des machines. Vous pouvez également sélectionner ou exclure des tâches qui sont indépendantes de la machine, auquel cas le rapport indique uniquement l'état des tâches du Core. Ce rapport n'est pas disponible depuis la perspective d'une machine protégée. Ce type de tâche peut être exécuté à partir de la console Core et à partir de la Central Management Console. • Lorsque exécuté depuis la console Core, les catégories d'informations de ce rapport comprennent le Core, la licence et la logithèque. Les informations s'affichent sous forme de liste, de diagramme et de tableau. • Lorsque exécuté depuis la Central Management Console, ce rapport peut spécifier les informations de synthèse de n'importe quelle combinaison de Cores ou de groupes de Cores configurés dans la console. Les seuls paramètres configurables sont le type de rapport et la plage de dates. Les catégories d'informations de ce rapport comprennent le Core, la licence et la logithèque. Le rapport récapitulatif inclut également un rapport des machines protégées et le taux de tâches réussies par rapport au nombre total de tâches. Les informations s'affichent sous forme de liste, de diagramme et de tableau. Pour plus d'informations sur ce type de rapport, voir Comprendre le rapport récapitulatif.
Rapport de logithèque	Ce type de rapport inclut un rapport de toutes les logithèques du ou des Cores sélectionnés. Vous pouvez également sélectionner une logithèque disponible pour le Core. Ce rapport est uniquement disponible à partir de la console Core, et uniquement depuis la perspective du Core. Pour plus d'informations sur ce type de rapport, voir Comprendre le rapport de logithèque.
Rapport planifié	Vous pouvez également planifier un de ces rapports depuis la console Core. Planifier un rapport entraîne la génération répétée du rapport spécifié sur le programme établi. Vous pouvez également établir des notifications par e-mail à chaque fois qu'un rapport est généré. Pour plus d'informations sur la planification, la modification, la mise en pause ou la suppression de rapports, voir Gestion des rapports planifiés depuis la console Core.

Selon le type de rapport et les paramètres que vous avez sélectionné, vous pouvez générer un rapport sur un ou plusieurs Cores Rapid Recovery ou pour une ou plusieurs machines protégées.

Depuis la Central Management Console, vous pouvez générer un rapport de n'importe quelle combinaison de Cores ou de groupes de Cores configurés dans cette Console.

Génération d'un rapport depuis la console Core

Vous pouvez générer des rapports à la demande depuis la console Core. Les règles suivantes s'appliquent :

- Tous les rapports peuvent être générés depuis la perspective d'un Core.
- De plus, deux types de tâches (le rapport de tâche et le rapport d'échec) peuvent être générés depuis la perspective d'une machine protégée. Pour de tels rapports, seules les données de la machine sélectionnée sont générées.
- Les rapports d'échec contiennent uniquement des données si les tâches des Cores sélectionnés (ou machines protégées) ont échoué.

La méthode de génération des rapports à la demande est similaire, que le rapport soit généré à partir du Core ou de la perspective d'une machine protégée. Cependant, la navigation diffère légèrement.

Vous pouvez également planifier une génération de rapports répétée. Pour plus d'informations sur la planification, la modification, la mise en pause ou la suppression de rapports, voir [Gestion des rapports planifiés depuis la console Core](#).

Génération d'un rapport Core à la demande

Comme indiqué dans la rubrique [À propos des rapports Rapid Recovery](#), vous pouvez générer la gamme complète des rapports disponibles dans la Core Console.

Appliquez les étapes de la procédure suivante pour générer un rapport depuis la vue du Core Rapid Recovery.

- 1 Naviguez jusqu'à la Core Console Rapid Recovery.
- 2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Rapports**.
La page **Rapport de tâche** s'affiche. À droite du nom du rapport dans le titre de page, une flèche vers le bas s'affiche, à partir de laquelle vous pouvez sélectionner un autre type de rapport.

Si vous souhaitez générer un rapport de tâche, passez à l'[Étape 6](#) pour commencer à spécifier les critères de votre rapport.
- 3 Pour choisir un autre type de rapport, cliquez sur la flèche à droite du nom du rapport pour afficher un menu comportant les rapports disponibles.
- 4 Pour la définition des rapports programmés, voir [Planification d'un rapport](#).
- 5 Pour générer un rapport de logithèque uniquement, passez à l'[Étape 11](#).
- 6 Pour un rapport récapitulatif ou un rapport sur la tâche, le récapitulatif de la tâche, les défaillances, sélectionnez une plage de dates à partir du menu déroulant **Plage de dates**.
Lorsque vous ne choisissez pas de plage de dates, l'option par défaut (31 derniers jours) est utilisée. Vous pouvez choisir parmi les options disponibles dans le tableau suivant.

Option	Description
Dernières 24 heures	Relève l'activité du dernier jour, par rapport à l'heure de génération du rapport.
7 derniers jours	Relève l'activité de la dernière semaine, par rapport à l'heure de génération du rapport.
31 derniers jours	Relève l'activité des 31 derniers jours, par rapport à l'heure de génération du rapport.
90 derniers jours	Relève l'activité des 90 derniers jours, par rapport à l'heure de génération du rapport.
Année précédente	Relève l'activité de l'année précédente, par rapport à l'heure de génération du rapport.
Toute la durée	Cette période s'étend sur la totalité de la durée de vie du Core.
Personnalisée	Cette période nécessite que vous indiquiez des dates de début et de fin.
Mois en cours	Relève l'activité depuis le premier jour du mois en cours jusqu'à la date de génération du rapport.
Année en cours	Relève l'activité depuis le premier jour de l'année civile en cours jusqu'à la date de génération du rapport.

REMARQUE : dans tous les cas, aucune donnée de rapport n'est disponible avant le déploiement du logiciel du Core ou avant la protection des machines sur le Core.

- 7 Pour un rapport sur les tâches ou sur les défaillances, à partir du menu déroulant **Cores cibles**, sélectionnez le ou les Core appropriés pour lesquels vous souhaitez générer un rapport.
La sélection par défaut inclut tous les Cores disponibles.
- 8 À partir du menu déroulant **Machines protégées**, sélectionnez la ou les machines pour lesquelles vous souhaitez générer le rapport.
Par défaut, cet ensemble d'informations comprend les tâches pour toutes les machines : chaque machine protégée, machine répliquée et machine comportant uniquement des points de restauration dans les Cores spécifiés. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure des machines. Vous pouvez également sélectionner ou exclure des tâches qui sont indépendantes de la machine, auquel cas le rapport indique uniquement l'état des tâches du Core.

Choisissez parmi les options suivantes :

Option	Description
Sélectionner tout	Cette option sélectionne toutes les machines protégées qui sont protégées sur ce Core.

REMARQUE : vous pouvez sélectionner toutes les machines, puis effacer certaines des sélections pour spécifier un sous-ensemble de toutes les machines.

Option	Description
Indépendant de la machine	Sélectionnez cette option pour générer un rapport comportant les tâches depuis la perspective d'un Core. Les types de tâches, tels que la création ou la suppression d'une logithèque, ou encore la création d'un CD d'amorçage, ne sont pas associés à une machine spécifique. Si le déploiement du logiciel Agent est effectué sur une machine qui n'est pas encore protégée, ce type de tâche est également considéré comme indépendant de la machine. Ces tâches ne répertorient pas une machine protégée dans la colonne Machine protégée du rapport obtenu. En revanche, si vous déployez le logiciel Agent sur une machine qui est déjà protégée dans le Core, le nom de la machine protégée est inclus dans le rapport. Il n'est pas considéré comme indépendant de la machine.
Machines protégées	Cette option répertorie les machines protégées sur ce Core. Vous pouvez toutes les sélectionner, ou sélectionner un sous-ensemble des machines protégées.
Points de restauration uniquement	Cette option répertorie les machines qui ont été protégées dans le passé, mais qui comportent toujours des points de restauration enregistrés dans la logithèque.
[Cores source]	Si votre Core est un Core cible et qu'il réplique les points de restauration des machines protégées sur un Core source, alors le nom de ce Core source s'affiche (en majuscules). Cette option répertorie toutes les machines protégées sur ce Core source. Vous pouvez sélectionner toutes les machines répliquées dans ce Core cible ou un sous-ensemble de celles-ci.
[Groupes personnalisés]	Si vous disposez de groupes personnalisés créés sur ce Core, le nom de chaque groupe personnalisé s'affiche comme une option. Chaque objet de ce groupe personnalisé s'affiche. Vous pouvez sélectionner tous les objets du groupe ou un sous-ensemble de ceux-ci.

9 Si vous générez un rapport récapitulatif, passez à l'[Étape 12](#).

10 Pour un rapport sur la tâche, le récapitulatif de la tâche ou les défaillances, sélectionnez les types de tâches appropriés à partir du menu déroulant **Types de tâches**.

Par défaut, cet ensemble d'informations inclut toutes les tâches pour les machines protégées sélectionnées. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure une tâche de la catégorie Tâches principales et une tâche de la catégorie Autres tâches. Vous pouvez également développer chacune de ces catégories lors de la définition des paramètres de la tâche et sélectionner uniquement les types de tâches depuis la catégorie que vous souhaitez afficher dans le rapport. Cliquez sur la case à cocher d'un type de tâche pour sélectionner ou effacer ce type. Vous pouvez sélectionner plusieurs tâches ou la totalité des tâches d'une catégorie.

Vous pouvez choisir parmi les **autres** types de tâche suivants :

11 Pour un rapport de logithèque, à partir du menu Logithèques, sélectionnez la ou les logithèques que vous souhaitez inclure dans le rapport.

La sélection par défaut inclut toutes les logithèques disponibles.

12 Cliquez sur **Aperçu** pour générer le rapport avec les critères spécifiés.

Si le critère du rapport sélectionné n'est pas trouvé, le rapport est quand même généré, mais il contient une ligne vide. Par exemple, s'il n'y a aucune erreur, le contenu de la colonne Erreur est « null » dans le rapport.

13 Effectuez l'une des opérations suivantes :

- Affichez le rapport généré en ligne.
- Mettez à jour dynamiquement le rapport en modifiant l'un des critères, puis cliquez à nouveau sur **Aperçu**.
- Utilisez le **menu Rapports** pour sélectionner un format d'exportation (y compris PDF, le format par défaut) et cliquez sur  pour exporter le rapport. Pour plus d'informations sur le menu Rapports, voir [Utilisation du menu Rapports](#).
- Utilisez la **barre d'outils Rapports** pour afficher, manipuler ou imprimer le rapport. Pour plus d'informations sur la barre d'outils Rapports, voir [Utilisation de la barre d'outils Rapports](#).

Génération d'un rapport de machine protégée à la demande

Vous pouvez générer un rapport de tâche ou un rapport d'échecs pour n'importe quelle machine protégée.

Suivez les étapes de la procédure suivante pour générer un rapport d'une machine protégée.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 À partir du menu Machines protégées, cliquez sur la machine protégée pour laquelle vous souhaitez générer un rapport.
La page Synthèse de la machine protégée sélectionnée s'affiche.
- 3 En haut de la page, dans les options de menu près du nom de la machine protégée, cliquez sur la flèche dirigée vers le bas près de Rapports, puis sélectionnez un type de rapport.
 - Si vous voulez générer un rapport de toutes les tâches correspondant à cette machine protégée, y compris les tâches en échec, cliquez sur **Rapport de tâche**, et commencez par spécifier vos critères de rapport.
 - Si vous voulez générer un rapport de toutes les tâches en échec correspondant à cette machine protégée, cliquez sur **Rapport de tâche** et commencez par spécifier vos critères de rapport.
- 4 Pour un rapport sur les tâches ou les échecs, sélectionnez une plage de dates à partir du menu déroulant **Plage de dates**.
Lorsque vous ne choisissez pas une plage de dates, l'option par défaut (31 derniers jours) est utilisée. Vous pouvez choisir parmi les options disponibles dans le tableau suivant.

Option	Description
Dernières 24 heures	Relève l'activité du dernier jour, par rapport à l'heure de génération du rapport.
7 derniers jours	Relève l'activité de la dernière semaine, par rapport à l'heure de génération du rapport.
31 derniers jours	Relève l'activité des 31 derniers jours, par rapport à l'heure de génération du rapport.
90 derniers jours	Relève l'activité des 90 derniers jours, par rapport à l'heure de génération du rapport.
Année précédente	Relève l'activité de l'année précédente, par rapport à l'heure de génération du rapport.
Toute la durée	Cette période s'étend sur la totalité de la durée de vie du Core.
Personnalisée	Cette période nécessite que vous spécifiez les dates de début et de fin.
Mois en cours	Relève l'activité depuis le premier jour du mois en cours jusqu'à la date de génération du rapport.
Année en cours	Relève l'activité depuis le premier jour de l'année civile en cours jusqu'à la date de génération du rapport.

REMARQUE : Dans tous les cas, aucune donnée de rapport n'est disponible avant le déploiement du logiciel du Core ou avant la protection des machines sur le Core.

- 5 Depuis le menu déroulant **Types de tâches**, sélectionnez les types de tâche appropriés.
Par défaut, cet ensemble d'informations inclut toutes les tâches pour les machines protégées sélectionnées. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure une tâche de la catégorie Tâches principales et une tâche de la catégorie Autres tâches. Vous pouvez également développer chacune de ces catégories lors de la définition des paramètres de la tâche et sélectionner uniquement les types de tâches depuis la catégorie que vous souhaitez afficher dans le rapport. Cliquez sur la case à cocher d'un type de tâche pour sélectionner ou effacer ce type. Vous pouvez sélectionner plusieurs tâches ou la totalité des tâches d'une catégorie.
- 6 Cliquez sur **Aperçu** pour générer le rapport avec les critères spécifiés.
Si le critère de rapport sélectionné n'est pas trouvé, le rapport est quand même généré, mais il contient une ligne vide. Par exemple, s'il n'y a aucune erreur, le contenu de la colonne Erreur est « null » dans le rapport.
- 7 Effectuez l'une des opérations suivantes :
 - Affichez le rapport généré en ligne.
 - Mettez à jour dynamiquement le rapport en modifiant l'un des critères ; puis cliquez à nouveau sur **Aperçu**.
 - Utilisez le **menu Rapports** pour sélectionner un format d'exportation et d'exporter le rapport. Pour plus d'informations sur la barre d'outils, voir [Utilisation du menu Rapports](#).
 - Utilisez la **barre d'outils Rapports** pour afficher, manipuler ou imprimer le rapport. Pour plus d'informations sur la barre d'outils, voir [Utilisation de la barre d'outils Rapports](#).

Gestion des rapports planifiés depuis la console Core

Vous pouvez planifier tout rapport disponible dans la console Core. Planifier un rapport entraîne la répétition de sa génération dans le futur. La planification définit si la génération du rapport doit s'effectuer quotidiennement, hebdomadairement ou mensuellement.

De plus, Rapid Recovery vous permet d'envoyer une notification par e-mail à un ou plusieurs destinataires lorsque de la génération de chaque rapport. L'e-mail spécifie le type de rapport, le format de rapport et la plage de dates, il inclut également le rapport en pièce jointe.

REMARQUE : Avant de pouvoir envoyer les rapports par e-mail, vous devez configurer un serveur SMTP pour le Core. Pour plus d'informations, voir [Configurer un serveur de messagerie électronique](#).

Que vous choisissiez ou non d'envoyer les notifications par e-mail, vous pouvez enregistrer les rapports générés localement ou sur un emplacement réseau accessible par le serveur Core.

Vous devez spécifier la notification et la livraison des e-mails, ou vous devez spécifier un emplacement où enregistrer des rapports. Vous pouvez également choisir ces deux options.

Cette section contient les rubriques suivantes :

Liens connexes

[Planification d'un rapport](#)

[Modification d'une planification de rapport](#)

[Mise en pause, reprise ou suppression d'un rapport planifié](#)

Planification d'un rapport

Vous pouvez planifier un rapport disponible depuis la Core Console. Le rapport est alors généré sur les horaires que vous avez définis jusqu'à ce que vous interrompiez ou supprimiez le rapport.

Vous devez spécifier la notification et la livraison des e-mails, ou vous devez spécifier l'emplacement où enregistrer des rapports. Vous pouvez également choisir ces deux options.

Effectuez cette procédure pour planifier un rapport.

- 1 Accédez à la Rapid Recovery Core Console.
- 2 Sur la barre d'icônes, cliquez sur  (Plus), puis sélectionnez **Rapports**.
La page **Rapport de tâche** s'affiche. Une flèche vers le bas s'affiche à droite du nom du rapport sélectionné.
- 3 Cliquez sur la flèche située à droite du nom du rapport, puis, à partir du menu déroulant, sélectionnez **Rapports programmés**.
La page **Rapports programmés** s'affiche.
- 4 Pour planifier un rapport en vue de le générer plusieurs fois, cliquez sur **Ajouter**.
L'Assistant de définition de planification de rapports s'affiche.
- 5 Sur la page **Configuration** de l'Assistant, entrez les détails du rapport que vous souhaitez planifier, puis cliquez sur **Suivant**. Les options de configuration sont décrites dans le tableau suivant.

Tableau 161. Options de configuration du rapport programmé

Machine	Rapports disponibles
Nom	Entrez le nom d'affichage que vous souhaitez attribuer à cette planification. Le nom par défaut est Rapport planifié 1. Limitez votre nom à un maximum de 64 caractères. N'utilisez pas caractères interdits ou expressions interdites .
Format de rapport	Sélectionnez un rapport de sortie de rapport. Si vous ne sélectionnez pas de valeur, le format par défaut (pdf) est utilisé.
Type de rapport	Sélectionnez le type de rapport que vous souhaitez générer de manière répétée.
Libellés	Sélectionnez les libellés que vous voulez afficher sur le rapport planifié. Au moins une étiquette est nécessaire.

Machine	Rapports disponibles
	La fonction Groupes personnalisés vous permet de regrouper les objets du Core dans un conteneur logique, pour lequel vous définissez un libellé. À l'aide du paramètre Libellés de l'Assistant de définition de planification de rapports, vous pouvez sélectionner un groupe personnalisé pour lequel les rapports planifiés seront exécutés. Si aucun libellé personnalisé n'existe, les options disponibles dans le menu déroulant Libellés incluent les options Tout sélectionner et Machines protégées. Si des groupes personnalisés s'affichent, chaque groupe s'affiche comme une option. Vous pouvez sélectionner ou désélectionner les options pour inclure ou exclure ces objets dans le rapport planifié.
Machine protégée	Sélectionnez une ou plusieurs machines protégées à inclure dans le rapport. Cette option n'est pas disponible pour le rapport de logithèque.
Types de tâches	Sélectionnez les types de tâches que vous souhaitez afficher dans le rapport. Par défaut, cet ensemble d'informations comprend les tâches pour toutes les machines : chaque machine protégée, machine répliquée et machine comportant uniquement des points de restauration dans les Cores spécifiés. Dans les paramètres du rapport, vous pouvez personnaliser le rapport. Utilisez les filtres pour sélectionner ou exclure des machines. Vous pouvez également sélectionner ou exclure des tâches qui sont indépendantes de la machine, auquel cas le rapport indique uniquement l'état des tâches du Core. Le paramètre Types de tâche n'est pas disponible pour les types de rapport planifiés Récapitulatif du Core et Logithèque.

6 Sur la page **Destination** de l'Assistant, sélectionnez une destination pour les rapports que vous souhaitez planifier. Vous devez choisir l'une des options suivantes et pouvez sélectionner les deux. Une fois les sélections effectuées, cliquez sur **Suivant**.

- Dans le champ **Adresse e-mail de destination**, saisissez une ou plusieurs adresses e-mail valides pour prévenir les utilisateurs par e-mail lorsqu'un rapport planifié est généré.

REMARQUE : Si vous ne spécifiez pas la notification et la livraison des e-mails, vous devez alors spécifier un emplacement de stockage.

- Sélectionnez **Enregistrer comme fichier** pour enregistrer les fichiers du rapport généré dans un emplacement que vous spécifiez. Dans le menu déroulant **Type d'emplacement**, sélectionnez un emplacement local, réseau ou sur le cloud. Ensuite, dans le champ **Emplacement**, spécifiez des informations supplémentaires sur l'emplacement tel que décrit dans le tableau suivant.

Tableau 162. Options d'emplacement pour les rapports planifiés

Type d'emplacement	Description du type d'emplacement	Emplacement
Local	Sélectionnez le type d'emplacement Local pour enregistrer des rapports générés dans un chemin local accessible pour le Core.	Spécifiez le chemin d'accès dans le champ Emplacement. Entrez un emplacement accessible localement pour le Core. Par exemple, pour stocker les rapports dans le dossier Rapports du lecteur D, entrez D:\Reports\.
Réseau	Sélectionnez le type d'emplacement Réseau pour enregistrer des rapports générés dans un chemin accessible au Core sur le réseau. Spécifiez le chemin d'accès dans le champ Emplacement.	Spécifiez le chemin d'accès dans le champ Emplacement. Entrez un emplacement accessible pour le Core à partir du réseau. Utilisez le format \\servername\sharename. Par exemple, pour stocker des rapports sur le serveur de données dans le dossier partagé nommé Rapports, entrez \Data\Reports\. Spécifiez les identifiants réseau dans les champs Nom d'utilisateur et Mot de passe.

Type d'emplacement	Description du type d'emplacement	Emplacement
Cloud	Sélectionnez le type d'emplacement Cloud pour enregistrer les rapports générés dans un compte de stockage Cloud configuré dans le Core. Le compte de stockage doit déjà être défini avant d'effectuer cette étape. Pour plus d'informations sur la configuration d'un compte de stockage Cloud et la liaison de celui-ci avec le Core, voir Gestion des comptes Cloud.	Dans le champ Account (Compte), sélectionnez le compte de stockage Cloud approprié à utiliser pour stocker les rapports générés. À partir du champ Conteneur, spécifiez un conteneur approprié dans le compte de stockage. Dans le champ Nom du dossier, spécifiez un dossier dans lequel stocker les futurs rapports générés.

- 7 Une fois vos options de Destination définies, cliquez sur **Suivant**.
- 8 Sur la page **Planification** de l'Assistant, à partir du menu **Envoyer les données**, sélectionnez une option pour déterminer la fréquence de génération du rapport spécifié. Vous pouvez générer des rapports tous les jours, toutes les semaines ou tous les mois. Chaque option possède ses propres paramètres, comme cela est décrit dans le tableau suivant.

Tableau 163. Options de fréquence de génération des rapports planifiés

Fréquence	Détails de la fréquence	Paramètres de la fréquence
Tous les jours	Génère et enregistre ou envoie le rapport spécifié une fois par jour à l'heure indiquée. L'heure par défaut pour cette action est 12 h 00 (en fonction de l'heure du serveur Core).	Pour modifier l'heure de génération du rapport par défaut, dans la zone de texte de l'heure, entrez une nouvelle valeur ou utilisez les commandes pour changer l'heure, ainsi que l'indicateur du matin/après-midi.
Toutes les semaines	Génère et enregistre/envoie le rapport spécifié une fois par semaine à l'heure définie de la journée indiquée. L'heure par défaut pour cette action est le dimanche à 12 h 00 (en fonction de l'heure du serveur Core).	Pour modifier le jour de génération du rapport par défaut, à partir du menu du jour de la semaine, sélectionnez un jour de la semaine. Pour modifier l'heure de génération du rapport par défaut, dans la zone de texte de l'heure, entrez une nouvelle valeur ou utilisez les commandes pour changer l'heure, ainsi que l'indicateur du matin/après-midi.
Tous les mois	Génère et enregistre/envoie le rapport spécifié une fois par mois à l'heure définie de la journée indiquée. La date par défaut pour cette action est le premier de chaque mois à 12 h 00 (en fonction de l'heure du serveur Core).	Pour modifier la date par défaut de génération du rapport, à partir du menu Jour du mois, sélectionnez une date. Pour modifier l'heure de génération du rapport par défaut, dans la zone de texte de l'heure, entrez une nouvelle valeur ou utilisez les commandes pour changer l'heure, ainsi que l'indicateur du matin/après-midi.

- 9 Facultativement, sur la page **Planification** de l'Assistant, si vous voulez empêcher le rapport planifié de se générer jusqu'à la reprise des rapports mis en pause, sélectionnez **Suspendre initialement les rapports**.
Si vous souhaitez que ce rapport se génère de la manière planifiée, décochez cette option.
- 10 Lorsque vous êtes satisfait de votre planification, cliquez sur **Terminer** pour quitter l'assistant et enregistrer votre travail.
La nouvelle planification de rapport s'affiche dans le tableau récapitulatif Rapport récapitulatif.

Modification d'une planification de rapport

Une fois le rapport planifié, vous pouvez modifier ses paramètres ou ses détails. Vous pouvez modifier les informations de la configuration du rapport (nom du rapport, format de sortie, type de rapport, logithèques incluses). Vous pouvez également modifier les options de notification par e-mail et la destination de sauvegarde du rapport généré. Enfin, vous pouvez également modifier la planification du rapport.

Suivez les étapes de cette procédure pour modifier les paramètres d'un rapport planifié.

- 1 Accédez à la console Core Rapid Recovery.
- 2 À partir de la barre d'icônes, cliquez sur , puis sélectionnez **Rapports**.
La page **Rapport de tâche** s'affiche. Une flèche vers le bas s'affiche à droite du nom du rapport sélectionné.
- 3 Cliquez sur la flèche située à droite du nom du rapport, puis, à partir du menu déroulant, sélectionnez **Rapports programmés**.
La page **Rapports programmés** s'affiche.
- 4 Dans le tableau récapitulatif des rapports planifiés, depuis la ligne du rapport que vous souhaitez modifier, cliquez sur l'icône Paramètres , puis sélectionnez **Modifier**.
L'Assistant de définition de planification de rapports s'affiche.
- 5 Naviguez dans les pages de cet Assistant, modifiez l'un des paramètres nécessaires. Pour plus d'informations sur les paramètres de cet Assistant, voir la rubrique [Planification d'un rapport](#).
- 6 Dans la page **Planification** de l'Assistant, cliquez sur **Terminer** pour fermer l'Assistant et enregistrer vos modifications.
L'Assistant se ferme, la planification de rapport est modifiée.

Mise en pause, reprise ou suppression d'un rapport planifié

Une fois le rapport planifié, il se génère sur le programme défini. Si vous souhaitez interrompre temporairement la génération d'un rapport planifié, vous pouvez mettre en pause la planification.

Si un rapport planifié est suspendu, et si vous souhaitez reprendre la génération du rapport, vous pouvez alors reprendre le rapport comme indiqué dans cette procédure.

Si vous êtes actuellement en train de générer un rapport planifié, et n'avez plus besoin de générer ce rapport, vous pouvez le supprimer.

Pour déterminer si un rapport planifié est suspendu, vérifiez la colonne État dans le tableau récapitulatif des rapports planifiés. Un voyant vert indique qu'un rapport à planification active ; une sphère jaune indique une planification suspendue ; et une sphère rouge indique une erreur.

Effectuez cette procédure pour mettre en pause, reprendre ou supprimer une planification d'un rapport.

- 1 Accédez à la console Core Rapid Recovery.
- 2 À partir de la barre d'icônes, cliquez sur , puis sélectionnez **Reports (Rapports)**.
La page **Rapport de tâche** s'affiche. Une flèche vers le bas s'affiche à droite du nom du rapport sélectionné.
- 3 Cliquez sur la flèche située à droite du nom du rapport, puis, à partir du menu déroulant, sélectionnez **Scheduled Reports (Rapports programmés)**.
La page **Scheduled Reports (Rapports programmés)** s'affiche.
- 4 Dans le tableau récapitulatif des rapports planifiés, affichez l'état de tous les rapports planifiés à l'aide des indicateurs colorés.
- 5 Pour chaque rapport que vous souhaitez suspendre ou reprendre, cochez la case dans la première colonne.
- 6 Depuis la fenêtre Rapports planifiés située au-dessus du tableau récapitulatif des options, effectuez l'une de opérations suivantes :
 - Pour interrompre la génération des rapports sélectionnés, cliquez sur **Pause**.
 - Pour reprendre la génération de rapports planifiés qui ont été interrompues, cliquez sur **Reprendre**.
 - Pour supprimer les planifications sélectionnées pour les rapports planifiés existants, cliquez sur **Supprimer**.
Supprimer un rapport planifié prévient uniquement la génération des rapports ultérieurs. Si les rapports planifiés précédents ont été enregistrés, ils ne seront pas supprimés.

Utilisation du menu Rapports

Le menu Rapports s'affiche dans la partie supérieure de la page lors de l'affichage des rapports. Ce menu inclut un titre de rapport, qui est également un menu déroulant vous permettant de voir les types de rapport disponibles. Sous ce menu se trouvent un ou plusieurs filtres qui vous aideront à définir vos critères de rapport.

Les filtres spécifiques disponibles dépendent du type de rapport. Pour plus d'informations sur les paramètres qui s'appliquent à chaque type de rapport, voir la rubrique correspondante à ce type de rapport.

Sur le côté droit du menu Rapports, certaines commandes s'affichent. Ces commandes, qui sont décrites dans le tableau suivant, vous aident à générer et exporter le rapport.

Tableau 164. Commandes du menu Rapports

Élément de l'IU	Description
Bouton Aperçu	Cliquez sur le bouton Aperçu pour générer un rapport basé sur le type de rapport sélectionné et sur les paramètres de rapport spécifiés dans les filtres.
Menu déroulant Format d'exportation	Le menu déroulant Exportation vous permet de sélectionner un format de sortie pour le rapport . Si vous ne sélectionnez pas une valeur, le format par défaut (pdf) est utilisé.
Bouton/icône Télécharger	Le bouton Télécharger permet d'exporter le rapport généré dans le type de format sélectionné sous le menu Exportation.

Les rapports comprennent maintenant des unités de mesure, ce qui permet de déterminer plus facilement si une colonne est exprimée en Go, en To ou en secondes.

Si vous n'êtes pas satisfait de l'apparence d'un rapport exporté ou généré, vous pouvez modifier la police utilisée dans les rapports. Pour plus d'informations, voir [Gestion des paramètres des rapports](#).

Une fois le rapport généré, vous pouvez utiliser la barre d'outils des rapports.

Liens connexes

[Comprendre le rapport de tâche](#)

[Comprendre le rapport des échecs](#)

[Comprendre le rapport récapitulatif](#)

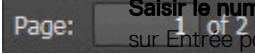
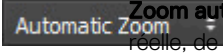
[Comprendre les rapports de noyau de la Console de gestion centrale](#)

Utilisation de la barre d'outils Rapports

Une fois généré depuis le menu Rapports, le rapport s'affiche sous une barre d'outils Rapports. La barre d'outils peut vous permettre de gérer la sortie des rapports, notamment pour les enregistrer et les imprimer.

Sur la gauche de la barre d'outils se trouve une option de basculement de la barre latérale. Cet outil développe ou réduit la barre latérale, ce qui permet d'accéder à davantage d'options d'affichage. À droite de la barre d'outils, l'option Outils développe un menu déroulant fournissant des commandes de navigation dans le rapport. Les éléments de la barre d'outils Rapports sont présentés dans le tableau suivant.

Tableau 165. Icônes de la barre d'outils des rapports

Icône	Description
	Basculement de la barre latérale. Toutes les pages du rapport s'affichent en tant que miniatures. Les autres options de la barre latérale ne sont pas prises en charge.
	Barre latérale : afficher les miniatures. Il s'agit de la vue par défaut de toutes les pages d'un rapport généré.
	Barre latérale : afficher l'aperçu du document. Cette fonction n'est pas prise en charge.
	Barre latérale : afficher les pièces jointes. Les rapports ne comportent pas de pièces jointes. Cette fonction n'est pas prise en charge.
	Rechercher. Permet de rechercher du texte dans le rapport généré. Contient des options permettant de mettre en surbrillance tout le texte correspondant aux critères saisis et de respecter ou d'ignorer la casse.
	Page précédente. Revenir à la page précédente dans la vue du rapport.
	Page suivante. Accéder à la page suivante dans la vue du rapport.
	Saisir le numéro de page. Cliquez sur le champ de texte Numéro de page, saisissez un numéro de page valide, puis appuyez sur Entrée pour accéder à la page en question dans la vue du rapport.
	Zoom arrière. Permet d'effectuer un zoom arrière dans vue du rapport généré. Chaque clic successif permet de dézoomer davantage, jusqu'à 25 %.
	Zoom avant. Permet d'effectuer un zoom avant dans vue du rapport généré. Chaque clic successif permet de zoomer davantage, jusqu'à 1 000 %.
	Zoom automatique. Permet de contrôler le niveau de zoom dans la vue du rapport généré, de sorte à l'afficher en taille réelle, de manière adaptée à la page ou en pleine largeur ; ou encore en définissant un pourcentage, par exemple 50 %, 75 %, 100 %, 125 %, 150 %, 200 %, 300 % ou 400 %.
	Ouvrir un fichier. Permet de parcourir votre système de fichiers pour rechercher et ouvrir un rapport enregistré.
	Imprimer. Permet d'imprimer le rapport généré.
	Outils. Lorsque vous cliquez sur cette icône, le menu déroulant Outils se développe ou se réduit. Les options du menu Outils sont présentées ci-après.
	Outils : accéder à la première page. Vous conduit à la première page du rapport généré.
	Outils : accéder à la dernière page. Vous conduit à la dernière page du rapport généré.
	Outils : faire pivoter dans le sens des aiguilles d'une montre. Cette option fait pivoter le canevas du rapport généré dans le sens horaire.

Icône	Description
	Outils : faire pivoter dans le sens inverse des aiguilles d'une montre. Cette option fait pivoter le canevas du rapport généré dans le sens antihoraire.
	Outils : outil Main. Lorsque vous sélectionnez cet outil, il vous permet de déplacer le rapport en cliquant dessus et en le faisant glisser sur l'écran.
	Outils : propriétés du document. Fournit des informations sur les propriétés de document du rapport généré. Cliquez sur Fermer pour fermer la fenêtre.

Pour en savoir plus sur la génération d'un rapport, voir [Génération d'un rapport depuis la console Core](#). Pour en savoir plus sur la génération d'un rapport pour plusieurs Cores dans la console de gestion centrale, voir [Générer un rapport à partir de Central Management Console](#).

Comprendre le rapport de tâche

Le rapport de tâche est disponible pour le Core Rapid Recovery et pour les machines protégées sur le Core. Ce rapport vous fournit une méthode de visualisation des états des tâches effectuées par un Core ou machine protégée sélectionnée. Les lignes ou colonnes de données qui s'affichent dans le rapport et ne contenant aucune donnée indiquent que le paramètre testé était null. Par exemple, si une colonne (telles que Erreurs) s'affiche et ne contient aucune information, aucune erreur n'est s'est produite pour l'enregistrement sélectionné. Si le rapport génère une ligne vide, la tâche de l'enregistrement sélectionné reflète l'activité de la machine.

Pour plus d'informations sur la génération d'un rapport de tâche sur le Core, voir [Génération d'un rapport Core à la demande](#). Pour plus d'informations sur la génération d'un rapport de tâche sur une machine protégée, voir [Génération d'un rapport de machine protégée à la demande](#).

Lorsque vous générez un rapport de tâche, les détails du rapport comprennent les éléments suivants :

- Critères de sélection pour le rapport
- Un tableau récapitulatif montrant une ligne pour chaque tâche dans la plage de dates spécifiée. En plus de répertorier le Core, la machine protégée et type de tâche appropriés, chaque ligne comprend :
 - La synthèse de la tâche
 - L'état de la tâche
 - Toutes les erreurs liées à la tâche
 - Les dates de début et de fin de la tâche
 - La durée en secondes de la tâche
 - Le travail total en Mo

Si les informations sont pas liées à une catégorie spécifique, cette cellule s'affiche sans informations dans le rapport. Par exemple, si le Core pour une machine protégée spécifié n'a aucune erreur, la colonne Erreur est vide pour cette ligne du rapport.

Présentation du rapport récapitulatif des tâches

Le rapport récapitulatif des tâches est disponible lors de la génération de rapport uniquement du point de vue du Core. Ce rapport n'est pas disponible à partir des rapports concernant une machine protégée. Ce rapport contient un seul récapitulatif, qui fournit des informations récapitulatives sur toutes les tâches effectuées sur le Core, notamment le nombre de tâches ayant échoué et réussi, ainsi que celles qui ont été annulées. Il est plus détaillé que le rapport de tâche, car il spécifie chaque tâche dans une ligne distincte dans le rapport.

Pour en savoir plus sur la génération d'un rapport récapitulatif des tâches, voir [Génération d'un rapport depuis la console Core](#).

Les paramètres du rapport pour ce type de rapport comprennent :

- Plage de dates
- Machines protégées
- Types de tâche

Lorsque vous générez un rapport récapitulatif des tâches, les détails de ce rapport incluent les critères de sélection du rapport, ainsi que des informations relatives aux machines protégées, aux volumes et aux types de tâche.

Informations sur le Core

La section Core du rapport récapitulatif contient des données concernant le Core Rapid Recovery faisant l'objet d'un rapport. Cette information comprend :

- Nombre de machines protégées dans le Rapid Recovery Core
- Le nombre de machines incluant des tâches ayant échoué

Synthèse des machines protégées

La section Machines protégées du rapport récapitulatif contient des données relatives à toutes les machines protégées par le Rapid Recovery Core sélectionné et les volumes sur ces machines.

Le diagramme affiche une ligne pour chaque type de tâche de chaque machine. Il indique le taux de tâches réussies (tout type confondu), le nombre de tâches réussies, le nombre de tâches ayant échoué et les tâches annulées. (Les tâches annulées ne sont pas prises en compte dans ces statistiques.)

Comprendre le rapport des échecs

Le rapport des échecs est un sous-ensemble du rapport de tâche, il est disponible sur le Core Rapid Recovery et sur les machines protégées sur le Core. Un rapport d'échec inclut uniquement les tâches annulées et ayant échouées répertoriées dans le rapport de tâche, et il les compile dans un rapport unique qui peut être imprimé et exporté. Si le rapport se génère avec une ligne vide, il n'y a pas d'erreurs au sein de la plage de dates spécifiée dans vos critères de rapport.

❗ REMARQUE : Les résultats pour les paramètres relatifs aux Cores cibles et aux machines protégées s'affichent uniquement pour le rapport au niveau du Core.

Pour plus d'informations sur la génération d'un rapport de tâche sur le Core, voir [Génération d'un rapport Core à la demande](#). Pour plus d'informations sur la génération d'un rapport de tâche sur une machine protégée, voir [Génération d'un rapport de machine protégée à la demande](#).

Lorsque vous générez un rapport des échecs, un tableau récapitulatif s'affiche, il indique une ligne pour chaque tâche de la plage de dates spécifiée. En plus de répertorier le Core, la machine protégée et type de tâche appropriés, chaque ligne comprend :

- La synthèse de la tâche
- L'état de la tâche
- Toutes les erreurs liées à la tâche
- Les dates de début et de fin de la tâche
- La durée en secondes de la tâche
- Le travail total en Mo

Comprendre le rapport récapitulatif

Le rapport récapitulatif est disponible pour un ou plusieurs Cores. Ce rapport n'est pas disponible à partir des rapports d'une machine protégée. Le rapport récapitulatif contient des informations sur les logithèques présentes sur le Core Rapid Recovery sélectionné et sur les machines protégées par ce Core. Les informations présentées s'affichent sous forme de deux synthèses dans un rapport.

Pour en savoir plus sur la génération d'un rapport récapitulatif, voir [Génération d'un rapport depuis la console Core..](#)

Les paramètres de ce type de rapport incluent les suivants :

- Plage de dates
- Machines protégées

Lorsque vous générez un rapport récapitulatif, les détails de ce rapport incluent les critères de sélection du rapport, ainsi que des informations relatives aux logithèques et aux machines protégées.

Informations sur le Core

La section Core du rapport récapitulatif contient des données concernant le Core Rapid Recovery faisant l'objet d'un rapport. Cette information comprend :

- La clé de licence (identificateur)
- La version actuelle du logiciel du Core Rapid Recovery

Synthèse des logithèques

La section Logithèques du rapport récapitulatif comprend des données relatives aux logithèques se trouvant sur le Core Rapid Recovery sélectionné. Cette information comprend :

- Le nombre de logithèques du Core Rapid Recovery
- Une synthèse des logithèques du Core.

Synthèse des machines protégées

La section Machines protégées du rapport récapitulatif contient des données relatives à toutes les machines protégées par le ou les Cores Rapid Recovery sélectionnés. Cela inclut un graphique et un tableau récapitulatif.

Le graphique affiche les machines protégées en indiquant le rapport tâches réussies (quel qu'en soit le type)/tâches échouées. (Les tâches annulées ne sont pas prises en compte dans ces statistiques.)

X, l'axe horizontal, indique le nombre de machines protégées. Y, l'axe vertical, indique les niveaux de réussite. Plus précisément, l'axe Y indique, parmi les machines protégées, combien ont :

- effectué aucune tâche ;
- moins de 50 % de succès ;
- 50 % de succès ou plus ;
- un taux de réussite de 100 %.

Des informations sur les machines protégées s'affichent en dessous du graphique. Cette information comprend :

- La quantité de machines protégées

- Le nombre de machines protégées incluant des tâches ayant échoué
- Un tableau récapitulatif indiquant, pour chaque machine protégée :
 - Le nom de la machine protégée
 - Les volumes protégés par la machine
 - L'espace protégé (total et actuel), en Go
 - Le taux de changement quotidien (moyen et médian)
 - Les statistiques de tâche (réussite, fin, échec, annulation)
 - Si un chiffrement a été appliqué
- La version du Core

Comprendre le rapport de logithèque

Le rapport de logithèque contient des informations sur les logithèques présentes sur le Core Rapid Recovery sélectionné et sur les machines protégées par ce Core. Les informations présentées s'affichent sous forme de deux synthèses dans un rapport.

Pour plus d'informations sur la génération d'un rapport de logithèque sur le Core, voir [Génération d'un rapport Core à la demande](#).

Les paramètres du rapport pour ce type de rapport comprennent uniquement les logithèques.

Lorsque vous générez un rapport sur les logithèques, ce rapport inclut, pour chaque logithèque, une liste récapitulative des logithèques sur le Core.

Central Management Console

La Rapid Recovery Central Management Console est un composant facultatif destiné aux environnements ayant deux ou plusieurs Cores Rapid Recovery. Ce composant est un portail Web fournissant une interface centrale où vous pouvez grouper, gérer et générer les rapports de plusieurs Cores.

Les exigences de système d'exploitation pour la Central Management Console sont identiques à celles relatives au Core Rapid Recovery. Ces composants peuvent être installés sur la même machine ou sur des machines différentes, selon vos besoins.

Après l'installation, vous devez configurer la Central Management Console en ajoutant les Cores que vous souhaitez gérer, individuellement ou dans le cadre de groupes de Cores.

❗ REMARQUE : Vous devez exécuter le programme d'installation avec les privilèges d'administrateur local.

Les systèmes d'exploitation Windows 8, 8.1 et 10, et Windows Server 2012 et 2012 R2 doivent avoir la fonction ASP.NET 4.5 installée sur le serveur pour un chargement correct de l'interface graphique. Cette configuration est incluse dans le programme d'installation de Rapid Recovery.

Pour plus d'informations sur l'installation de ce composant, voir la rubrique « Installation de la Rapid Recovery Central Management Console » du guide d'installation et de mise à jour de *Dell Data Protection | Rapid Recovery*.

Pour plus d'informations sur la configuration de ce composant, voir la rubrique [Configuration de la Rapid Recovery Central Management Console](#) de guide d'utilisation de *Dell Data Protection | Rapid Recovery*.

Pour plus d'informations sur l'interface utilisateur de ce composant, voir la rubrique [Compréhension de la Rapid Recovery Central Management Console](#) du guide d'utilisation de *Dell Data Protection | Rapid Recovery*.

Compréhension de la Rapid Recovery Central Management Console

Lorsque vous ouvrez la Central Management Console, les informations s'affichent dans la vue Console. La page **Bienvenue** s'affiche, et vous pouvez voir les éléments suivants :

Tableau 166. Éléments d'interface utilisateur dans la Rapid Recovery Central Management Console

Élément de l'IU	Description
Zone de la marque	Pour les environnements typiques, la partie supérieure gauche de la Central Management Console contient le nom du produit parent complet, Dell Data Protection Rapid Recovery. Si l'utilisateur du navigateur Web clique sur n'importe quelle partie de la zone du nom, il est dirigé vers la documentation du produit sur le site Web du support technique de Dell.
Zone de navigation gauche	La zone de navigation gauche s'affiche sous la zone de la marque, sur le côté gauche de l'interface utilisateur. Les fonctions de la zone de navigation varient selon le mode sélectionné dans la partie supérieure droite de la Central Management Console. Mode console. Dans la zone de navigation, en mode console, le fait de cliquer sur n'importe quel Core ou groupe de Cores ouvre le Core ou le groupe de Cores sélectionné dans la Rapid Recovery Core Console. Mode rapports. Dans la zone de navigation, en mode rapports, le fait de sélectionner les Cores ou groupes de Cores détermine l'ensemble des informations qui s'affichent à la génération des rapports. Mode gestion. Dans la zone de navigation, en mode gestion, vous pouvez parcourir les paramètres des Cores et des groupes de Cores. Vous pouvez également ajouter et supprimer des Cores et des groupes de Cores en mode gestion. Cliquez sur les flèches pour développer et réduire le menu. Les niveaux suivants de la hiérarchie sont inclus : Organisation, Groupes de Cores et Cores. Si vous cliquez sur la flèche gauche, la zone de navigation se réduit. Pour développer la zone de navigation, cliquez sur la flèche droite.
Menu Liens	Contactez le service de support Dell. Lien vers le site web du support technique de Dell dans une nouvelle fenêtre de navigateur, qui permet de discuter en direct avec un technicien et propose des didacticiels vidéo, des articles de la base de connaissances de Rapid Recovery, une foire aux questions, et plus encore.
Menu Liens	Documentation. Lien vers le site web du support technique de Dell dans une nouvelle fenêtre de navigateur, qui permet de discuter en direct avec un technicien et propose des didacticiels vidéo, des articles de la base de connaissances de Rapid Recovery, une foire aux questions, et plus encore.
Menu Liens	Versión. Répertoire la version actuelle de la Central Management Console. Le fait de cliquer sur ce lien ouvre la boîte de dialogue À propos.
Menu Liens	Sélecteur de mode. Le nom de l'utilisateur Windows actuellement connecté s'affiche dans un menu déroulant, dans la partie supérieure droite du menu de liens. Ce menu vous permet de modifier la vue de la Central Management Console. Vous pouvez choisir parmi les vues suivantes : Console. Il s'agit du mode par défaut, vous permettant d'afficher les Cores et groupes de Cores dans votre environnement à partir d'un seul endroit. Rapports. Ce mode vous permet de générer, d'afficher et d'exporter les rapports à partir des Cores configurés dans cette console. Gérer. Le mode Gérer vous permet de supprimer ou d'ajouter d'autres Cores à la Central Management Console, seuls ou en groupes. Langue. Dans les versions qui prennent en charge la localisation, l'option Langue est répertoriée. Cette option permet d'ouvrir la boîte de dialogue Changer de langue, dans laquelle vous pouvez sélectionner une langue d'affichage pour la Central Management Console. .

Élément de l'UI	Description
	Effacer le cache du compte. Sélectionnez cette option pour effacer les informations existantes pour le compte d'utilisateur connecté.

Vous pouvez modifier la vue de la Central Management Console en sélectionnant une option dans le sélecteur de mode (menu déroulant dans le coin supérieur droit de la page). Par exemple :

- Pour gérer les Cores ou groupes de Cores qui sont déjà configurés, utilisez la vue Console.
- Pour configurer la Central Management Console, basculez vers la vue Gérer.
- Pour générer des rapports, basculez vers la vue Rapports.

Les Cores que vous pouvez afficher et gérer s'affichent dans le menu de navigation gauche. Vous pouvez configurer les Cores individuels ou les organiser par groupes. Vous pouvez restreindre l'accès aux Cores dans des groupes spécifiques en utilisant les noms d'utilisateur Windows ou groupes.

Configuration de la Rapid Recovery Central Management Console

La configuration de la Rapid Recovery Central Management Console consiste à ajouter des Cores et des groupes de Cores, à définir leurs paramètres et à spécifier les paramètres d'accès aux groupes (le cas échéant).

Une fois la configuration terminée, vous pourrez gérer les paramètres et tous les Cores depuis un même emplacement central.

Pour configurer la Central Management Console, vous pouvez effectuer toutes les tâches répertoriées dans Liens associés ci-dessous.

Liens connexes

- [Ajout d'un Core à la Central Management Console](#)
- [Configuration des paramètres du Core dans la Central Management Console](#)
- [Ajout d'un groupe de Cores à la Central Management Console](#)
- [Configuration des paramètres du groupe de Cores](#)
- [Configuration de l'accès au groupe de Cores](#)

Ajout d'un Core à la Central Management Console

Si vous souhaitez ajouter un Core à un groupe de Cores, le groupe doit être créé au préalable. Pour plus d'informations, voir [Ajout d'un groupe de Cores à la Central Management Console](#). Vous pouvez également modifier ultérieurement les détails du Core pour spécifier un groupe.

Ajoutez un ou plusieurs Cores à la Central Management Console pour les gérer ou pour générer des rapports à partir d'une interface unique.

Suivez les étapes de la procédure ci-dessous pour ajouter un Core à la Central Management Console.

- 1 À partir de la Rapid Recovery Central Management Console, cliquez sur la liste déroulante de sélection du mode, puis sélectionnez **Gérer**.
La page est actualisée, et elle contient les icônes Ajouter un Core, Ajouter un groupe et Supprimer.
- 2 Dans la partie supérieure du menu de navigation de gauche, cliquez sur **Ajouter un Core**.
La page **Ajouter un Core** s'affiche.
- 3 Saisissez les informations demandées pour vous connecter au Core, comme indiqué dans le tableau suivant.

Tableau 167. Détails de la page Ajouter un Core

Zone de texte	Description
Groupe parent	Facultativement, si vous souhaitez que le Core soit ajouté à un groupe de Cores existant, sélectionnez le nom parent dans l'organisation appropriée.
Nom d'affichage	Entrez un nom d'affichage pour le Core. Le nom d'affichage ne doit pas comprendre plus de 150 caractères. Il est préférable que ce nom ne fasse pas plus de 33 caractères. N'utilisez pas de caractères interdits ni d'expressions interdites. Pour en savoir plus sur les expressions ou caractères interdits, voir le <i>Dell Data Protection Rapid Recovery User Guide</i> (Guide d'utilisation de Dell Data Protection Rapid Recovery).
Nom d'hôte	Entrez l'adresse IP d'accès au Core. Si le Core que vous ajoutez est le serveur actuel, vous pouvez utiliser localhost.
Port	Entrez un numéro de port pour la connexion. La valeur par défaut est 8006.
Nom d'utilisateur	Entrez le nom d'utilisateur servant à accéder au service de Core pour le Core nouvellement ajouté.
Mot de passe	Entrez le mot de passe servant à accéder au service de Core pour le Core nouvellement ajouté.

- 4 Cliquez sur **Tester la connexion** pour tester la configuration.
Si le test réussit, un message s'affiche pour le confirmer. Cliquez sur **OK** pour fermer le message de confirmation.
- 5 Cliquez sur **Enregistrer**.
Vos modifications sont enregistrées, et le Core a été ajouté au groupe parent.

Liens connexes

[Ajout d'un groupe de Cores à la Central Management Console](#)

Configuration des paramètres du Core dans la Central Management Console

Suivez les étapes de la procédure ci-après pour configurer les paramètres du Core dans la Central Management Console.

- 1 Dans la Rapid Recovery Central Management Console, cliquez sur le menu déroulant de sélection du mode, puis sélectionnez **Gérer**.
La page s'actualise et affiche les icônes Ajouter un Core, Ajouter un groupe et Supprimer.
- 2 Dans le menu de navigation de gauche, cliquez sur le nom du Core approprié.
La page **Paramètres** du Core sélectionné s'affiche.
- 3 Dans l'onglet Paramètres, modifiez les informations du Core comme indiqué dans le tableau suivant.

Tableau 168. Paramètres du Core

Zone de texte	Description
Groupe parent	Sélectionnez le groupe de Cores parent pour les paramètres du nouveau Core à ajouter.
Nom d'affichage	Entrez le nom d'affichage du Core.
Nom d'utilisateur	Saisissez le nom d'utilisateur du Core.
Mot de passe	Entrez le mot de passe du Core.
Comment le portail de gestion	Sélectionnez une option spécifiant le type de connexion. Options disponibles : • Utiliser la dernière adresse IP connue de [nom du Core] (xxx.xxx.xxx.xxx) ou • Utiliser le nom d'hôte ou l'adresse IP [nom d'hôte ou adresse IP].

Zone de texte	Description
doit-il se connecter à [nom du Core] ?	Si vous choisissez de demander la connexion via un nom d'hôte ou une adresse IP, il vous faut saisir les informations appropriées dans le champ du nom d'hôte ou de l'adresse IP.
Sur quel port [nom du Core] écoute-t-il ?	Sélectionnez l'une des options de port. Choisissez une des options suivantes : - Port par défaut (8006) ou - Port personnalisé [port] Si vous choisissez de spécifier un port, saisissez son numéro dans le champ Port personnalisé.

- 4 Cliquez sur **Test de connexion**.
Si le test réussit, un message vous indique que la connexion a réussi.
- 5 Cliquez sur **Enregistrer**.

Ajout d'un groupe de Cores à la Central Management Console

Suivez les étapes de la procédure ci-après pour ajouter un groupe de Cores à la Rapid Recovery Central Management Console.

- 1 Dans la Rapid Recovery Central Management Console, cliquez sur le menu déroulant de sélection du mode, puis sélectionnez **Gérer**. La page s'actualise et affiche les icônes Ajouter un Core, Ajouter un groupe de Cores et Supprimer.
- 2 Dans la partie supérieure du menu de navigation gauche, cliquez sur **Ajouter un groupe**. La page **Ajouter un groupe** s'affiche.
- 3 Sélectionnez le groupe parent et le nom d'affichage comme indiqué dans le tableau suivant.

Tableau 169. Ajout d'un groupe de Cores

Zone de texte	Description
Groupe parent	Sélectionnez le groupe parent des Cores pour le nouveau groupe de Cores à ajouter.
Nom d'affichage	Saisissez le nom d'affichage du groupe de Cores. Le nom d'affichage ne doit pas dépasser 150 caractères. Il est préférable que ce nom ne fasse pas plus de 33 caractères. N'utilisez pas de caractères interdits ni d'expressions interdites. Pour en savoir plus sur les expressions ou caractères interdits, voir le <i>Dell Data Protection Rapid Recovery User Guide</i> (Guide d'utilisation de Dell Data Protection Rapid Recovery).

- 4 Cliquez sur **Enregistrer**.

Liens connexes

[Ajout d'un groupe de Cores à la Central Management Console](#)

Configuration des paramètres du groupe de Cores

Pour pouvoir configurer les paramètres ou l'accès du groupe de Cores, vous devez d'abord créer le groupe. Pour plus d'informations, voir [Ajout d'un groupe de Cores à la Central Management Console](#).

Appliquez les étapes de la procédure suivante pour configurer les paramètres du groupe de Cores.

- 1 À partir de la Rapid Recovery Central Management Console, cliquez sur la liste déroulante de sélection du mode, puis sélectionnez **Gérer**. La page s'actualise et affiche les icônes Ajouter un Core, Ajouter un groupe de Cores et Supprimer.
- 2 Dans le menu de navigation à gauche, cliquez sur le nom du groupe de Cores que vous souhaitez configurer.

La page Paramètres s'affiche pour le groupe de Cores sélectionné.

- 3 Modifiez les informations du groupe de Cores, tel que décrit dans le tableau suivant.

Tableau 170. Paramètres du groupe de Cores

Zone de texte	Description
Groupe parent	Sélectionnez le groupe parent des Cores pour les paramètres du nouveau groupe de Cores à ajouter.
Nom d'affichage	Entrez un nom d'affichage pour le groupe de Cores. Le nom d'affichage doit être limité à 150 caractères au maximum. Il est préférable que ce nom ne fasse pas plus de 33 caractères. N'utilisez pas de caractères interdits ni d'expressions interdites. Pour plus d'informations sur les expressions ou caractères interdits, voir le guide d'utilisation de Dell Data Protection Rapid Recovery.

- 4 Cliquez sur **Enregistrer**.

Configuration de l'accès au groupe de Cores

Pour pouvoir configurer les paramètres ou l'accès du groupe de Cores, vous devez d'abord créer le groupe. Pour plus d'informations, voir [Ajout d'un groupe de Cores à la Central Management Console](#).

Pour pouvoir ajouter ou afficher des Cores dans la Central Management Console, le compte utilisateur actuel doit être membre du groupe d'administrateurs de domaine Active Directory. Sinon, vous pouvez fournir l'accès à des utilisateurs ou groupes individuels à l'aide de cette procédure.

Appliquez les étapes de la procédure suivante pour configurer l'accès au groupe de Cores.

- 1 À partir de la Rapid Recovery Central Management Console, cliquez sur la liste déroulante de sélection du mode, puis sélectionnez **Gérer**.
La page est actualisée, et elle contient les icônes Ajouter un Core, Ajouter un groupe et Supprimer.
- 2 Dans le menu de navigation à gauche, cliquez sur le nom du groupe de Cores que vous souhaitez configurer.
La page **Paramètres** du Core sélectionné s'affiche.
- 3 Cliquez sur l'onglet **Accès**.
Les paramètres Accès du groupe de Cores s'affichent.
- 4 Cliquez sur **Ajouter**.
La boîte de dialogue **Autoriser l'accès** s'affiche. Vous pouvez fournir l'accès à une personne ou à un groupe.
- 5 Effectuez l'une des opérations suivantes :
 - Si vous souhaitez fournir l'accès à une personne, saisissez son nom dans le champ de texte **Nom**, puis cliquez sur **Utilisateur**. Il s'agit de l'option par défaut.
Par exemple, saisissez Administrateur (ou, si la machine est dans un domaine, [nom de domaine] \Administrator).
 - Si vous voulez fournir l'accès à un groupe, dans le champ de texte **Nom**, saisissez le nom du groupe, puis cliquez sur **Groupe**.
Par exemple, saisissez AdminGroup (ou, si la machine est dans un domaine, [nom de domaine] \AdminGroup).
- 6 Cliquez sur **Vérifier le nom** pour vérifier que le nom d'utilisateur ou le nom du groupe que vous avez spécifié est accessible.
Si le nom saisi est valide, un message Compte vérifié s'affiche.
- 7 Une fois que vous avez saisi et validé un nom, cliquez sur **Enregistrer**.
La boîte de dialogue **Autoriser l'accès** se ferme et les modifications sont enregistrées. Le nom d'accès s'affiche dans l'onglet Accès pour le groupe de Cores.

Comprendre les rapports de noyau de la Console de gestion centrale

La Rapid Recovery vous permet de générer et d'afficher des rapports d'opérations, des rapports d'échec, ainsi que des informations récapitulatives pour de nombreux Noyaux de la Rapid Recovery. Les informations détaillées concernant les Noyaux sont présentées dans des tableaux récapitulatifs proposant les mêmes catégories que celles décrites dans les sections [Comprendre le rapport de tâche](#), [Comprendre le rapport des échecs](#) et [Comprendre le rapport récapitulatif](#).

Pour savoir comment générer un rapport concernant plusieurs noyaux, veuillez consulter [Générer un rapport à partir de Central Management Console](#).

Générer un rapport à partir de Central Management Console

Suivez cette procédure pour générer un rapport sur plusieurs Cores Rapid Recovery à partir de la Central Management Console.

- 1 À partir de la Rapid Recovery Central Management Console, cliquez sur le menu déroulant de sélection du mode situé dans le coin supérieur droit, puis sélectionnez **Reports (Rapports)**.
La page report selection (Sélection de rapport) s'affiche. Le CoreJobReport est sélectionné par défaut. À droite du nom du rapport, une flèche vers le bas s'affiche, à partir de laquelle vous pouvez sélectionner un autre type de rapport.
- 2 Dans le menu de navigation de gauche, sélectionnez une combinaison de Cores ou de groupes de Cores Rapid Recovery que vous souhaitez inclure dans le rapport.
- 3 À partir du menu déroulant report type (Type de rapport), sélectionnez le type de rapport que vous souhaitez générer. Vous pouvez choisir une des options suivantes :
 - Rapport de tâche
 - Rapport d'échec
 - Rapport récapitulatif
 - Rapport récapitulatif des tâches

Pour en savoir plus sur ces types de rapports, voir [À propos des rapports Rapid Recovery](#).

- 4 À partir du menu déroulant date range (Plage de dates), sélectionnez une plage de dates.
Vous pouvez choisir parmi les options disponibles dans le tableau suivant.

Option	Description
Jour	Relève l'activité du dernier jour, par rapport à l'heure de génération du rapport.
Semaine	Relève l'activité de la dernière semaine, par rapport à l'heure de génération du rapport.
Mois	Relève l'activité des 31 derniers jours, par rapport à l'heure de génération du rapport.
Année	Relève l'activité de l'année précédente, par rapport à l'heure de génération du rapport.
Toute la durée	Cette période s'étend sur la totalité de la durée de vie du Core.
Personnalisée	Cette période nécessite que vous spécifiez les dates de début et de fin.

REMARQUE : Dans tous les cas, aucune donnée de rapport n'est disponible avant le déploiement du logiciel du Core ou avant la protection des machines sur le Core.

- 5 Effectuez l'une des opérations suivantes :
 - Cliquez sur **Preview (Prévisualisation)** pour générer et afficher le rapport généré en ligne.
 - Mettez à jour dynamiquement le rapport en modifiant les critères du rapport ; cliquez à nouveau sur **Preview (Prévisualisation)**.
 - Choisissez un format d'exportation (cela inclut le format par défaut, XLSX) puis cliquez sur **Download (Télécharger)**.
 - Utilisez la **Reports toolbar (barre d'outils Rapports)** pour afficher, manipuler ou imprimer le rapport. Pour en savoir plus sur la barre d'outils Rapports, voir [Utilisation de la barre d'outils Rapports](#).

Comprendre l'utilitaire Command Line Management Rapid Recovery

Dell Data Protection | Rapid Recovery se compose de plusieurs composants logiciels. Les composants clés correspondant à cette rubrique comprennent les éléments suivants :

- Le Core Rapid Recovery gère l'authentification des machines protégées, les planifications de transfert des données pour la sauvegarde et la réplication, l'export vers des machines virtuelles, la création de rapports et la restauration BMR vers des machines identiques ou différentes.
- L'Agent Rapid Recovery est chargé des instantanés de volume et du transfert rapide des données vers la logithèque gérée par le Core.
- L'utilitaire Command Line Management Rapid Recovery, cmdutil.exe, fournit un accès tiers pour gérer les fonctionnalités du système. Cet outil permet d'exécuter des scripts liés aux fonctions de gestion du Core Rapid Recovery.

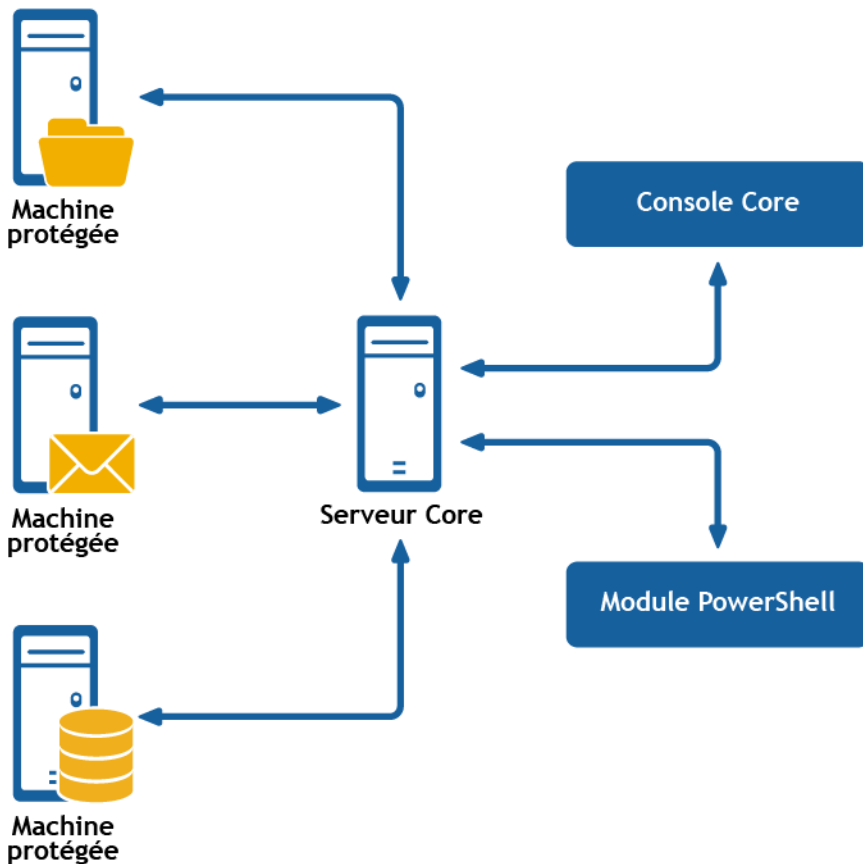


Figure 13. L'utilitaire Command Line Management Rapid Recovery fournit des fonctions de ligne de commande

Command Line Management Rapid Recovery est un utilitaire de ligne de commande sous Windows permettant aux utilisateurs d'interagir avec le serveur Core Rapid Recovery . Il offre certaines des fonctions que l'interface utilisateur graphique de la console Core Rapid Recovery fournit. Par exemple, l'utilitaire Command Line Management Rapid Recovery peut monter les points de restauration ou forcer un instantané.

L'utilitaire Command Line Management Rapid Recovery est intégré à chaque installation du Core Rapid Recovery. Pour ouvrir l'utilitaire Command Line Management en vue d'effectuer une installation par défaut, naviguez vers l'emplacement **C:\Program Files\AppRecovery\care\core\CoreService**, puis double-cliquez sur le fichier `cmdutil.exe`

En mode Ligne de commande, des signalements d'action peuvent être transmis à l'utilitaire Command Line Management Rapid Recovery via une sélection d'options de commandes et de qualificatifs pour réaliser des fonctions limitées de gestion.

Sujets :

- [Commandes](#)
- [Localisation](#)

Commandes

Cette section décrit les commandes et les options disponibles pour l'utilitaire Command Line Management de Rapid Recovery. Les commandes suivantes sont disponibles :

- [Archivage](#)
- [CancelActiveJobs](#)
- [CheckRepository](#)
- [CreateArchiveRepository](#)
- [CreateBootCD](#)
- [CreateRepository](#)
- [DeleteRepository](#)
- [Dismount](#)
- [DismountArchiveRepository](#)
- [EditEsxServer](#)
- [Forcer](#)
- [ForceAttach](#)
- [ForceChecksum](#)
- [ForceLogTruncation](#)
- [ForceMount](#)
- [ForceReplication](#)
- [ForceRollup](#)
- [ForceVirtualStandby](#)
- [Aide](#)
- [List](#)
- [Montage](#)
- [MountArchiveRepository](#)
- [NewCloudAccount](#)
- [OpenDvmRepository](#)
- [Suspendre](#)
- [Protect](#)
- [ProtectCluster](#)
- [ProtectEsxServer](#)
- [RemoveAgent](#)
- [RemoveArchiveRepository](#)
- [RemovePoints](#)

- [RemoveScheduledArchive](#)
- [RemoveVirtualStandby](#)
- [Replicate](#)
- [Réplication](#)
- [RestoreAgent](#)
- [RestoreArchive](#)
- [RestoreUrc](#)
- [Reprendre](#)
- [SeedDrive](#)
- [StartExport](#)
- [UpdateRepository](#)
- [Version](#)
- [VirtualStandby](#)

Archivage

Les entreprises utilisent souvent un stockage à long terme pour l'archivage des données conformes et non conformes. La fonction d'archivage de Rapid Recovery prend en charge la rétention prolongée de données conformes et non conformes. L'administrateur peut enregistrer une archive sur le stockage local ou à un emplacement réseau en spécifiant le paramètre `-path` et les informations d'identification.

Utilisation

L'utilisation de la commande est la suivante :

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername [name] -archivepassword [password] -comment [text]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `archive` :

Tableau 171. Options de la commande Archive

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
<code>-all</code>	Archiver tous les points de restauration pour toutes les machines protégées sur le Core.

Option	Description
-protectedserver	Machine protégée avec des points de restauration à archiver. Vous pouvez spécifier plusieurs noms de machine entourés de guillemets doubles (") et séparés par des espaces.
-path	Le chemin où les données archivées doivent être placées ; par exemple : d:\work\archive or network path \servername\sharename.
-startdate	La date de début de sélection des points de restauration par date de création. La valeur doit être saisie entre guillemets doubles ; par exemple : "04/30/2012 02:55 PM".
-enddate	Facultatif. La date de fin de sélection des points de restauration par date de création. La valeur doit être saisie entre guillemets doubles ; par exemple : "05/31/2012 11:00 AM". L'heure actuelle du système est utilisée par défaut.
-archiveusername	Facultatif. Nom d'utilisateur pour la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-archivepassword	Facultatif. Mot de passe de connexion à la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-comment	Facultatif. Le texte du commentaire doit être saisi entre guillemets doubles ; par exemple : -comment "comment goes here...".

Exemples :

Archiver tous les points de restauration avec des dates de création commençant à partir du 30/04/2012 14:55 pour toutes les machines du Core :

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE0#$$sdd -path d:\work\archive -startdate "04/30/2012 02:55 PM" -all
```

Archiver tous les points de restauration correspondant à une plage de dates pour deux machines protégées :

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE0#$$sdd -protectedserver "10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate "05/31/2012 11:00 AM"
```

CancelActiveJobs

Utilisez la commande `cancelactivejobs` pour annuler l'exécution de toutes les tâches en cours d'un type spécifique, comme un transfert ou une réplication.

Utilisation

L'utilisation de la commande est la suivante :

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type filter]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `cancelactivejobs` :

Tableau 172. Options de la commande CancelActiveJobs

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Détermine la machine protégée sur laquelle les tâches doivent être annulées.
-all	Sélectionne et annule des événements d'un type spécifié pour tous les serveurs protégés.
-jobtype	Facultatif. Indique le filtre de type de tâche. Les valeurs disponibles sont : • 'transfer' (transfert de données) • 'repository' (maintenance de la logithèque) • 'replication' (réplications locales et distantes) • 'backup' (sauvegarde et restauration) • 'bootcdbuilder' (créer des CD d'amorçage) • 'diagnostics' (charger les journaux) • 'exchange' (vérification des fichiers Exchange Server) • 'export' (exportation du point de restauration) • 'pushinstall' (déployer les agents) • 'Restaurer' (restaurer un point de restauration) • 'rollup' (consolidation des points de restauration) • 'sqlattach' (vérifications de la capacité d'attachement de l'agent) • 'mount' (monter la logithèque) Toutes les tâches du type spécifié sont annulées par défaut.

Exemple :

Annuler toutes les tâches de transfert du Core 10.10.10.10 :

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

CheckRepository

Vous pouvez utiliser la commande CheckRepository pour vérifier l'intégrité d'une logithèque DVM existante créée sous un Core AppAssure ou Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `CheckRepository` :

Tableau 173. Options de la commande `CheckRepository`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Facultatif. Cette option permet de vérifier toutes les logithèques DVM associées au Core.
-repository	Nom de la logithèque DVM.
-force	Facultatif. Cette option permet d'effectuer une vérification sans votre confirmation.

Exemple :

Pour démarrer la vérification de la logithèque DVM :

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

CreateArchiveRepository

Lorsque vous créez une logithèque d'archivage, vous créez une destination pour le contenu d'une archive planifiée. Cette fonction vous permet de monter un point de restauration archivé et de restaurer une machine sans importer l'archive.

Utilisation

L'utilisation de la commande est la suivante :

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name [archive repository name] -path [path to the archive] -archiveusername [network user name] -
```

archivepassword [network password] -cloudaccountname [name of the cloud account] -
cloudcontainer [name of the cloud container]

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `CreateArchiveRepository` :

Tableau 174. Options de la commande `CreateArchiveRepository`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-name	Requis. Le nom de la logithèque d'archivage.
-path	Le chemin d'accès à l'archive existante. Il peut s'agir d'un emplacement local, réseau ou cloud. Par exemple : d:\work\archive ou \\servername\sharename.
-archiveusername	Facultatif. Cette option est l'identifiant de connexion à la machine distante. Uniquement obligatoire pour le chemin d'accès réseau.
-archivepassword	Facultatif. Cette option est le mot de passe de la machine distante. Uniquement obligatoire pour le chemin d'accès réseau.
-cloudaccountname	Facultatif. Cette option est le nom affiché du compte Cloud existant. Uniquement obligatoire pour le chemin d'accès au cloud.
-cloudcontainer	Facultatif. Le conteneur cloud où l'archive se situe. Uniquement obligatoire pour le chemin d'accès au cloud.

Exemples :

Créez une logithèque d'archivage portant le nom « NewArchive: ».

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

De plus, si une archive contient plus d'un emplacement, la commande doit alors inclure des chemins d'accès pour tous les segments commandés auprès de 1 à N, où N est égal au nombre de segments.

Créez une logithèque d'archivage portant le nom « 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

Cette commande vous permet de créer un CD d'amorçage de restauration BMR sans utiliser la console Core Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `CreateBootCD` :

Tableau 175. Options de la commande CreateBootCD

Option	Description
-?	Affiche de l'aide sur la commande.
-ip	Facultatif. Cette option spécifie l'adresse IP de la machine BMR cible. Elle est générée automatiquement par défaut.
-mask	Facultatif. Cette option spécifie le masque de sous-réseau de la machine BMR cible. Elle est générée automatiquement par défaut.
-defaultgateway	Facultatif. Cette option spécifie la passerelle par défaut de la machine BMR cible. Elle est générée automatiquement par défaut.
-dnsserver	Facultatif. Cette option spécifie le serveur DNS de la machine BMR cible. Elle est générée automatiquement par défaut.
-vncpassword	Facultatif. Cette option spécifie le mot de passe de l'utilisateur pour un compte UltraVNC existant. Cette option est vide par défaut.
-vncport	Facultatif. Cette option spécifie le port à utiliser pour UltraVNC. Vous pouvez uniquement le modifier si vous avez utilisé l'option <code>-vncpassword</code> . Le port par défaut est 5900.
-isofilepath	Facultatif. Cette option spécifie le correctif au fichier du CD d'amorçage. Le chemin d'accès par défaut est C:\ProgramData\AppRecovery\Boot CDs.

Exemple :

Créez un CD d'amorçage :

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


CreateRepository

Utilisez la commande `createrepository` pour créer une nouvelle logithèque DVM sur une machine locale ou sur un emplacement de partage CIFS.

Utilisation

L'utilisation de la commande lors de la création d'une logithèque sur un emplacement local se fait de la sorte :

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

L'utilisation de la commande lors de la création d'une logithèque DVM sur un emplacement partagé se fait de la sorte :

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `createrepository` :

Tableau 176. Options de la commande CreateRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-name	Nom de la logithèque.
-size	La taille de l'emplacement de stockage de la logithèque. Les unités disponibles sont o, Ko, Mo, Go, To et Po.
-datapath	Pour l'emplacement local uniquement. Détermine le chemin des données de l'emplacement de stockage de la logithèque.
-metadatapath	Pour l'emplacement local uniquement. Détermine le chemin des métadonnées de l'emplacement de stockage de la logithèque.
-uncpath	Pour l'emplacement partagé uniquement. Détermine les chemins des données et des métadonnées de l'emplacement de stockage de la logithèque.
-shareusername	Pour l'emplacement partagé uniquement. Détermine le nom d'utilisateur pour l'emplacement partagé.

Option	Description
-sharepassword	Pour l'emplacement partagé uniquement. Détermine le mot de passe de connexion à l'emplacement partagé.
-comment	Facultatif. Description de la logithèque.
-concurrentoperations	Facultatif. Le nombre maximal d'opérations qui peuvent être en attente à un moment donné. Valeur par défaut : 64.

Exemples :

Créez une logithèque DVM sur un emplacement local :

```
>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
```

Créez une logithèque DVM sur un emplacement de partage :

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

DeleteRepository

Vous pouvez utiliser la commande DeleteRepository pour supprimer une logithèque DVM entière créée sous un Core AppAssure ou Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeDeleteRepository :

Tableau 177. Options de la commande DeleteRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.

Option	Description
-a	Facultatif. Cette option permet de supprimer toutes les logithèques DVM associées au Core.
-name	Le nom de la logithèque DVM que vous souhaitez supprimer.

Exemple :

Supprimez toutes les logithèques DVM :

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

Supprimez la logithèque portant le nom « RepositoryName » :

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

Dismount

Utilisez la command `dismount` pour démonter un point de restauration monté et défini par l'option `-path`, pour démonter des points de l'agent sélectionné avec le paramètre `-protectedserver`, ou démonter tous les points de restauration montés avec `-all`

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la command `dismount` :

Tableau 178. Options de la commande Dismount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Démonte tous les points de restauration montés.
-protectedserver	Démonter tous les points de restauration pour l'agent utilisé.

Option	Description
-path	Démonter le point de montage sélectionné.

Exemple :

Démonter un point de restauration qui a été monté sur le dossier c:\mountedrecoverypoint :

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

DismountArchiveRepository

Après avoir récupéré les informations souhaitées depuis une archive, vous devez démonter l'archive pour prévenir tout problème éventuel.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeDismountArchiveRepository :

Tableau 179. Options de la commande DismountArchiveRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-name	Requis. Le nom de la logithèque d'archivage.

Exemples :

Démontez la logithèque nommée « NewArchive: »

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

EditEsxServer

Vous pouvez utiliser la commande `editEsxServer` chaque fois que vous souhaitez effectuer des modifications sur le nombre de machines virtuelles ESX(i) VMware que vous souhaitez protéger sans agent.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `editEsxServer` :

Tableau 180. Options de la commande EditEsxServer

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-repository	Requis. Le nom de la logithèque associée au Core que vous souhaitez utiliser pour protéger la machine virtuelle. ❗ REMARQUE : vous devez mettre le nom entre guillemets doubles.
-protectedserver	Utilisez cette option pour modifier les objets vCenter et ESX(i) d'une machine protégée spécifique.
-add	Utilisez cette option pour ajouter un objet ESXi ou vCenter spécifié.
-remove	Utilisez cette option pour supprimer un objet ESXi ou vCenter spécifié.
-virtualmachines	Facultatif. Cette option vous permet de répertorier les machines virtuelles à protéger.
-autoprotect	Facultatif. Cette option vous permet de répertorier les nouvelles machines virtuelles à protéger automatiquement.

Exemples :

Protégez automatiquement les objets ESXi ou vCenter spécifiques d'un serveur vCenter ou ESXi avec le Core :

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

Forcer

La commande `force` force un instantané pour un serveur protégé spécifié. Forcer un instantané permet de forcer un transfert de données pour la machine protégée actuelle. Lorsque vous forcez un instantané, le transfert démarre immédiatement ou sera ajouté à la file d'attente. Seules les données qui ont changé depuis un point de restauration précédent seront transférées. S'il n'existe aucun point de restauration précédent, toutes les données des volumes protégés seront transférées.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `force` :

Tableau 181. Options de la commande Force

Option	Description
-?	Affiche de l'aide sur la commande.
-force	Facultatif. Type d'instantané à créer. Valeurs disponibles : « snapshot » (instantané incrémentiel) et « base » (instantané de l'image de base). Par défaut, c'est un instantané incrémentiel qui est effectué.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Forcer les instantanés pour toutes les machines sur le Core.
-protectedserver	Forcer un instantané pour une machine protégée spécifique.

Exemple :

Forcer un instantané pour toutes les machines présentes sur le Core :

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

ForceAttach

La commande `forceattach` vous permet de forcer une vérification de la capacité d'attachement des fichiers de la base de données SQL. Lorsque vous forcez une vérification de la capacité d'attachement, la vérification commence immédiatement.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forceattach` :

Tableau 182. Options de la commande ForceAttach

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	La machine protégée à utiliser pour effectuer la vérification de la capacité d'attachement.
-rpn	Le numéro d'un point de restauration à utiliser pour effectuer des vérifications (exécuter la commande <code>/list rps</code> pour obtenir les numéros). Pour effectuer des vérifications en utilisant plusieurs points de restauration à l'aide d'une seule commande, vous pouvez spécifier plusieurs numéros séparés par des espaces.
-time	Sélectionnez un point de restauration en fonction de son moment de création. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC.

Exemple :

Effectuer des vérifications de capacité d'attachement pour les points de restauration portant les numéros 5 et 7 :

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

ForceChecksum

La commande `forcechecksum` vous permet de forcer une vérification de l'intégrité des bases de données de messages Exchange éventuellement présentes au point ou aux points de restauration spécifiés. Lorsque vous forcez une vérification de la somme de contrôle, la commande commence immédiatement.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forcechecksum` :

Tableau 183. Options de la commande ForceChecksum

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	La machine protégée à utiliser pour effectuer la vérification de la somme de contrôle.
-rpn	Le numéro d'un point de restauration à utiliser pour effectuer des vérifications (exécuter la commande <code>/list rps</code> pour obtenir les numéros). Pour effectuer des vérifications en utilisant plusieurs points de restauration à l'aide d'une seule commande, vous pouvez spécifier plusieurs numéros séparés par des espaces.
-time	Sélectionnez un point de restauration en fonction de son moment de création. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC.

Exemple :

Effectuer une vérification de la somme de contrôle pour les points de restauration portant les numéros 5 et 7 :

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

ForceLogTruncation

Forcer la troncature de journal vous permet d'effectuer cette tâche à la demande. Cela va tronquer les journaux immédiatement pour l'agent du serveur SQL spécifié.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forcelogtruncation` :

Tableau 184. Options de la commande LogTruncation

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
- protectedserver	La machine protégée pour laquelle forcer la consolidation des points de restauration.

Exemple :

Forcer la troncature de journal pour un serveur protégé :

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

ForceMount

Utilisez la commande `forcemount` pour effectuer une vérification ponctuelle de la montabilité du point de restauration. Cela va déterminer si le ou les points de restauration spécifiés peuvent ou non être montés et utilisés pour restaurer les données sauvegardées. Vous devez énoncer un ou plusieurs points de restauration spécifiques pour lesquels effectuer la vérification, ou une plage de dates pendant laquelle les points de restauration ont été créés.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forcemount` :

Tableau 185. Options de la commande ForceMount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	La machine protégée à utiliser pour effectuer la vérification de la montabilité.
-rpn	Le numéro d'un point de restauration à utiliser pour effectuer des vérifications (exécuter la commande <code>/list rps</code> pour obtenir les numéros). Pour effectuer des vérifications en utilisant plusieurs points de restauration à l'aide d'une seule commande, vous pouvez spécifier plusieurs numéros séparés par des espaces.
-time	Sélectionnez un point de restauration en fonction de son moment de création. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC.

Exemple :

Effectuer des vérification de la montabilité pour les points de restauration portant les numéros 5 et 7 :

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

ForceReplication

Utilisez la commande `forcereplication` pour forcer un transfert ponctuel des données répliquées du Core source vers le Core cible. Vous pouvez répliquer un serveur protégé spécifique ou répliquer tous les serveurs protégés. Les serveurs protégés doivent être déjà configurés pour la réplication.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forcereplication` :

Tableau 186. Options de la commande ForceReplication

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-targetcore	Nom d'hôte du Core cible à utiliser pour forcer la réplication.
-protectedserver	La machine protégée que vous souhaitez répliquer.
-all	Forcer la réplication pour toutes les machines en cours de réplication sur le Core cible.

Exemple :

Forcer la réplication pour un serveur protégé sur un Core cible spécifique :

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

ForceRollup

Utilisez la commande `forcerollup` pour forcer la consolidation des points de restauration d'une machine protégée.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `forcerollup` :

Tableau 187. Options de la commande ForceRollup

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Facultatif. Machine protégée à utiliser pour effectuer la consolidation).

Exemple :

Forcer la consolidation pur l'agent 10.10.10.1 du Core :

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

ForceVirtualStandby

L'exportation de données d'une machine protégée vers une machine virtuelle crée une machine de secours virtuelle. Si vous avez configuré l'exportation virtuelle continue, vous pouvez utiliser cette commande pour forcer Rapid Recovery à exporter des données à la demande, quelle que soit la programmation prédéterminée.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `ForceVirtualStandby` :

Tableau 188. Options de la commande `ForceVirtualStandby`

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
<code>-protectedserver</code>	Nom de machine virtualisée ou noms de machine virtualisée séparés par un espace.
<code>-all</code>	Cette commande indique si toutes les exportations virtuelles planifiées doivent être forcées.

Exemples :

Forcer toutes les exportations de secours virtuelles :

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

Forcer l'exportation de secours virtuelle pour deux machines :

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

Aide

La commande `help` affiche une liste des commandes disponibles et de leur définition. Elle fournit également des renseignements sur la version et les droits d'auteur.

Utilisation

L'utilisation de la commande est la suivante :

```
/help
```

Exemple :

Demander de l'aide sur les lignes de commande :

```
>cmdutil /help
```

List

La commande `list` renvoie des informations sur la totalité des points de restauration, tâches actives, tâches terminées, tâches échouées, points de restauration non valides (échoués) et valides (réussis), montages, serveurs protégés, volumes, serveurs virtualisés, volumes non protégés, clusters, groupes de protection, bases de données SQL, bases de données Exchange, serveurs répliqués et logithèques de l'agent spécifié ou affiche la liste des serveurs actuellement protégés par le Core. Les enregistrements les plus récents sont renvoyés par défaut. Vous pouvez afficher la liste de tous les enregistrements ou spécifier combien d'enregistrements afficher en utilisant un paramètre nombre. Ce paramètre devra contenir la lettre "l" pour le dernier point de restauration et "r" pour le premier point de restauration. Chaque point de restauration a son nombre propre que l'administrateur peut utiliser pour le montage.

Utilisation

L'utilisation de la commande est la suivante :

```
/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
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `list` :

Tableau 189. Options de la commande List

Option	Description
-?	Affiche de l'aide sur la commande.
-list	Sélectionnez l'une des options suivantes : • tous les points de restauration ('rps') • les points de restauration valides ('passed') • les points de restauration non valides ('failed') • les montages ('mounts') • les volumes protégés ('volumes') • les volumes non protégés ('unprotectedvolumes') • les machines protégées ('protectedservers') • les tâches actives ('activejobs') • les tâches échouées ('failedjobs') • les tâches terminées ('completedjobs') • les serveurs virtualisés ('virtualizedservers') • les clusters ('clusters') • Les groupes de protection ('protectiongroups') • Les bases de données SQL Server ('sqldatabases') • Les bases de données MS Exchange ('exchangemailstores') • les serveurs répliqués ('replicatedservers') • les logithèques ('repositories')

Option	Description
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Pour afficher les tâches uniquement. Affiche tous les événements d'un type spécifique (actif/échoué/terminé) sur le serveur Core.
-protectedserver	Machine protégée avec des points de restauration à afficher.
-number	Facultatif. Nombre de données à afficher. Utilisez uniquement les spécificateurs suivants : 'rps', 'activejobs' (tâches actives), 'completedjobs' (tâches terminées), 'failedjobs' (tâches échouées). Les valeurs disponibles sont : - all (récupérer toutes les données individuelles) - l[number] ou [number] (récupérer les ## données les plus importantes) - f[number] (récupérer les ## premières données) Prend uniquement effet lors de l'affichage des tâches et des points de restauration.
-jobtype	Facultatif. Résultats filtrés par type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données) 'repository' (maintenance de la logithèque) 'replication' (réplications locales et distantes) 'backup' (sauvegarde et restauration) 'bootcdbuilder' (créer des CD d'amorçage) 'diagnostics' (charger les journaux) 'exchange' (vérification des fichiers Exchange Server) 'export' (exportation des points de restauration) 'pushinstall' (déployer les agents) 'restore' (restaurations de points de restauration) 'rollup' (consolidations des machines protégées) 'sqlattach' (vérifications de la capacité d'attachement de l'agent SQL) 'mount' (monter la logithèque)

Exemples :

Afficher la liste des 30 points de restauration les plus récents :

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

Afficher toutes les tâches de transfert de données échouées effectuées par une machine protégée :

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

Montage

La commande `mount` monte l'instantané d'un ou plusieurs lecteurs. Vous pouvez spécifier si le montage doit être en lecture, en écriture ou en lecture seule avec écritures précédentes. Le choix par défaut est lecture seule.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `mount` :

Tableau 190. Options de la commande Mount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Machine protégée avec un ou des points de restauration à monter.
-mounttype	Facultatif. Spécifie un mode de montage. Les valeurs disponibles sont : 'read' (read-only) (en lecture seule), 'readOnlyWithPreviousWrites' (en lecture seule avec les écritures précédentes), 'write' (accessible en écriture). Le mode par défaut est read-only (en lecture seule).
-volumes	Facultatif. Liste des noms de volumes à monter. Si rien n'est spécifié, tous les volumes seront montés. Les valeurs doivent être saisies entre guillemets doubles (") et séparées par un espace, par exemple : "c:" "d:". Ne pas utiliser de slashes dans les noms des volumes.
-path	Chemin vers un dossier du serveur Core sur lequel le point de restauration doit être monté. Si aucun n'existe, un dossier est créé automatiquement.
-rpn	Facultatif. Le numéro séquentiel d'un point de restauration à monter (utiliser la commande <code>list rps</code> pour obtenir les numéros). Spécifiez plusieurs numéros séparés par des espaces pour monter plusieurs points de restauration à l'aide d'une seule commande. Dans ce cas, les données de chacun des points de restauration seront stockées dans un dossier enfant distinct. Remarque : si ni l'option <code>-time</code> , ni l'option <code>-rpn</code> n'est spécifiée, c'est alors le point de restauration ayant réussi la vérification d'intégrité le plus récemment qui sera monté.

Option	Description
-time	Facultatif. Détermine le ou les points de restauration à sélectionner pour le montage. Les valeurs disponibles incluent les suivantes : 'latest' (le plus récent), 'passed' (réussi), horodatage exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC. Si ni l'option -time, ni l'option -rpn n'est spécifiée, c'est alors le point de restauration ayant réussi une vérification d'intégrité le plus récemment qui sera monté.
-localdrive	Facultatif. Effectuer un montage sur le disque utilisateur du PC local.

Exemples :

Monter les points de restauration les plus récents contenant les volumes "c:\" et "d:\" en mode lecture seule :

```
>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:"
```

Monter les points de restauration portant les numéros 2 et 7 :

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

MountArchiveRepository

Pour restaurer les données à partir d'une archive de Rapid Recovery, vous devez d'abord la monter.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `mountarchiverepository` :

Tableau 191. Options de la commande MountArchiveRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.

Option	Description
-name	Requis. Le nom de la logithèque d'archivage.

Exemples :

Montez la logithèque nommée « NewArchive: »

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

NewCloudAccount

Utilisez la commande NewCloudAccount pour ajouter au Core Rapid Recovery un compte pour un fournisseur de services cloud. Vous pouvez ensuite utiliser ce compte pour stocker des archives à des fins de rétention ou de réplication.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeNewCloudAccount :

Tableau 192. Options de la commande NewCloudAccount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-displayname	Nom que vous souhaitez utiliser pour le compte cloud.
-type	Type de compte cloud. Les valeurs disponibles sont : • Amazon • Openstack • Rackspace • Windowsazure • « Windows Azure »

Option	Description
	• Azure
-username	Nom d'utilisateur du compte cloud que vous souhaitez ajouter. Cette valeur correspond aux informations d'identification que vous utilisez pendant le processus d'authentification. Selon le type de cloud, la propriété a les variantes suivantes : • Amazon : clé d'accès • OpenStack : nom d'utilisateur • Rackspace : nom d'utilisateur • Windows Azure : nom du compte de stockage
-key	Clé d'authentification du compte cloud que vous souhaitez ajouter. Cette valeur correspond aux informations d'identification que vous utilisez pendant le processus d'authentification. Selon le type de cloud, la propriété a les variantes suivantes : • Amazon : clé secrète • OpenStack : clé API • Rackspace : clé API • Windows Azure : clé d'accès
-region	Région du compte cloud que vous souhaitez ajouter. Cette option est requise uniquement pour les comptes OpenStack et Rackspace.
-tenantid	ID que vous utilisez pour authentifier un compte cloud OpenStack. Cette option est requise uniquement pour les comptes OpenStack.
-authurl	URL que vous utilisez pour authentifier un compte cloud OpenStack. Cette option est requise uniquement pour les comptes OpenStack.

Exemples :

Pour ajouter un nouveau compte cloud portant le nom suivant : « Amazon S3 Account » avec la clé d'accès « akey » et la clé secrète « Sclé » :

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

OpenDvmRepository

Utilisez cette commande pour ouvrir une logithèque DVM créée dans un Core AppAssure ou Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `OpenDvmRepository` :

Tableau 193. Options de la commande `OpenDvmRepository`

Option	Description
-?	Affiche de l'aide sur la commande.
-localpath	Chemin du dossier contenant une logithèque DVM sur le Core local.
-sharepath	Chemin du dossier contenant la logithèque DVM sur un partage CIFS.
-shareusername	Nom d'utilisateur utilisé pour accéder au dossier partagé.
-sharepassword	Mot de passe utilisé pour accéder au dossier partagé.

Exemple :

Ouvrir une logithèque DVM sur la machine locale :

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

Suspendre

Un administrateur peut suspendre les instantanés, exporter vers des machines virtuelles ou répliquer un Core. La commande `pause` accepte trois paramètres : `snapshot`, `vmexport` et `replication`. Un seul paramètre peut être spécifié. Un instantané peut être suspendu jusqu'à un certain temps, si le paramètre temps est spécifié.

Un utilisateur peut suspendre une réplication de trois façons :

- Sur un Core source pour toutes les machines protégées. (`- [outgoing]`).
L'administrateur doit spécifier le nom de la machine distante avec la réplication sortante appariée pour suspendre la réplication sortante sur le Core source :

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

- Sur le Core source pour une seule machine protégée. (`-protectedserver`) :

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

- Sur le Core cible (`-incoming`).

Si le Core local est un Core cible, l'administrateur peut suspendre la réplication en spécifiant le Core source et en utilisant le paramètre entrant :

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

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `pause` :

Tableau 194. Options de la commande Pause

Option	Description
-?	Affiche de l'aide sur la commande.
-pause	[snapshots], [replication] ou [vmexport].
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Facultatif. Suspension de tous les agents sur le Core sélectionné.
-protectedserver	Facultatif. Suspension du serveur protégé actuel.
-incoming	Facultatif. Nom d'hôte du Core distant qui réplique sur la machine Core.
-outgoing	Facultatif. Nom d'hôte du Core cible distant sur lequel les données sont répliquées.
-time	Facultatif. Le moment au format 'Day-Hours-Minutes' (« Jour-Heures-Minutes ») où les instantanés seront repris (seulement pour les instantanés suspendus).

Exemples :

Suspendre la création d'instantanés pour un serveur protégé spécifique :

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

Suspendre la création d'instantanés pour une machine protégée, puis la reprendre après trois jours, 20 heures et 50 minutes :

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

Suspendre l'exportation vers la machine virtuelle pour toutes les machines protégées sur le Core local :

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

Suspendre la réplication sortante sur le Core pour une machine protégée spécifique :

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

Suspendre la réplication sortante pour toutes les machines protégées sur le Core cible :

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

Suspendre la réplication entrante pour toutes les machines protégées sur le Core cible :

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

Protect

La commande `protect` permet d'ajouter un serveur sous la protection d'un Core.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `protect` :

Tableau 195. Options de la commande Protect

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-repository	Le nom d'une logithèque sur le Core où les données des machines protégées doivent être stockées. Le nom doit être entouré de guillemets doubles (").
-agentname	Nom ou adresse IP du serveur à protéger.
-agentusername	Nom d'utilisateur du cluster à protéger.
-agentpassword	Mot de passe du serveur à protéger.
-agentport	Numéro de port du serveur protégé.
-volumes	Liste des volumes à protéger. Les valeurs doivent être entre guillemets et séparées par un espace. N'utilisez pas de barre oblique finale dans les noms des volumes. Par exemple : « c: » « d: ».

Exemple :

Protéger des volumes spécifiques d'un serveur avec le 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

La commande `protectcluster` permet d'ajouter un cluster sous la protection d'un core.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `protectcluster` :

Tableau 196. Options de la commande ProtectCluster

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-repository	Le nom d'une logithèque sur le Core où les données des machines protégées doivent être stockées. Le nom doit être entouré de guillemets doubles (").
-clustername	Nom ou adresse IP du cluster à protéger.
-clusterusername	Nom d'utilisateur du cluster à protéger.
-clusterpassword	Mot de passe du cluster à protéger.
-clusterport	Numéro de port du serveur de cluster protégé.

Option	Description
-clustervolumes	Liste des volumes à protéger. Les valeurs doivent être entre guillemets et séparées par un espace. Ne pas utiliser de slash dans les noms des volumes ; par exemple : « c: » « d: ».
-clusternodes	Liste des nœuds de cluster et des volumes que vous souhaitez protéger sur chaque nœud.

Exemple :

Protéger des volumes spécifiques d'un serveur de cluster avec le Core :

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE0#$$sdd -
repository "Repository 1" -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes "C:\ClusterStorage\Volumel" -clusternodes
nodeName 10.10.8.150 volumes "c:" nodeName 10.10.8.151 volumes "c:"
```

ProtectEsxServer

Vous pouvez utiliser la commande `protectesxserver` chaque fois que vous souhaitez ajouter une machine virtuelle ESX(i) VMware à protéger.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `protectesxserver` :

Tableau 197. Options de la commande ProtectEsxServer

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-repository	Requis. Le nom de la logithèque associée au Core que vous souhaitez utiliser pour protéger la machine virtuelle.



REMARQUE : vous devez mettre le nom entre guillemets doubles.

Option	Description
-server	Le nom ou l'adresse IP du serveur vCenter ou ESXi à protéger.
-serverusername	Le nom d'utilisateur nécessaire pour se connecter au serveur vCenter ou ESXi à protéger.
-serverpassword	Le mot de passe nécessaire pour se connecter au serveur vCenter ou ESXi à protéger.
-serverport	Facultatif. Le numéro de port nécessaire pour se connecter au serveur vCenter ou ESXi à protéger.
-virtualmachines	Facultatif. Cette option vous permet de répertorier les machines virtuelles à protéger.
-autoprotect	Facultatif. Cette option vous permet de répertorier les nouvelles machines virtuelles à protéger automatiquement.

Exemples :

Protégez des machines virtuelles spécifiques à partir d'un serveur vCenter ou ESXi avec le 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"
```

RemoveAgent

La commande `RemoveAgent` vous permet de supprimer une machine protégée de la protection d'un Core, et éventuellement de supprimer les points de restauration de la machine supprimée. Si vous ne supprimez pas les points de récupération, Rapid Recovery les conserve et les classe comme une machine comportant uniquement des points de restauration.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `RemoveAgent` :

Tableau 198. Options de la commande RemoveAgent

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Nom ou adresse IP du serveur à supprimer de la protection.
-deleterecoverypoints	Facultatif. Supprime tous les points de restauration correspondant à la machine que vous voulez supprimer.

Exemple :

Supprimer la protection d'une machine et supprimer les points de restauration associés :

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

RemoveArchiveRepository

Vous pouvez utiliser la commande `removearchiverepository` pour supprimer une logithèque à partir du Core Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `removearchiverepository` :

Tableau 199. Options de la commande RemoveArchiveRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-name	Requis. Le nom de la logithèque d'archivage.

Exemples :

Supprimez la logithèque nommée « NewArchive » à partir du Core local :

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

RemovePoints

La commande `removepoints` vous permet de supprimer des points de restauration spécifiques d'une machine protégée.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `removepoints` :

Tableau 200. Options de la commande RemovePoints

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Nom ou adresse IP du serveur pour lequel vous voulez supprimer des points de restauration
-rpn	Facultatif. Le numéro d'un point de restauration à supprimer (utilisez la commande <code>/list rps</code> pour obtenir les numéros). Spécifiez plusieurs numéros séparés par des espaces pour supprimer plusieurs points de restauration à l'aide d'une seule commande.
-time	Facultatif. Détermine le ou les points de restauration à supprimer sur la base de leur date de création. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC.

Exemple :

Supprimer les points de restauration portant les numéros 5 et 7 :

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

RemoveScheduledArchive

Utilisez cette commande pour interrompre une archive continue planifiée Rapid Recovery existante.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `removescheduledarchive` :

Tableau 201. Options de la commande RemoveScheduledArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Cette option spécifie si toutes les archives planifiées qui sont associées à ce Core doivent être supprimées.
-ids	Utilisez cette option pour répertorier l'ID ou les ID de chaque archive planifiée que vous souhaitez supprimer. Pour spécifier plusieurs ID, séparez-les par des espaces.

Exemples :

Pour supprimer toutes les archives planifiées :

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

Pour supprimer une seule archive planifiée :

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

RemoveVirtualStandby

Utilisez cette commande pour interrompre l'exportation de données en continu vers une machine virtuelle dans l'utilitaire de commande Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `removevirtualstandby` :

Tableau 202. Options de la commande RemoveVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Nom de la machine virtualisée (ou noms des machines virtualisées séparés par des espaces)
-all	Cette commande spécifie si toutes les exportations virtuelles planifiées doivent être supprimées.

Exemples :

Pour supprimer toutes les exportations de disque virtuel de secours :

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

Pour supprimer l'exportation de disque virtuel de secours pour deux machines :

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

Replicate

Utilisez la commande `Replicate` pour configurer la réplication entre deux Cores Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Replicate` :

Tableau 203. Options de la commande Replicate

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-request	Facultatif. Définissez cette option si vous voulez utiliser un abonnement à un tiers fournissant des services de sauvegarde et de restauration après sinistre hors site.
-targetserver	Le nom du serveur sur lequel vous souhaitez établir la réplication. Elle comprend les paramètres suivants : • port • nom d'utilisateur • password Le paramètre de port est facultatif, sa valeur par défaut est 8006. Si vous avez utilisé l'option <code>request</code>, vous devez également utiliser le nom d'utilisateur et le mot de passe du serveur cible.
-replicationname	Facultatif. Utilisez le nom de la tâche de réplication si vous n'utilisez pas l'option <code>request</code> .
-seeddrive	Facultatif. Utilisez cette option pour spécifier un disque source pour le transfert de données initial. Le paramètre Comment est facultatif.
-protectedserver	La liste des machines protégées que vous souhaitez répliquer. Si vous utilisez l'option <code>request</code> , seuls les noms ou adresses IP des machines protégées seront répertoriés. Autrement, les deux machines protégées et les noms de logithèque correspondants seront répertoriés.

Exemple :

Répliquez deux machines protégées vers le Core distant à l'aide d'un disque source provenant d'un partage réseau :

```
>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
```

Réplication

Utilisez la commande `replication` pour contrôler la réplication existante entre deux Cores Rapid Recovery et gérer les demandes de réplication en attente.

REMARQUE : cette commande termine la commande `Replicate` qui établit la connexion (appelée couplage) entre les Cores et utilise un lecteur source pour le transfert de données initial. Pour plus d'informations sur cette commande, voir [Replicate](#).

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `replication` :

Tableau 204. Options de la commande Réplication

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-list	La liste des tâches de réplication entrantes ou sortantes, ou les demandes de réplication en attente.
-accept	Accepte la demande de réplication.
-deny	Refuse la demande de réplication.
-ignore	Ignore la demande de réplication.

Option	Description
<code>-delete</code>	Utilisez cette option pour supprimer une tâche de réplication existante ou une machine de la tâche de réplication. Indiquez uniquement le paramètre <code>-id</code> pour supprimer la totalité de la relation de réplication, ou spécifiez les paramètres <code>-id</code> et <code>-protectedserver</code> pour uniquement supprimer des machines spécifiques de la réplication.
<code>-edit</code>	Modifie la planification de toutes les tâches de réplication existantes.
<code>-id</code>	L'identificateur de la tâche de réplication ou la demande de réplication en attente. Il peut être un identifiant du Core distant, le nom de l'hôte, l'identifiant du client, l'adresse e-mail ou l'identifiant de la demande de réplication en attente.
<code>-protectedserver</code>	Pour répondre à une demande de réplication, utilisez cette option pour appliquer votre réponse à la liste des serveurs protégés avec un nom de logithèque ou un identifiant. Utilisez le paramètre « all » pour appliquer la réponse à toutes les machines demandées.
<code>-responsecomment</code>	Le commentaire que vous fournissez avec la réponse à une demande de réplication en attente.
<code>-deleterecoverypoints</code>	Utilisez cette option si des points de restauration spécifiques provenant d'une machine répliquée déjà supprimée doivent également être supprimés.
<code>-schedulesype</code>	Si vous utilisez l'option <code>-edit</code> , cette option spécifie le type de planification de réplication. Incluez l'une des quatre valeurs suivantes : <code>atalltimes</code> - réplication automatique à tout moment. <code>daily</code> - réplication quotidienne. Spécifiez les paramètres <code>-dailystarttime</code> et <code>-dailyendtime</code>. <code>custom</code> - lorsque vous utilisez la réplication quotidienne, utilisez cette valeur pour planifier la réplication durant les jours de la semaine ou les week-ends. Spécifiez les paramètres <code>-weekdaystarttime</code>, <code>-weekdayendtime</code>, <code>-weekendstarttime</code>, et <code>-weekendendtime</code>.
<code>-dailystarttime</code>	Uniquement utilisé pour la valeur quotidienne de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la première heure à laquelle vous souhaitez que la réplication ait lieu.
<code>-dailyendtime</code>	Uniquement utilisé pour la valeur quotidienne de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la dernière heure du jour à laquelle vous souhaitez que la réplication démarre.
<code>-weekdaystarttime</code>	Uniquement utilisé pour la valeur personnalisée de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la première heure d'un jour de la semaine à laquelle vous souhaitez que la réplication démarre.
<code>-weekdayendtime</code>	Uniquement utilisé pour la valeur personnalisée de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la dernière heure d'un jour de la semaine à laquelle vous souhaitez que la réplication démarre.
<code>-weekendstarttime</code>	Uniquement utilisé pour la valeur personnalisée de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la première heure du week-end à laquelle vous souhaitez que la réplication démarre.
<code>-weekendendtime</code>	Uniquement utilisé pour la valeur personnalisée de l'option <code>-schedulesype</code> . Utilisée pour établir un laps de temps à l'exécution de la réplication. Utilisez cette option pour spécifier la dernière heure du week-end à laquelle vous souhaitez que la réplication démarre.

Exemple :

Listez toutes les répliquions entrantes :

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

Acceptez les demandes de répliquion en attente pour deux machines protégées :

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

Refusez une demande de répliquion en attente :

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

Supprimez la répliquion existante avec des points de restauration répliqués :

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

Supprimez deux machines de la répliquion existante :

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

Modifiez une planification de répliquion avec heures de jour de la semaine et week-end spécifiées :

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

RestoreAgent

La commande `restoreagent` vous permet de restaurer une machine protégée ou un volume à partir d'un point de restauration Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `restoreagent` :

Tableau 205. Options de la commande RestoreAgent

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Nom ou adresse IP du serveur à restaurer.
-rpn	Numéro d'identification du point de restauration à utiliser pour restaurer la machine. Pour trouver le numéro correct, utilisez la commande <code>list rps</code> .
-volumes	Identifiants ou noms des volumes à restaurer. Pour restaurer tous les volumes protégés, utilisez <code>-volumes all</code> .
-targetmachine	Nom de la machine vers laquelle vous souhaitez restaurer la machine protégée.
-targetvolume	Nom ou identifiant du volume vers lequel vous souhaitez restaurer la machine.
-forcedismount	Facultatif. Utilisez cette option pour forcer le démontage de la base de données sur demande.
-autorestart	Facultatif. Utilisez cette commande pour redémarrer un serveur Exchange.

Exemple :

Restaurer une machine vers une machine protégée portant l'adresse IP 192.168.20.130, en forçant le démontage de la base de données :

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

RestoreArchive

Cette commande restaure une archive à partir d'une archive locale ou d'un partage, et place les données restaurées dans une logithèque spécifiée.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `restorearchive` :

Tableau 206. Options de la commande RestoreArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Restaurer les données de toutes les machines protégées à partir des fichiers archive.
-protectedserver	Machine protégée avec des points de restauration à restaurer. Vous pouvez spécifier plusieurs noms de machine entourés de guillemets doubles (") et séparés par des espaces.
-repository	Le nom d'une logithèque du Core où les points de restauration restaurés doivent être placés. Le nom doit être entouré de guillemets doubles (").
-archiveusername	Facultatif. Nom d'utilisateur pour la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-archivepassword	Facultatif. Mot de passe de connexion à la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-path	L'emplacement où les données archivées doivent être restaurées ; par exemple : d:\work\archive ou le chemin réseau \\servername\sharename.

Exemples :

Restaurer les données archivées pour tous les serveurs protégés :

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

Restaurer les données archivées pour des serveurs protégés spécifiques :

```
>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

La commande `restoreurc` vous permet de restaurer une machine protégée ou un volume à partir d'un point de restauration Rapid Recovery spécifique vers une machine BMR utilisant l'Universal Recovery Console (URC).

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `restoreurc` :

Tableau 207. Options de la commande RestoreUrc

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Le nom ou l'adresse IP du serveur pour lequel vous voulez restaurer l'URC.
-rpn	Le numéro d'identification du point de restauration que vous voulez utiliser pour restaurer la machine. Pour trouver le numéro correct, utilisez la commande <code>/list rps</code> .
-volumes	Les identifiants ou les noms des volumes à restaurer. Pour restaurer tous les volumes protégés, utilisez <code>-volumes all</code> .
-targetmachine	Le nom de la machine vers laquelle vous souhaitez restaurer la machine protégée.
-urcpassword	La clé d'authentification provenant de la console URC.
-targetdisk	Les numéros des disques vers lesquels vous souhaitez restaurer la machine. Pour sélectionner tous les disques de la machine à l'aide de la console URC, utilisez <code>-targetdisk all</code> .

Exemple :

Restaurer une machine vers les disques 0 et 1 de la machine à l'aide de la console URC lorsque l'adresse IP pour la machine URC est 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
```

Reprendre

Un administrateur peut utiliser cette commande pour reprendre les snapshots, l'exportation vers une machine virtuelle et la réplication. Vous devez spécifier votre besoin à reprendre par un paramètre. Les paramètres suivants sont valides : `snapshot`, `vmexport` et `replication`. Voir [Suspendre](#) pour plus d'informations.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `resume` :

Tableau 208. Options de la commande Resume

Option	Description
-?	Affiche de l'aide sur la commande.
-restore	[snapshots], [replication] ou [vmexport].
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-all	Reprendre tous les agents sur le Core sélectionné.
-protectedserver	Reprendre le serveur protégé actuel.
-incoming	Nom d'hôte du Core distant qui réplique sur la machine Core.
-outgoing	Nom d'hôte du Core cible distant sur lequel les données sont répliquées.

Exemples :

Reprendre les instantanés pour un serveur protégé spécifique :

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

Reprendre l'exportation vers une machine virtuelle pour toutes les machines protégées sur le Core :

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

Reprendre la réplication sortante sur le Core pour une machine protégée spécifique :

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

Reprendre la réplication sortante pour toutes les machines protégées sur le Core cible :

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

Reprendre la réplication entrante pour toutes les machines protégées sur le Core cible :

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

SeedDrive

Vous pouvez utiliser un disque source pour le transfert de données initial lorsque vous établissez la réplication Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `seeddrive` :

Tableau 209. Options de la commande SeedDrive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-list	Liste des disques sources en attente incluant des informations détaillées.
-startcopy	Début de la copie du disque source.
-startconsume	Début de la consommation du disque source.

Option	Description
-abandon	Demande d'abandon de disque source en attente.
-path	Chemin local ou réseau du disque source.
-seeddriveusername	Facultatif. Nom d'utilisateur pour l'emplacement réseau du disque source.
-seeddrivepassword	Facultatif. Mot de passe pour l'emplacement réseau du disque source.
-targetcore	Facultatif. À utiliser uniquement avec l'option-copy. Il s'agit du nom ou de l'adresse IP du Core distant. Toutes les machines protégées effectuant une réplication vers ce Core reçoivent les points de restauration du disque source.
-remotecore	À utiliser uniquement avec l'option-consume. Il s'agit du nom du Core distant à partir duquel les points de restauration du disque source sont créés ou utilisés.
-protectedserver	Nom ou adresse IP de la machine protégée que vous utilisez pour créer ou utiliser le disque source des points de restauration. Par exemple : -protectedserver "10.10.60.48" "10.10.12.101".
-all	Cette option indique si toutes les machines protégées disponibles doivent être consommées ou copiées.
-usecompatibleformat	Le nouveau format d'archivage, bien que plus performant, n'est pas compatible avec les anciens Cores. Utilisez cette option lorsque vous gérez un Core AppAssure hérité.

Exemples :

Lister les disques sources en attente :

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

Copier deux machines protégées sur le lecteur source du partage réseau :

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

Début de l'utilisation du disque source :

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

Demande d'abandon d'un disque source en attente :

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

StartExport

La commande `startexport` force une exportation ponctuelle des données d'une machine protégée vers un serveur virtuel. Vous pouvez faire une exportation vers une machine virtuelle ESXi, VMware Workstation, Hyper-V ou VirtualBox. Si vous exportez vers ESXi, vous devez spécifier si le provisionnement du disque est "thick" (complet) ou "thin" (léger).

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `startexport` :

Tableau 210. Options de la commande StartExport

Option	Description
-?	Affiche de l'aide sur la commande.
-exporttype	Effectuer l'exportation des données depuis un serveur protégé vers un serveur ESXi ('esxi'), un serveur VMware Workstation ('vm'), un serveur Hyper-V ('hyperv') ou un serveur VirtualBox ('vb').
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Machine protégée avec des points de restauration à exporter.
-volumes	Facultatif. Liste des noms de volumes à exporter. Si rien n'est spécifié, tous les volumes seront exportés. Les valeurs doivent être entre guillemets doubles (") et séparées par des espaces, par exemple : « c: » « d: ». Ne pas utiliser de slashes dans les noms des volumes.
-rpn	Facultatif. Le numéro d'un point de restauration à exporter (utiliser la commande Get-RecoveryPoints pour obtenir les numéros). Si ni l'option -time, ni l'option -rpn n'est spécifiée, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le ou les points de restauration à sélectionner pour l'exportation. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre PC. Remarque : si ni l'option -time, ni l'option -rpn n'est spécifiée, c'est alors le point de restauration le plus récent qui est exporté.
-vmname	Le nom Windows de la machine virtuelle.
-hostname	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Nom d'hôte du serveur virtuel.
-linuxhostname	Pour les exportations VirtualBox uniquement. Nom d'hôte du serveur virtuel.

Option	Description
-hostport	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Numéro de port du serveur virtuel.
-hostusername	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Le nom d'utilisateur pour l'hôte du serveur virtuel.
-hostpassword	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Mot de passe de l'hôte du serveur virtuel.
-ram	Utilisez cette option pour allouer une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Utilisez cette option pour allouer la même quantité de RAM sur le serveur virtuel contenu dans la machine source.
-diskprovisioning	Utilisez cette option pour les exportations ESXi uniquement. Facultatif. La quantité d'espace disque que vous souhaitez allouer sur la machine virtuelle. Utilisez l'une des deux spécifications suivantes : - Thick - Cette spécification rend le disque virtuel aussi volumineux que le disque d'origine sur la machine protégée. - Thin - Cette spécification alloue la quantité d'espace disque effective occupée sur le disque d'origine avec quelques méga-octets supplémentaires. La spécification par défaut est « thin ».
-diskmapping	Utilisez cette option pour les exportations ESXi uniquement. Facultatif. Cette option détermine la manière d'adresser les disques de la machine protégée vers la machine virtuelle. Utilisez l'une des valeurs suivantes : - auto - Cette valeur adresse automatiquement les disques. - manuel - Cette valeur permet d'adresser les disques manuellement. - withvm - cette valeur stocke les disques virtuels dans un magasin de données que vous sélectionnez. La valeur par défaut est « auto ».
-targetpath	Pour les exportations de VMware Workstation et de VirtualBox uniquement. Cette option spécifie le chemin local ou réseau (ou chemin Linux, pour VirtualBox uniquement) vers le dossier dans lequel vous souhaitez stocker les fichiers de la machine virtuelle
-pathusername	Pour les exportations VMware Workstation uniquement. C'est le nom d'utilisateur de la machine réseau. Seulement nécessaire lorsque vous spécifiez le chemin réseau dans l'option -targetpath.
-pathpassword	Pour les exportations VMware Workstation uniquement. C'est le mot de passe de la machine réseau. Seulement nécessaire lorsque vous spécifiez le chemin réseau dans l'option -targetpath.
-uselocalmachine	Pour les exportations Hyper-V uniquement. Facultatif. Utilisez cette commande pour vous connecter au serveur Hyper-V local. Cette option ignore les options -hostname, -hostport, -hostusername, et -hostpassword.

Exemples :

Exporter les données vers une machine virtuelle ESXi avec un nom spécifique et la même quantité de RAM et la même taille de disque que le serveur protégé source :

```
>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
```

Créer une machine virtuelle au format VMware Workstation sur le disque local avec les données protégées du point de restauration n° 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
```

Créer des machines virtuelles au format Hyper-V à stocker sur un hôte distant :

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

UpdateRepository

La commande `updaterepository` ajoute un nouvel emplacement de stockage à une logithèque DVM existante.

Utilisation

L'utilisation de la commande est la suivante :

```
/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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `updaterepository` :

Tableau 211. Options de la commande UpdateRepository

Option	Description
-?	Affiche de l'aide sur la commande.
-name	Nom de la logithèque.
-size	La taille de l'emplacement de stockage de la logithèque. Les unités disponibles sont o, Ko, Mo, Go, To et Po.
-datapath	Pour l'emplacement local uniquement. Détermine le chemin des données de l'emplacement de stockage de la logithèque.
-metadatapath	Pour l'emplacement local uniquement. Détermine le chemin des métadonnées de l'emplacement de stockage de la logithèque.
-uncpath	Pour l'emplacement partagé uniquement. Détermine les chemins des données et des métadonnées de l'emplacement de stockage de la logithèque.
-shareusername	Pour l'emplacement partagé uniquement. Détermine le nom d'utilisateur pour l'emplacement partagé.
-sharepassword	Pour l'emplacement partagé uniquement. Détermine le mot de passe de connexion à l'emplacement partagé.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.

Exemples :

Créez un nouvel emplacement de stockage dans une logithèque DVM locale :

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

Créez un emplacement de stockage pour une logithèque DVM sur un emplacement partagé :

```
>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

La commande `version` affiche les informations relatives à la version du logiciel Rapid Recovery installé sur le serveur spécifié. Si vous ne spécifiez pas de Core ou de serveur protégé, les informations renvoyées s'appliquent au Core sur lequel vous travaillez actuellement.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `version` :

Tableau 212. Options de la commande Version

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Facultatif. Machine protégée pour laquelle vous souhaitez afficher les informations de version. Si vous ne spécifiez pas de machine protégée, cela renvoie des informations relatives au Core sur lequel vous êtes en train de travailler.

Exemple :

Afficher des informations sur la version de Rapid Recovery installée sur le Core Rapid Recovery actif :

```
>cmdutil /version
```

VirtualStandby

Vous pouvez utiliser la commande `virtualstandby` pour exporter des données à partir d'une machine protégée Rapid Recovery vers une machine virtuelle compatible.

Utilisation

L'utilisation de la commande est la suivante :

```
/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
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `virtualstandby` :

Tableau 213. Options de la commande VirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-exporttype	Cette option permet d'exporter les données d'une machine protégée vers l'un des serveurs virtuels spécifiés ci-après : • esxi (ESXi) • vm (VMware Workstation) • hyperv (Hyper-V) • vb (VirtualBox)
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Le nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-password	Facultatif. Le mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun mot de passe n'est fourni, ce sont les références de l'utilisateur connecté qui sont utilisées.
-protectedserver	Utilisez cette option pour spécifier la machine protégée contenant les points de restauration à exporter.
-volumes	Facultatif. Utilisez cette option pour répertorier les noms des volumes à exporter. Si vous ne spécifiez pas les volumes, alors tous les volumes du point de restauration seront exportés. Entrez les valeurs et placez celles-ci entre guillemets puis séparez-les avec un espace ; par exemple : « c: » « d: ». N'utilisez pas de slashes dans les noms des volumes.

Option	Description
-ram	Utilisez cette option pour allouer une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Utilisez cette option pour allouer la même quantité de RAM sur le serveur virtuel contenu dans la machine source.
-vmname	Le nom Windows de la machine virtuelle.
-gen2	Facultatif. Cette option spécifie la Seconde génération du serveur de machine virtuelle. Si vous ne spécifiez pas la génération, la commande utilisera la Génération 1. Les systèmes d'exploitation suivants prennent en charge la Seconde génération : • Windows • Windows Server 2012 R2 • Windows 8.1 • Ubuntu Linux • CentOS • RHEL • Oracle Linux 7
-hostname	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Nom d'hôte du serveur virtuel.
-linuxhostname	Pour les exportations VirtualBox uniquement. Nom d'hôte du serveur virtuel.
-hostport	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Numéro de port du serveur virtuel.
-hostusername	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Le nom d'utilisateur pour l'hôte du serveur virtuel.
-hostpassword	Pour les exportations virtuelles ESXi et Hyper-V uniquement. Mot de passe de l'hôte du serveur virtuel.
-diskprovisioning	Pour les exportations ESXi uniquement. Facultatif. La quantité d'espace disque que vous souhaitez allouer sur la machine virtuelle. Utilisez l'une des deux spécifications suivantes : • Thick - Cette spécification rend le disque virtuel aussi volumineux que le disque d'origine sur la machine protégée. • Thin - Cette spécification alloue la quantité d'espace disque effective occupée sur le disque d'origine avec quelques méga-octets supplémentaires. La spécification par défaut est « thin ».
-diskmapping	Pour les exportations ESXi uniquement. Facultatif. Cette option détermine la manière d'adresser les disques de la machine protégée vers la machine virtuelle. Utilisez l'une des valeurs suivantes : • auto - Cette valeur adresse automatiquement les disques. • manuel - Cette valeur permet d'adresser les disques manuellement. • withvm - cette valeur stocke les disques virtuels dans un magasin de données que vous sélectionnez. La valeur par défaut est « auto ».
-targetpath	Pour les exportations de VMware Workstation et de VirtualBox uniquement. Cette option spécifie le chemin local ou réseau (ou chemin Linux, pour VirtualBox uniquement) vers le dossier dans lequel vous souhaitez stocker les fichiers de la machine virtuelle
-pathusername	Pour les exportations VMware Workstation uniquement. C'est le nom d'utilisateur de la machine réseau. Seulement nécessaire lorsque vous spécifiez le chemin réseau dans l'option -targetpath.
-pathpassword	Pour les exportations VMware Workstation uniquement. C'est le mot de passe de la machine réseau. Seulement nécessaire lorsque vous spécifiez le chemin réseau dans l'option -targetpath.

Option	Description
-uselocalmachine	Pour les exportations Hyper-V uniquement. Facultatif. Utilisez cette commande pour vous connecter au serveur Hyper-V local. Cette option ignore les options -hostname, -hostport, -hostusername, et -hostpassword.
-edit	Facultatif. Cette option vous permet de modifier des machines virtuelles existantes. Elle ignore les options -exporttype et -initialexport.
-initialexport	Facultatif. Cette option permet de démarrer une exportation initiale de machine virtuelle à la demande après avoir configuré un disque de secours virtuel continu.

Exemples :

Configurer une exportation du disque de secours virtuel vers une machine virtuelle ESXi avec le nom, la quantité de RAM et la taille de disque du serveur source protégé :

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

Configurer une exportation du disque de secours virtuel vers un fichier de machine VMware Workstation sur le disque local :

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

Configurer une exportation de disque de secours virtuel vers plusieurs fichiers de machine Hyper-V et les stocker sur une machine distante :

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user administrator -password
23WE@#$sd -protectedserver 10.10.5.22 -vmname Win2008-Smith -vmlocation \\WIN7-Bobby
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword
12QWsdxc@# -ram 4096
```

Localisation

Lorsqu'il est exécuté sur la même machine que celle sur laquelle le Core Rapid Recovery est installé, l'utilitaire Command Line Management utility Rapid Recovery utilise la langue d'affichage définie pour Core Rapid Recovery. Dans la présente version, les langues prises en charge sont les suivantes : allemand, anglais, chinois (simplifié), coréen, français, japonais et portugais (Brésil).

Si l'utilitaire Command Line Management utility Rapid Recovery est installé sur une machine distincte, l'anglais est alors la seule langue prise en charge.

Références de la Core Console

Cette annexe comprend des tableaux de référence qui décrivent un grand nombre de fonctions et d'icônes disponibles dans la Rapid Recovery Core Console. Il s'agit d'un complément du chapitre [Compréhension de la console Core Rapid Recovery](#) du *Dell Data Protection | Rapid Recovery User Guide* (Guide d'utilisation de Dell Data Protection | Rapid Recovery).

Sujets :

- [Affichage de l'interface utilisateur de la Core Console](#)
- [Affichage du volet Machines protégées](#)

Affichage de l'interface utilisateur de la Core Console

La Core Console est l'interface utilisateur (IU) principale par laquelle les utilisateurs interagissent avec Rapid Recovery. Lorsque vous vous connectez à la Rapid Recovery Core Console, vous voyez les éléments suivants s'afficher.

Tableau 214. Éléments de l'IU dans Core Console

Élément de l'IU	Description
Zone de la marque	Dans les environnements typiques, la partie supérieure gauche de la Core Console contient le nom du produit complet, y compris le logo Dell. Si vous cliquez sur la marque, un nouvel onglet s'ouvre dans le navigateur web, présentant une documentation du produit sur le site web du support technique.
Barre des boutons	La barre des boutons, qui s'affiche à droite de la zone de la marque, contient des boutons accessibles à partir de n'importe quel emplacement dans la Core Console. Ces boutons lancent les Assistants permettant de réaliser des tâches courantes telles que la protection d'une machine, l'exécution d'une restauration depuis le point de restauration, la création, l'ajout ou l'importation d'une archive ou la réplication à partir de ce Core source vers un Core cible. Chaque bouton de la barre des boutons est décrit plus en détails dans le tableau Tableau 215. Boutons et menus de la barre des boutons .
Nombre de tâches en cours	Indique combien de tâches sont en cours d'exécution. Cette valeur est une fonction dynamique basée sur l'état du système. Si vous cliquez sur le menu déroulant, vous affichez le résumé des états de toutes les tâches en cours d'exécution. En cliquant sur X de n'importe quelle tâche, vous pouvez choisir d'annuler cette tâche.
Menu déroulant d'aide	Le menu Aide contient les options suivantes : • Aide. Liens vers l'aide sur les produits, qui s'ouvrent dans une fenêtre de navigateur distincte. • Documentation. Lien vers la documentation technique de Rapid Recovery sur le site web du support technique de Dell. • Support. Lien vers le site web du support technique de Dell, qui permet de discuter en direct avec un technicien et propose des didacticiels vidéo, des articles de la base de connaissances de Rapid Recovery, une foire aux questions, et plus encore. • Guide de démarrage rapide. Le guide de démarrage rapide est un ensemble guidé de tâches suggérées destinées à configurer et à utiliser Rapid Recovery. Ce guide s'ouvre automatiquement chaque fois que vous vous connectez à Core Console, sauf si vous désactivez cette fonctionnalité. Vous pouvez également ouvrir le guide de démarrage rapide depuis le menu d'aide. Pour plus d'informations sur le guide de démarrage rapide, voir Comprendre le guide de démarrage rapide.

Élément de l'IU	Description
	• À propos de. Ouvre la boîte de dialogue À propos de Core Dell Data Protection Rapid Recovery, qui fournit une description et des informations sur la version du logiciel.
Date et heure du serveur	La date et l'heure de la machine en train d'exécuter le service Core de Rapid Recovery s'affichent en haut à droite de la Core Console. Lorsque vous passez votre souris sur l'heure, la date du serveur s'affiche également. Il s'agit de la date et l'heure enregistrées par le système pour les événements comme les connexions, les planifications et les rapports. Par exemple, lorsque vous appliquez des planifications de protection, l'heure affichée dans Core Console est utilisée. Cela s'applique même si le fuseau horaire est différent sur le serveur de la base de données ou sur la machine client où s'exécute le navigateur.
Barre d'icônes	La barre d'icônes comprend une représentation graphique des principales fonctions accessibles dans la Core Console. Elle s'affiche sur le côté gauche de l'interface utilisateur (IU), juste en dessous du logo de la marque. En cliquant sur l'élément approprié dans la barre d'icônes, vous accédez à la section correspondante de l'interface utilisateur, dans laquelle vous pouvez gérer cette fonction. Chacune des icônes de la barre d'icônes est décrite plus en détails dans le Tableau 216. Barre d'icônes.
Zone de navigation gauche	La zone de navigation gauche s'affiche sur le côté gauche de l'interface utilisateur, en dessous de la barre d'icônes. • La zone de navigation gauche contient le filtre de texte et le menu Machines protégées. • Si vous avez ajouté la réplication à ce Core, cette zone va également comporter un menu Machines répliquées. • Si des machines ont été supprimées de la protection, mais que des points de restauration ont été sauvegardés pour ces machines, cette zone comporte alors un menu Points de restauration uniquement. • Si vous avez ajouté des groupes personnalisés, cette zone comporte alors un menu Groupes personnalisés. • Si vous avez ajouté une archive, cette zone contient un menu Archives attachées. Vous pouvez choisir d'afficher ou non la zone de navigation gauche. Cela s'avère pratique lorsque vous avez besoin d'afficher davantage de contenu dans le menu principal de l'interface utilisateur. Pour masquer cette section, cliquez sur la bordure grise qui sépare la zone de navigation gauche du menu principal. Pour afficher à nouveau cette composante de l'interface utilisateur, cliquez une nouvelle fois sur la bordure grise. Chacun des éléments de la zone de navigation gauche sont décrits plus en détails dans le tableau Tableau 218. Zone de navigation gauche et menus.
Aide contextuelle	  Dans la Rapid Recovery Core Console, lorsque vous cliquez sur l'icône Aide (un point d'interrogation bleu), une fenêtre de navigation redimensionnable s'ouvre, comportant deux cadres. Le cadre de gauche contient une arborescence de navigation présentant les rubriques du guide d'utilisation de Rapid Recovery de Dell. Le cadre de droite contient le texte de la rubrique d'aide sélectionnée. À tout moment, l'arborescence de navigation se développe pour afficher l'emplacement de la rubrique sélectionnée dans sa hiérarchie. Vous pouvez parcourir toutes les rubriques du Guide d'utilisation en utilisant l'aide contextuelle. Fermez le navigateur lorsque vous avez fini de consulter les rubriques. Vous pouvez également ouvrir l'aide à partir de l'option Aide du menu Aide.

Barre des boutons

Les détails sur la barre des boutons s'affichent dans le tableau suivant.

Tableau 215. Boutons et menus de la barre des boutons

Élément de l'IU	Description
Barre des boutons : bouton et menu Protéger	 Le bouton Protéger lance l'Assistant Protéger une machine, depuis lequel vous pouvez protéger une machine seule dans le Core de Rapid Recovery. De plus, pour d'autres options de protection, vous pouvez accéder au menu déroulant à côté de ce bouton, qui comprend les options suivantes. • L'option Protéger une machine est une autre méthode pour lancer l'assistant Protéger une machine afin de protéger une seule machine. • L'option Protéger le cluster permet de vous connecter à un cluster de serveurs. • L'option Protéger plusieurs machines ouvre l'Assistant Protéger plusieurs machines pour protéger au moins deux machines simultanément. • L'option Déployer le logiciel agent permet d'installer le logiciel agent de Rapid Recovery sur une ou plusieurs machines simultanément. Cette fonction utilise l'Assistant Déployer le logiciel agent.
Barre des boutons : bouton et le menu Restaurer	 Le bouton Restaurer ouvre l'assistant Restaurer une machine, qui vous permet de restaurer des données à partir de points de restauration sauvegardés depuis une machine protégée. De plus, pour d'autres options de restauration ou d'exportation, vous pouvez accéder au menu déroulant à côté de ce bouton, qui comprend les options suivantes. • L'option Restaurer une machine est une autre méthode pour lancer l'Assistant Restaurer une machine permettant de restaurer des données. • L'option Monter un point de restauration lance l'Assistant de montage, qui vous permet de monter les points de restauration à partir d'une machine protégée. • L'option Exportation de VM ouvre l'Assistant d'exportation. Grâce à cet assistant, vous pouvez créer une machine virtuelle à partir des points de restauration sauvegardés dans le Core de Rapid Recovery. Vous avez l'option de créer une exportation ponctuelle, ou vous pouvez définir des paramètres pour une machine virtuelle mise à jour en continu après chaque prise d'instantané d'une machine protégée.
Barre des boutons : bouton et menu Archiver	 Le bouton Archiver ouvre l'Assistant d'archivage. Grâce à cet assistant, vous pouvez créer une archive ponctuelle à partir des points de restauration sélectionnés ou vous pouvez créer une archive et l'enregistrer en continu selon la planification que vous avez définie. De plus, pour d'autres options d'archivage, vous pouvez accéder au menu déroulant à côté de ce bouton, qui comprend les options suivantes. • L'option Créer une archive est une autre méthode pour lancer l'Assistant de création d'une archive permettant de créer une archive ponctuelle ou d'archiver en continu. • L'option Importer une archive lance l'Assistant d'importation d'archive qui vous permet d'importer une archive. • L'option Attacher l'archive monte l'archive pour que vous puissiez lire le contenu comme un système de fichiers.
Barre des boutons : bouton Réplication	 Le bouton Réplication ouvre l'Assistant de réplication. Grâce à cet assistant, vous pouvez spécifier un Core cible, sélectionner des machines protégées sur votre Core source et répliquer des points de restauration à partir de machines sélectionnées vers le Core cible dans la logithèque que vous spécifiez. Vous pouvez suspendre la réplication lors de sa définition ou commencer la réplication immédiatement. De plus, vous pouvez indiquer si un disque source sera utilisé pour copier des données pour des points de récupération existants vers le Core cible.

Barre d'icônes

Les détails sur la barre d'icônes s'affichent dans le tableau suivant.

Tableau 216. Barre d'icônes

Élément de l'IU	Description
Barre d'icônes	La barre d'icônes comprend une représentation graphique des principales fonctions accessibles dans la Core Console. En cliquant sur l'élément approprié, vous accédez à la section correspondante de l'interface utilisateur, dans laquelle vous pouvez gérer cette fonction. Les icônes de la barre d'icônes comprennent :
Barre d'icônes : icône Accueil	 Accueil. Cliquez sur l'icône Accueil pour naviguer jusqu'à la page d'accueil du Core.
Barre d'icônes : icône Réplication	 Réplication. Cliquez sur l'icône Réplication pour afficher ou gérer la réplication entrante ou sortante.
Barre d'icônes : icône Disque de secours virtuel	 Disque de secours virtuel. Cliquez sur l'icône de disque de secours virtuel pour exporter les informations d'un point de restauration vers une machine virtuelle amorçable.
Barre d'icônes : icône Événements	 Événements. Cliquez sur l'icône Événements pour afficher le journal de tous les événements système liés au Core de Rapid Recovery.
Barre d'icônes : icône Paramètres	 Paramètres. Cliquez sur l'icône Paramètres pour afficher ou gérer les paramètres du Core de Rapid Recovery. Vous pouvez sauvegarder ou restaurer les paramètres de configuration du Core. Vous pouvez définir des paramètres généraux pour contrôler les ports ou afficher des aspects. De plus, vous pouvez configurer des paramètres dans les catégories suivantes : mises à jour automatiques, tâches nocturnes, paramètres de file d'attente de transfert, paramètres d'expiration du délai d'attente client, paramètres du cache de déduplication DVM, paramètres de Replay Engine et paramètres de déploiement. Vous pouvez afficher ou modifier les connexions de base de données, les paramètres du serveur SMTP, les paramètres du compte de stockage clous et modifier les paramètres de police pour les rapports. Vous pouvez définir les paramètres de capacité d'attachement SQL, les paramètres de la tâche du Core, les paramètres de la licence, les paramètres SNMP et les paramètres vSphere.
Barre d'icônes : icône Plus	 Plus. Cliquez sur l'icône Plus pour accéder à d'autres fonctions importantes. Chacune possède sa propre icône, répertoriés ci-dessous.
Barre d'icônes : icône Plus	 Infos système. Cliquez sur Infos système pour afficher les données relatives au serveur Core de Rapid Recovery. Vous pouvez y voir le nom d'hôte, le système d'exploitation, l'architecture et la mémoire du Core. Vous pouvez voir le nom affiché sur la Core Console. Vous pouvez également afficher le nom de domaine pleinement qualifié du Core sur votre réseau, et le chemin d'accès pour votre cache de métadonnées et vos caches de déduplication. Pour plus d'informations sur la façon de modifier le nom d'affichage, voir Compréhension des informations sur le système du Core . Pour plus d'informations sur le cache de déduplication, voir Compréhension du cache de déduplication et des emplacements de stockage . Pour en savoir plus sur la façon d'ajuster les paramètres, voir Configuration des paramètres du cache de déduplication DVM .

Élément de l'UI	Description		
Barre d'icônes : icône Plus	Archives		Archives. Rapid Recovery vous permet de gérer des archives d'informations depuis le Core. Vous pouvez afficher les informations sur les archives planifiées ou attachées et vous pouvez ajouter, vérifier ou importer des archives.
Barre d'icônes : icône Plus	Montages		Montages. Vous permet d'afficher et démonter des montages locaux et d'afficher et déconnecter des montages distants.
Barre d'icônes : icône Plus	CD d'amorçage		CD d'amorçage. Vous permet de gérer les CD d'amorçage, généralement utilisés pour une restauration BMR (bare metal restore). Vous pouvez créer une image ISO du CD d'amorçage, supprimer une image existante ou cliquer sur le chemin de l'image pour l'ouvrir ou l'enregistrer.
Barre d'icônes : icône Plus	Logithèques		Logithèques. Vous permet d'afficher et de gérer les logithèques associées à votre Core.
Barre d'icônes : icône Plus	Clés de chiffrement		Clés de chiffrement. Vous permet d'afficher, de gérer, d'importer ou d'ajouter des clés de chiffrement que vous pouvez appliquer aux machines protégées. Si elles ne sont pas en cours d'utilisation, vous pouvez supprimer des clés de chiffrement.
Barre d'icônes : icône Plus	Comptes Cloud		Comptes Cloud. Vous permet d'afficher et de gérer les connexions entre votre Core et les comptes de stockage du cloud.
Barre d'icônes : icône Plus	Stratégie de rétention		Stratégie de rétention. Vous permet d'afficher et de modifier la stratégie de rétention du Core, y compris la durée de conservation des points de restauration avant de les regrouper et éventuellement de les supprimer.
Barre d'icônes : icône Plus	Notifications		Notifications. Vous permet de configurer les notifications à propos des événements du Core, définir les paramètres de serveur SMTP pour les notifications par e-mail et définir les réductions des répétitions pour supprimer les notifications répétées sur le même événement.
Barre d'icônes : icône Plus	Téléchargements		Téléchargements. Vous pouvez télécharger le programme d'installation web du logiciel agent, l'utilitaire de montage local ou les fichiers MIB contenant les informations des événements à utiliser dans un navigateur SNMP.
Barre d'icônes : icône Plus	Rapports		Rapports. Vous permet d'accéder aux rapports de planification ou rapports du Core à générer en continu.
Barre d'icônes : icône Plus	Journal du Core		Journal du Core. Vous permet de télécharger fichier journal du Core à des fins de diagnostic.

Menu de navigation gauche

Le tableau suivant décrit l'ensemble des menus pouvant s'afficher dans la zone de navigation gauche :

Tableau 217. Options de menu de la zone de navigation gauche

Élément de l'UI	Description
Menu Machines protégées	Le menu Machines protégées est le premier menu de la zone de navigation gauche. Il s'affiche lorsque votre Core protège au moins une machine.

Élément de l'IU	Description
	Si vous cliquez sur le nom d'une machine en particulier dans ce volet, la page Synthèse s'ouvre et affiche les informations récapitulatives de la machine sélectionnée. Pour en savoir plus sur les opérations que vous pouvez effectuer sur la page Synthèse, voir Affichage des informations récapitulatives d'une machine protégée .
Menu Machines répliquées	Si le nom d'un autre Core Rapid Recovery figure dans les premiers menus du menu de navigation, cela signifie que le Core sur lequel vous consultez la Core Console est un Core cible. Le nom de ce menu provient du Core source, et chaque machine affichée en dessous représente une machine de ce Core source répliquée sur cette cible. Si ce Core cible réplique des points de restauration de plusieurs Core source, chaque Core source possède son propre menu dans la zone de navigation gauche. Si vous cliquez sur le nom d'une machine en particulier dans un menu Machines répliquées, la page Synthèse s'ouvre et affiche les informations récapitulatives de la machine répliquée sélectionnée. Pour en savoir plus sur la réplication, voir Réplication.
Menu Points de restauration uniquement	Si le menu Points de restauration uniquement s'affiche, cela signifie que votre Core conserve des points de récupération d'une ancienne machine protégée ou répliquée. Même si cette machine ne capture plus de nouveaux instantanés, vous conservez les points de restauration précédemment capturés sur votre Core. Ces points de restauration peuvent vous permettre de restaurer des fichiers, mais ne peuvent être utilisés pour restaurer des volumes complets, ajouter des données d'instantané ou effectuer une restauration BMR.
Menu Groupes personnalisés	Si vous avez créé des groupes personnalisés, un menu correspondant s'affiche dans le menu de navigation. Les groupes personnalisés sont des conteneurs logiques servant à regrouper des machines (ex. : par fonction, par organisation ou par site géographique). Les groupes personnalisés peuvent contenir des objets hétérogènes (machines protégées, machines répliquées, etc.). Vous pouvez définir le libellé d'un groupe personnalisé. Comme tous les autres menus, ce nom est affiché en majuscules. Vous pouvez exécuter des actions simultanées sur les éléments semblables d'un groupe personnalisé en cliquant sur la flèche à droite du titre du groupe personnalisé. Par exemple, vous pouvez forcer un instantané pour chaque machine protégée d'un groupe personnalisé. Pour en savoir plus sur la création et la gestion des groupes personnalisés, voir Comprendre les groupes personnalisés.
Menu Archives attachées	Si vous associez des archives à votre Core, chaque archive est répertoriée dans le menu de navigation gauche. Le libellé contient le nom de l'archive. La liste répertorie chaque machine incluse dans l'archive.

Les détails sur les éléments figurant dans la zone de navigation gauche s'affichent dans le tableau suivant.

Tableau 218. Zone de navigation gauche et menus

Élément de l'IU	Description
Filtre de texte des menus des machines 	Le filtre de texte est un champ de texte qui vous permet de filtrer les éléments affichés sur les menus des Machines protégées, des Machines répliquées et des Machines de points de restauration uniquement. Si vous tapez vos critères dans ce filtre, seules les machines correspondant à vos critères s'affichent dans les menus appropriés.
Développer et réduire les détails 	Cliquez sur la flèche à droite du filtre de texte pour développer et réduire les détails des menus des Machines protégées, Machines répliquées et Machines de points de restauration uniquement.
Menu Machines protégées 	Le menu Machines protégées s'affiche dans la zone de navigation gauche de l'interface utilisateur. Dans ce menu, vous pouvez afficher toutes les machines protégées, tous les clusters protégés et toutes les machines répliquées ayant été configurés dans votre Core. Si vous avez des groupes protégés ou des machines de point de restauration uniquement, ils vont également s'afficher dans ce menu.

Élément de l'IU	Description
	Vous pouvez réduire ou développer la vue des machines protégées dans votre Core en cliquant simplement sur la flèche située à gauche de l'étiquette du menu.
	L'icône affichée décrit le type de machine : • Une icône de machine unique représente une machine physique ou une machine virtuelle protégée disposant du logiciel agent de Rapid Recovery. • Une icône à plusieurs machines représente un cluster protégé. • Une icône à double machine vide représente une machine virtuelle VMware utilisant une protection sans agent. • Une icône à triple machine vide représente un hôte VMware vCenter. Si vous cliquez sur le menu Machines protégées, une page Machines protégées s'affiche. Elle affiche toutes les machines protégées sur ce Core dans le volet Machines protégées. Pour plus d'informations, voir Affichage du menu Machines protégées.
Menu Machines répliquées	Si vous répliquez des machines depuis un autre Core de Rapid Recovery, le nom de ce Core s'affiche comme menu distinct dans le menu Machines protégées. Chaque machine répliquée sur ce Core cible à partir du Core source répertorié s'affiche sous ce menu. Pour chaque machine répliquée, l'icône indique le type de machine en cours de réplication. Par exemple, si la réplication concerne une seule machine, l'icône indique une seule machine. Si la réplication concerne un cluster de serveurs, l'icône représente un cluster. Vous pouvez réduire ou développer la vue de ces machines répliquées en cliquant simplement sur la flèche située à gauche de l'étiquette de ce menu. Depuis le menu Machines répliquées, vous pouvez effectuer des actions sur toutes les machines répliquées. Si vous cliquez sur le menu Machines répliquées, la page Machines s'affiche. Cette page affiche toutes les machines protégées sur un autre Core (source) qui sont répliquées sur ce Core cible. Pour plus d'informations, voir Affichage des machines répliquées dans le menu de navigation.
Menu Points de restauration uniquement	Si une machine préalablement protégée sur le Core a été retirée de la protection, mais que ses points de restauration n'ont pas été supprimés, le menu Points de restauration uniquement s'affiche. Chacune des anciennes machines protégées avec des points de restauration conservés s'affichent dans cette liste. Vous pouvez réduire ou développer la vue des machines de points de restauration uniquement en cliquant simplement sur la flèche située à gauche de l'étiquette de ce menu. Depuis le menu Points de restauration uniquement, vous pouvez supprimer les points de restauration pour toutes les machines de type Points de restauration uniquement sur ce Core. Si vous cliquez sur le menu Points de restauration uniquement, la page Machines s'affiche. Elle répertorie toutes les machines pour lesquelles les points de restauration ont été enregistrés. Pour plus d'informations, voir Affichage du menu Points de restauration uniquement.
Menu Groupes personnalisés	Si votre Core comprend des groupes personnalisés, la zone de navigation gauche comporte alors un menu Groupes personnalisés. Chacun des objets de ce groupe personnalisé s'affiche dans cette liste. Vous pouvez réduire ou développer la vue des groupes personnalisés dans votre Core en cliquant simplement sur la flèche située à gauche de l'étiquette du menu. Depuis le menu Groupes personnalisés, vous pouvez effectuer des actions pour des éléments semblables dans le groupe. Si vous cliquez sur le menu Groupes personnalisés, la page Machines s'affiche. Elle présente un volet pour chacun des objets Rapid Recovery qui s'affichent dans votre groupe : machines protégées, machines répliquées et machines de points de restauration uniquement. Pour plus d'informations, voir Affichage du menu Groupes personnalisés.

Élément de l'IU	Description
Menu Archives attachées 	Si vous avez attaché des archives à votre Core, la zone de navigation gauche comprend un menu pour chaque archive attachée. Chacune des machines protégées comprises dans l'archive s'affiche dans cette liste. L'étiquette du menu utilise le nom spécifié lors de l'enregistrement de l'archive. Vous pouvez réduire ou développer la vue des archives attachées dans votre Core en cliquant simplement sur la flèche située à gauche de l'étiquette du menu. Depuis le menu Archives attachées, vous pouvez effectuer des actions pour des éléments semblables dans le groupe. Si vous cliquez sur le menu Archives attachées, la page Machines s'affiche. Elle présente un volet pour chacun des objets Rapid Recovery qui s'affichent dans votre groupe : machines protégées, machines répliquées et machines de points de restauration uniquement. Pour plus d'informations, voir Affichage du menu Groupes personnalisés.

Affichage du volet Machines protégées

Le volet Machines protégées contient des informations concernant toutes les machines protégées sur ce Noyau de la Rapid Recovery. Pour chaque machine protégée (le cas échéant), les informations décrites dans le tableau suivant sont affichées dans la liste.

Tableau 219. Informations concernant chaque machine protégée

Élément de l'interface utilisateur	Description
Sélectionner un élément	Pour chaque ligne du tableau récapitulatif, vous pouvez cocher les cases pour effectuer des actions listées dans les options du menu situées au-dessus du tableau.
Type	Affiche le type de la machine.
Voyant d'état	Des cercles colorés présents dans la colonne État indiquent si une machine est en ligne ou impossible à joindre. L'état de la machine s'affiche lorsque vous placez le curseur au-dessus du cercle de couleur. Les états possibles incluent le vert (machine en ligne et protégée), le jaune (protection suspendue), le rouge (erreur d'authentification) et le gris (hors ligne ou non joignable).
État de chiffrement	L'icône de verrou indique l'état du chiffrement de la machine protégée sélectionnée. Un verrou ouvert indique qu'aucun chiffrement n'a été effectué, tandis qu'un verrou fermé indique que des clés de chiffrement ont été créées. Pour plus d'informations sur le chiffrement, veuillez consulter Comprendre les clés de clés de chiffrement .
Nom d'affichage	Ce champ correspond au nom d'affichage de la machine protégée.
Dernier instantané	Ce champ indique la date et l'heure du dernier transfert de sauvegarde ayant eu lieu pour cette machine.
Nom de la logithèque	Ce champ indique la logithèque dans laquelle les données appartenant à cette machine sont conservées.
Points de récupération	Ce champ indique le nombre de points de récupération ainsi que la quantité d'espace qu'ils occupent dans la logithèque.
Version	Ce champ affiche la version du logiciel Agent de la Rapid Recovery installé sur la machine.
Actions	Lorsque vous cliquez sur le menu déroulant intitulé Paramètres de cette colonne, une liste des actions à effectuer sur la machine protégée sélectionnée s'affiche.

Si une quelconque machine protégée dans ce Noyau est configurée pour une mise en veille virtuelle, vous verrez apparaître des informations supplémentaires, décrites dans le tableau suivant.

Tableau 220. Informations concernant les machines protégées configurées pour une mise en veille virtuelle

Élément de l'interface utilisateur	Description
Dernière exportation	Ce champ indique la date et l'heure de la dernière exportation virtuelle.
Destination	Ce champ indique la destination permettant d'enregistrer la machine protégée en tant que machine virtuelle. Par exemple, ESXi, VMware Workstation, Hyper-V ou VirtualBox.
État	Ce champ indique l'état de la machine configurée pour la mise en veille virtuelle. Les différents états incluent « En cours de synchronisation », « En pause » et « Non activée ».

Depuis le menu déroulant intitulé Actions situé sur le volet Machines protégées, vous pouvez effectuer les actions décrites dans le tableau suivant. Certaines options apparaissent uniquement avec un serveur Exchange ou SQL, comme il est indiqué.

Tableau 221. Actions disponibles depuis le volet Machines protégées

Élément de l'interface utilisateur	Description
Forcer un instantané	Cette option vous permet de forcer un instantané par incréments ou une image de base pour tous les volumes protégés sur les machines protégées sélectionnées. Pour plus d'informations, veuillez consulter Forcer un instantané .
Exportation ponctuelle	Cette option permet de démarrer l'assistant Exportation de machines virtuelles. Grâce à cet assistant, vous pouvez effectuer une exportation ponctuelle des données d'un point de récupération présent sur une machine protégée pour les transférer à une machine virtuelle, dans un format de MV pris en charge. Pour plus d'informations, veuillez consulter VM export (Exportation NFS) .
Mise en veille virtuelle	Cette option permet de démarrer l'assistant Exportation de machines virtuelles. Grâce à cet assistant, vous pouvez effectuer une mise en veille virtuelle afin d'exporter continuellement les données d'un point de récupération présent sur une machine protégée et de les transférer à une machine virtuelle, dans un format de MV pris en charge. Pour plus d'informations, veuillez consulter VM export (Exportation NFS) .
Monter	Cette option permet de démarrer l'assistant Montage. Grâce à cet assistant, vous pouvez monter des points de récupération provenant de la machine protégée sélectionnée.
Points de récupération	Cette option ouvre la page Récapitulatif des points de récupération.
Restaurer	Cette option permet de démarrer l'assistant Restauration de machines. Cette procédure vous permet de restaurer des données provenant d'un point de récupération du Noyau sur une machine protégée. Pour plus d'informations, veuillez consulter À propos de la restauration de volumes à partir d'un point de restauration .
Retirer une machine	Cette option retire la protection du Noyau de la Rapid Recovery d'une machine sélectionnée, vous laissant le choix de supprimer ou de conserver les points de récupération déjà présents sur le Noyau de la Rapid Recovery. Pour plus d'informations, veuillez consulter Supprimer une machine .

Vous pouvez effectuer des actions sur deux machines, ou plus, présentes dans la liste des machines protégées. Pour cela, cochez la case de chaque machine protégée, ensuite, à partir du menu situé au-dessus du tableau récapitulatif, vous pourrez effectuer n'importe quelle action décrite dans le tableau suivant.

Tableau 222. Actions supplémentaires disponibles dans le volet Machines protégées lorsque des machines sont sélectionnées

Élément de l'interface utilisateur	Description
Forcer un instantané	Cette option vous permet de forcer un instantané par incréments pour tous les volumes protégés sur les machines protégées sélectionnées. Pour plus d'informations, veuillez consulter Forcer un instantané .
Forcer une image de base	Cette option vous permet de forcer une image de base pour tous les volumes protégés sur les machines protégées sélectionnées. Pour plus d'informations, veuillez consulter Forcer un instantané .
Protection > suspendre ou reprendre	Cette option vous permet de suspendre la protection pour les machines sélectionnées si la protection était auparavant active, ou de la reprendre si elle avait été suspendue. Pour plus d'informations, veuillez consulter Suspendre et reprendre la protection .
Réplication	Cette option vous permet d'effectuer, de forcer, de copier, de suspendre ou de reprendre une réplication. Vous pouvez également copier des points de récupération existants et les transférer à un lecteur de départ. Pour plus d'informations, veuillez consulter Gestion des paramètres de réplication .
Annuler	Cette option vous permet d'annuler toutes les opérations en cours sur les machines sélectionnées ou d'annuler uniquement les instantanés en cours sur les machines sélectionnées. Cela n'a aucun impact sur les opérations planifiées.
Retirer des machines	Cette option retire la protection du Noyau de la Rapid Recovery d'une machine sélectionnée, vous laissant le choix de supprimer ou de conserver les points de récupération déjà présents sur le Noyau de la Rapid Recovery. Pour plus d'informations, veuillez consulter Supprimer une machine .

Depuis le menu déroulant Configuration, disponible pour chaque machine protégée, vous pouvez effectuer les actions listées dans le tableau suivant. Certaines options apparaissent uniquement pour les serveurs Exchange ou SQL, comme il est indiqué.

Tableau 223. Actions disponibles depuis le volet Machines protégées

Élément de l'interface utilisateur	Description
Forcer un instantané	Cette option vous permet de forcer un instantané par incréments ou une image de base pour un ou plusieurs volumes sur les machines sélectionnées. Pour plus d'informations, veuillez consulter Forcer un instantané .
Forcer la troncature des journaux pour Exchange	Pour une machine protégée sous Exchange Server, cette option force la troncature des journaux Exchange, ce qui libère de l'espace sur le serveur Exchange. Pour plus d'informations, veuillez consulter Forcer la troncature de journal pour une machine SQL .
Forcer la troncature des journaux pour SQL	Pour une machine protégée sous SQL Server, cette option force la troncature des journaux SQL Server, ce qui identifie de l'espace libre sur le serveur SQL. Pour plus d'informations, veuillez consulter Forcer la troncature de journal pour une machine SQL .
Exporter	Cette option démarre l'assistant Exportation. Grâce à cet assistant, vous pouvez exporter les données d'un point de récupération provenant d'une machine protégée et les transférer à une machine virtuelle, dans un format de MV pris en charge. Vous pouvez effectuer une exportation ponctuelle ou configurer une mise en veille virtuelle pour des exportations continues. Pour plus d'informations, veuillez consulter VM export (Exportation NFS) .
Monter	Cette option ouvre la boîte de dialogue intitulée Monter un point de récupération, qui vous permet de parcourir les données d'un instantané enregistrées au moyen du Noyau de la Rapid Recovery dans le but de monter un point de récupération particulier. Pour plus d'informations, veuillez consulter Monter un point de restauration ou Monter un volume d'un point de restauration sur une machine Linux .
Points de récupération	Cette option ouvre l'onglet Points de récupération pour la machine agent sélectionnée. Pour plus d'informations, veuillez consulter Gérer les instantanés et les points de restauration .

Élément de l'interface utilisateur	Description
Restaurer	Cette option permet de démarrer l'assistant Restauration de machines. Cette procédure vous permet de restaurer des données provenant d'un point de récupération du Noyau sur une machine protégée. Pour plus d'informations, veuillez consulter À propos de la restauration de volumes à partir d'un point de restauration .
Retirer une machine	Cette option retire la protection du Noyau de la Rapid Recovery d'une machine sélectionnée, vous laissant le choix de supprimer ou de conserver les points de récupération déjà présents sur le Noyau de la Rapid Recovery. Pour plus d'informations, veuillez consulter Supprimer une machine .

Affichage des événements pour une machine protégée

Sur la page **Événements**, vous pouvez afficher les tâches qui se sont déjà produites ou sont en cours pour la machine protégée que vous avez sélectionnée. Les boutons situés en haut de la page vous permettent de naviguer jusqu'aux listes des tâches dans chacune des trois catégories d'activités :

- **Tâches.** Une tâche que Rapid Recovery doit exécuter pour fonctionner correctement.
- **Alertes.** Notification relative à une tâche ou un événement, comprenant les erreurs et les avertissements.
- **Journal.** Combinaison de toutes les tâches et alertes relatives à la machine protégée.

Le tableau suivant comprend des descriptions de chacun des éléments de la page **Événements**.

Tableau 224. Éléments de la page Événements

Élément de l'UI	Description
Mot-clé de recherche	Vous permet de rechercher un élément spécifique dans chaque catégorie. Disponible pour les tâches uniquement.
From	Pour affiner vos résultats, vous pouvez entrer la date à laquelle vous voulez commencer la recherche. Disponible pour les tâches uniquement.
To	Pour affiner vos résultats, vous pouvez entrer la date à laquelle vous voulez arrêter la recherche. Disponible pour les tâches uniquement.
Icônes d'état	Chaque icône représente un état différent de la tâche. Pour les alertes et les tâches, en cliquant sur une des icônes, vous pouvez filtrer la liste en fonction de cet état, ce qui va générer un rapport. En cliquant sur l'icône une deuxième fois, vous supprimez le filtre pour cet état. Vous pouvez filtrer en utilisant plus d'un état. Les états comprennent : • Actif. Une tâche en cours. • En file d'attente. Une tâche en attente de la fin d'une autre tâche pour pouvoir commencer. • En attente. Une tâche qui attend votre approbation ou une finalisation, comme un disque source. (Pour plus d'informations sur les disques sources, voir Réplication.) • Terminé. Une tâche qui a été achevée avec succès. • Échec. Une tâche qui a échoué et n'a pas pu être terminée.
Icône de service	Ce bouton ajoute des tâches de service à la liste des tâches. Lorsque vous cliquez sur cette icône, une icône de service plus petite s'affiche sur chacune des icônes d'état, ce qui vous permet de filtrer par tâches de service dans cet état (s'il y en a). Exemples de tâches de service : suppression des fichiers d'indexation ou retrait de la protection d'une machine.
Liste déroulante des types d'exportation	La liste déroulante comprend les formats auxquels vous pouvez exporter le rapport des événements. Disponible pour les tâches uniquement. Elle comprend les formats suivants : • PDF

Élément de l'IU	Description
	• HTML • CSV • XLS • XLSX
 (Icône d'exportation)	Convertit le rapport des événements au format choisi. Disponible pour les tâches uniquement.
Choix des pages	Les rapports des événements peuvent inclure de multiples tâches réparties sur plusieurs pages. Les numéros et les flèches au bas de la page Événements vous permettent de naviguer entre les différentes pages du rapport.

La page **Événements** affiche tous les événements sous forme de tableau. Le tableau suivant répertorie les informations affichées pour chaque élément.

Tableau 225. Informations détaillées sur le tableau récapitulatif des événements

Élément de l'IU	Description
État	Indique l'état de la tâche, de l'alerte ou de l'élément de journal. Disponible pour les alertes ou les éléments de journal, cliquez sur l'en-tête pour filtrer les résultats par état.
Nom	Le nom est uniquement disponible pour les tâches. Ce champ de texte répertorie les types de tâche qui se sont terminées pour cette machine protégée. Exemples : transfert de volume, entretien de logithèque, consolidation, vérification de montabilité, vérification de somme de contrôle, etc.
Heure de début	Disponible pour les tâches, alertes et éléments de journal. Affiche la date et l'heure auxquelles la tâche ou l'opération a débuté.
Heure de fin	Disponible pour les tâches uniquement. Indique la date et l'heure auxquelles l'événement est survenu.
 Détails de la tâche	Disponible pour les tâches uniquement. Ouvre la boîte de dialogue Surveiller la tâche active , afin de pouvoir afficher les détails d'une tâche ou d'une opération spécifique. Ces informations comprennent un ID pour la tâche, la vitesse de transfert du Core (si applicable), le temps écoulé pour l'exécution de la tâche, le travail total en gigaoctets et toute tâche enfant associée à la tâche.
Message	Disponible pour les alertes et éléments de journal. Ce champ de texte fournit un message descriptif de l'alerte ou de l'élément du journal.

Affichage du menu Plus pour une machine protégée

Le menu **Plus** offre des options supplémentaires pour gérer la machine protégée sélectionnée. Pour accéder à ces outils, cliquez sur le menu déroulant intitulé Plus et sélectionnez une des options décrites dans le tableau suivant.

Tableau 226. Outils accessibles depuis l'option Plus pour une machine protégée

Élément de l'interface utilisateur	Description
	Ce champ affiche les informations de la machine protégée : les informations système, les volumes, les processeurs, les adaptateurs réseau et les adresses IP. Pour en savoir plus, veuillez consulter Affichage des informations sur le système d'une machine protégée.

Élément de l'interface utilisateur

Description

Informations système



Montages

À partir du volet Montages locaux, vous pouvez afficher ou démonter les volumes montés localement. Depuis le volet Montages à distance, vous pouvez afficher ou démonter les volumes montés à l'aide de l'utilitaire de montage local.

Pour plus d'informations sur le démontage des volumes, veuillez consulter [Démonter des points de restauration](#).

Pour plus d'informations sur le montage local d'un point de récupération, veuillez consulter [Monter un point de restauration](#) ou encore [Monter un volume d'un point de restauration sur une machine Linux](#).



Stratégie de conservation

Cette option vous permet de définir une stratégie de conservation pour la machine sélectionnée. Vous pouvez sélectionner la stratégie par défaut du Noyau ou définir une stratégie de conservation unique à cette machine.

Pour plus d'informations, veuillez consulter [Personnalisation des paramètres de la stratégie de conservation pour une machine protégée](#).



Notifications

Cette option vous permet de définir un groupe de notifications personnalisé pour les événements ayant trait à cette machine. Cela n'affecte pas les notifications préalablement définies sur le Noyau. Pour plus d'informations, veuillez consulter [Configurer les groupes de notification](#).



Journal de l'agent

Cette option vous permet de télécharger et d'afficher le fichier journal pour une machine protégée au moyen du logiciel Agent de la Rapid Recovery. Pour plus d'informations, veuillez consulter [Téléchargement et affichage du fichier journal d'une machine protégée](#).

Description du module PowerShell de Rapid Recovery

Dell Data Protection | Rapid Recovery comprend plusieurs composants logiciels. Cette rubrique décrit les principaux composants du logiciel :

- Le Core Rapid Recovery gère l'authentification des machines protégées, planifie le transfert des données sauvegardées et répliquées, exporte des données vers des machines virtuelles, génère des rapports et effectue des restaurations BMR (sur un matériel similaire ou différent).
- L'agent Rapid Recovery est chargé de réaliser des instantanés de volume et de transférer rapidement les données vers la logithèque gérée par le Core.
- Le module PowerShell de Rapid Recovery est un utilitaire Windows qui permet aux utilisateurs d'interagir avec le serveur Core à l'aide de scripts Windows PowerShell®. Ce module dispose de fonctionnalités en commun avec l'interface utilisateur graphique de la console Core de Rapid Recovery. Par exemple, le module Powershell de Rapid Recovery peut monter des points de restauration Rapid Recovery ou forcer un instantané d'une machine protégée.

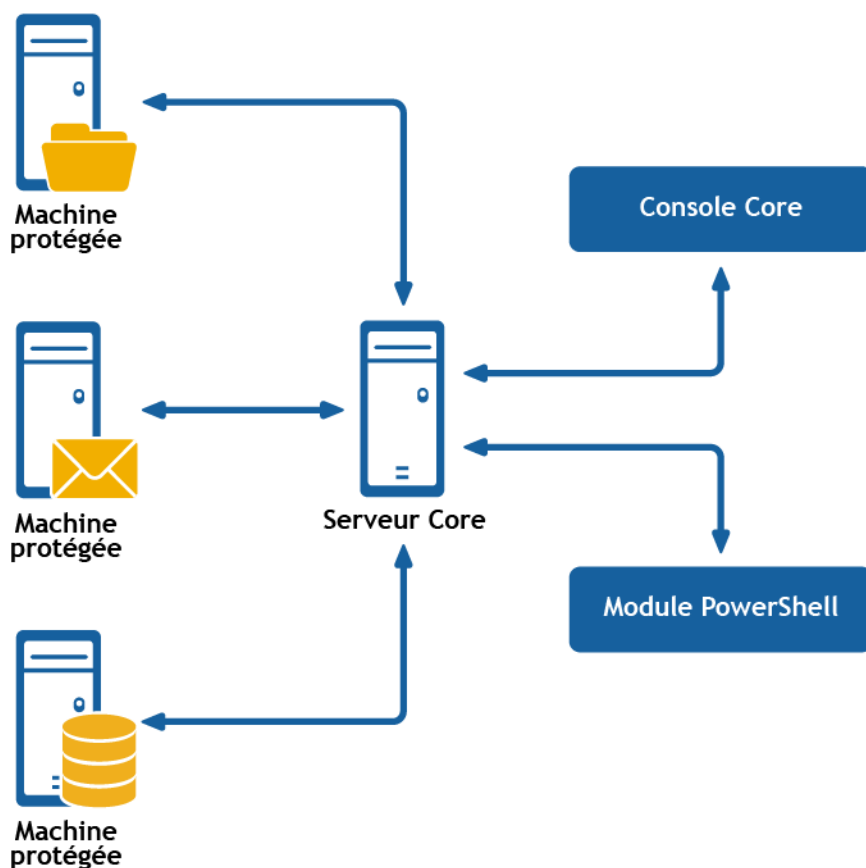


Figure 14. Le module PowerShell interagit avec le Core Rapid Recovery

PowerShell est un environnement connecté Microsoft .NET Framework conçu pour l'automatisation administrative. Cette section décrit le module PowerShell de Rapid Recovery et les cmdlets que les administrateurs peuvent utiliser pour scripter certaines fonctions sans interagir avec l'interface graphique du Core Rapid Recovery.

❗ **REMARQUE :** Vous pouvez également exécuter des scripts PowerShell en tant que pré- ou post-scripts. Pour en savoir plus et avoir des exemples de scripts, voir [Extension des tâches Rapid Recovery avec des scripts](#).

Sujets :

- [Prérequis pour l'utilisation de PowerShell](#)
- [Utilisation de commandes et de cmdlets](#)
- [Cmdlets PowerShell de Rapid Recovery](#)
- [Localisation](#)
- [Qualificateurs](#)

Prérequis pour l'utilisation de PowerShell

Avant d'utiliser le module PowerShell de Rapid Recovery, vous devez installer Windows PowerShell version 2.0 ou ultérieure. En raison de nouvelles fonctionnalités introduites dans PowerShell 3.0, notamment la facilitation de l'accès aux propriétés des objets, l'accès à PowerShell Web, et la prise en charge d'appels REST, Dell recommande l'utilisation de PowerShell version 3.0 ou ultérieure.

❗ **REMARQUE :** Veillez à placer le fichier `powershell.exe.config` dans le répertoire de base PowerShell. Par exemple, 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>
```

Lancement de PowerShell et importation du module

Contrairement à d'autres modules du système, le module PowerShell de Rapid Recovery n'est pas chargé par défaut. À chaque session, vous pouvez ouvrir Windows PowerShell avec des privilèges administratifs, puis importer le module. Suivez les étapes de cette procédure pour lancer PowerShell et importer le module PowerShell de Rapid Recovery.

- 1 Ouvrez une invite de commande avec privilèges élevés pour Windows PowerShell. Par exemple, tapez Windows PowerShell dans le menu Démarrer, puis pour l'application Windows PowerShell résultante, faites un clic droit et sélectionnez **Exécuter comme administrateur**.
Windows PowerShell s'ouvre dans une nouvelle fenêtre de commande.
- 2 Entrez la commande suivante, puis appuyez sur Entrée :
`Import-Module "RapidRecoveryPowerShellModule"`
Le module PowerShell Rapid Recovery est importé pour votre session actuelle. Vous pouvez commencer à exécuter des applets dans la fenêtre de commande existante.

Utilisation de commandes et de cmdlets

Les cmdlets sont des commandes spécialisées utilisées dans un script Windows PowerShell qui exécute une seule fonction. Une cmdlet est normalement exprimée en tant que paire verbe-substantif. Le résultat renvoyé par une cmdlet est un objet.

Vous pouvez utiliser le mécanisme de pipeline (chaînage des processus) pour les commandes PowerShell, ce qui permet d'envoyer le résultat d'une cmdlet à une autre cmdlet en entrée. Pour donner un unique exemple, vous pouvez demander la liste des commandes du module Rapid Recovery PowerShell, et trier cette liste par nom. L'exemple de script pour ce cas de figure est le suivant :

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

Aide et exemples pour les cmdlets

Après avoir ouvert PowerShell et importé le module PowerShell de Rapid Recovery, vous pouvez demander des renseignements complémentaires à tout moment à l'aide de la cmdlet `Get-Help <nom_de_la_commande>`. Par exemple, pour obtenir des informations sur la cmdlet d'exportation de machine virtuelle, entrez la cmdlet suivante, puis appuyez sur Entrée :

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

L'objet renvoyé comprend le nom, le synopsis et la syntaxe de la commande, ainsi que toutes les options que vous pouvez utiliser avec la commande.

Une autre méthode permettant d'obtenir de l'aide pour une cmdlet spécifique consiste à saisir le nom de la commande, suivi de `-?`. Par exemple :

```
Start-VMExport -?
```

Vous pouvez également demander des exemples d'une cmdlet en exécutant la commande suivante :

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

Cmdlets PowerShell de Rapid Recovery

Cette section décrit les cmdlets et les options disponibles dans le module PowerShell de Rapid Recovery. Toutes les cmdlets du module PowerShell de Rapid Recovery prennent en charge les paramètres communs suivants :

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

Pour en savoir plus, utilisez la commande `Get-Help about_commonparameters`.

Les cmdlets disponibles sont répertoriées dans le tableau suivant.

Tableau 227. Cmdlets du module PowerShell de Rapid Recovery

Nom de la cmdlet	Description
Edit-EsxiVirtualStandby	Permet de modifier une configuration de disque de secours virtuel ESXi existante.
Edit-HyperVVirtualStandby	Permet de modifier une configuration de disque de secours virtuel Hyper-V existante.
Edit-VBVirtualStandby	Permet de modifier une configuration de disque de secours virtuel VirtualBox existante.

Nom de la cmdlet	Description
Edit-VMVirtualStandby	Permet de modifier une configuration de disque de secours virtuel VMware Workstation existante.
Edit-ScheduledArchive	Permet de modifier une configuration d'archive programmée existante.
Get-ActiveJobs	Permet de récupérer un ensemble de tâches actives.
Get-CloudAccounts	Permet de récupérer des informations sur les comptes Cloud enregistrés dans le Core.
Get-Clusters	Permet de récupérer un ensemble de clusters protégés.
Get-CompletedJobs	Permet de récupérer un ensemble de tâches terminées.
Get-ExchangeMailStores	Permet de récupérer un ensemble de magasins d'e-mails Exchange.
Get-Failed	Permet de récupérer des informations sur les points de restauration ayant échoué.
Get-FailedJobs	Permet de récupérer un ensemble de tâches ayant échoué.
Get-Mounts	Permet d'afficher tous les points de restauration montés.
Get-Passed	Permet de récupérer des informations sur les points de restauration ayant réussi.
Get-ProtectedServers	Permet de récupérer des informations sur les serveurs protégés.
Get-ProtectionGroups	Permet de récupérer un ensemble de groupes de protection.
Get-QueuedJobs	Permet de récupérer un ensemble de tâches placées en file d'attente.
Get-RecoveryPoints	Permet de récupérer des informations sur les points de restauration.
Get-ReplicatedServers	Permet de récupérer des informations sur les serveurs répliqués.
Get-Repositories	Permet de récupérer des informations sur les logithèques.
Get-ScheduledArchive	Permet de récupérer des informations sur les tâches d'archivage récurrentes.
Get-SqlDatabases	Permet de récupérer un ensemble de bases de données SQL.
Get-UnprotectedVolumes	Permet de récupérer un ensemble de volumes non protégés.
Get-VirtualizedServers	Permet de récupérer des informations sur les serveurs virtualisés.
Get-Volumes	Permet de récupérer des informations sur les volumes.
New-Base	Permet de forcer un instantané de l'image de base.
New-CloudAccount	Permet d'ajouter un nouveau compte Cloud au Core.
New-EncryptionKey	Permet de créer une nouvelle clé de chiffrement.
New-EsxiVirtualStandby	Permet de créer une nouvelle machine virtuelle avec disque de secours virtuel ESXi.
New-HyperVVirtualStandby	Permet de créer une nouvelle machine virtuelle avec disque de secours virtuel Hyper-V.
New-Mount	Permet de monter des points de restauration.
New-Replication	Permet de configurer et de forcer la réplication.
New-Repository	Permet de créer une nouvelle logithèque DVM.
New-ScheduledArchive	Permet de planifier un nouvel archivage récurrent.
New-Snapshot	Permet de forcer un instantané.
New-VBVirtualStandby	Permet de créer une nouvelle machine virtuelle avec disque de secours virtuel VirtualBox.

Nom de la cmdlet	Description
New-VMVirtualStandby	Permet de créer une nouvelle machine virtuelle avec disque de secours virtuel VMware Workstation.
Push-Replication	Permet de forcer la réplication.
Push-Rollup	Permet de forcer la consolidation.
Remove-Agent	Permet de mettre fin à la protection d'une machine.
Remove-Mount	Permet de démonter un point de restauration.
Remove-Mounts	Permet de démonter tous les points de restauration montés.
Remove-RecoveryPoints	Permet de supprimer les points de restauration d'une machine protégée.
Remove-Repository	Permet de supprimer une logithèque DVM existante.
Remove-ScheduledArchive	Permet d'annuler un archivage planifié.
Remove-VirtualStandby	Permet de supprimer une machine virtuelle avec disque virtuel de secours du Core.
Resume-Replication	Permet de reprendre la réplication.
Resume-RepositoryActivity	Permet de relancer l'activité d'une logithèque.
Resume-ScheduledArchive	Permet de reprendre un archivage planifié.
Resume-Snapshot	Permet de reprendre un instantané.
Resume-VirtualStandby	Permet de reprendre l'exportation de données vers une machine virtuelle avec disque virtuel de secours.
Start-Archive	Permet d'archiver des points de restauration.
Start-AttachabilityCheck	Permet de forcer la vérification de la capacité d'attachement des bases de données MS SQL protégées.
Start-ChecksumCheck	Permet de forcer la vérification de la capacité d'attachement des magasins d'e-mails Exchange protégés.
Start-EsxiExport	Permet de forcer l'exportation sur un serveur ESXi.
Start-HypervExport	Permet de forcer l'exportation sur un serveur Hyper-V.
Start-LogTruncation	Permet de forcer la troncature de journal.
Start-MountabilityCheck	Permet de forcer la vérification de la montabilité des magasins d'e-mails Exchange protégés.
Start-Protect	Permet de mettre un serveur sous protection.
Start-ProtectCluster	Permet de mettre un cluster sous protection.
Start-RepositoryCheck	Permet de forcer la vérification d'une logithèque DVM.
Start-RestoreArchive	Permet de restaurer l'archive à l'aide de points de restauration.
Start-ScheduledArchive	Permet de forcer le transfert de données d'un archivage planifié.
Start-VBExport	Permet de forcer l'exportation sur un serveur VirtualBox.
Start-VirtualStandby	Permet de forcer un transfert de données vers une machine virtuelle avec disque de secours virtuel existante.
Start-VMExport	Permet de forcer l'exportation sur un serveur VMWare Workstation.
Stop-ActiveJobs	Permet d'annuler les tâches actives.

Nom de la cmdlet	Description
Suspend-Replication	Permet de suspendre la réplication.
Suspend-RepositoryActivity	Permet de suspendre l'activité d'une logithèque.
Suspend-ScheduledArchive	Permet de suspendre les transferts de données d'un archivage planifié.
Suspend-Snapshot	Permet de suspendre un instantané.
Suspend-VirtualStandby	Permet de suspendre les transferts de données vers une machine virtuelle avec disque de secours virtuel.
Update-Repository	Permet d'ajouter une extension à une logithèque DVM.

Edit-EsxiVirtualStandby

La commande `Edit-EsxiVirtualStandby` permet d'utiliser PowerShell pour modifier une exportation virtuelle existante sur une machine virtuelle ESXi.

Utilisation

L'utilisation de la commande est la suivante :

```

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

```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Edit-EsxiVirtualStandby` :

Tableau 228. Options de la commande Edit-EsxiVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Option	Description
-all	Affiche toutes les tâches, dont celles exécutées par le core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont les suivantes : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance de logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD de démarrage), 'diagnostics' (chargement de journaux), 'exchange' (vérification de fichiers Exchange Server), 'export' (exportation de point de restauration), 'pushinstall' (déploiement d'agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation de points de restauration), 'sqlattach' (vérifications de la capacité d'attachement de l'agent) et 'mount' (montage de logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Edit-HyperVVirtualStandby

La commande `Edit-HyperVVirtualStandby` permet d'utiliser PowerShell pour modifier une exportation virtuelle existante sur une machine virtuelle Hyper-V.

Utilisation

L'utilisation de la commande est la suivante :

```
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>]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Edit-HyperVVirtualStandby` :

Tableau 229. Options de la commande Edit-HyperVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont les suivantes : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance de logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD de démarrage), 'diagnostics' (chargement de journaux), 'exchange' (vérification de fichiers Exchange Server), 'export' (exportation de point de restauration), 'pushinstall' (déploiement d'agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation de points de restauration), 'sqlattach' (vérifications de la capacité d'attachement de l'agent) et 'mount' (montage de logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Edit-ScheduledArchive

La commande `Edit-ScheduledArchive` vous permet d'utiliser PowerShell pour apporter des modifications à une archive planifiée existante.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Edit-ScheduledArchive` :

Tableau 230. Options de la commande `Edit-ScheduledArchive`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	La machine protégée contenant les points de restauration que vous souhaitez archiver. Vous pouvez spécifier plusieurs noms de machine entourés de guillemets doubles et séparés par des virgules.
-all	Archivez les points de restauration de toutes les machines protégées.
-path	Le chemin où sauvegarder les données archivées. Par exemple : - Machine locale : « d: \work\archive » - Chemin réseau : « \\servername\sharename » - Dossier dans un compte Cloud : « nom du dossier »  REMARQUE : Le nombre de symboles ne doit pas être supérieur à 100 pour les emplacements locaux et réseau, et il ne doit pas être supérieur à 150 pour un emplacement de Cloud.
-cloudaccountname	Facultatif. À utiliser uniquement pour l'archivage Cloud. Le nom du compte Cloud dans lequel vous souhaitez enregistrer l'archive.

Option	Description
<code>-cloudcontainer</code>	Facultatif. À utiliser uniquement pour l'archivage Cloud. Le nom du conteneur dans le compte Cloud choisi, où l'archive doit être enregistrée. Lorsque vous utilisez cette option, vous devez également spécifier le paramètre « <code>-cloudaccountname</code> ».
<code>-recycleaction</code>	Le type d'action de recyclage. Spécifié en utilisant une des quatre valeurs suivantes : « <code>replacethiscore</code> » - Remplace les données archivées existantes appartenant au Core, mais ne change pas les données des autres Cores. « <code>erasecompletely</code> » - Efface toutes les données archivées du répertoire avant d'écrire la nouvelle archive. « <code>incremental</code> » - Permet d'ajouter des points de restauration à une archive existante. La fonction compare les points de restauration pour éviter de dupliquer les données qui existent déjà dans l'archive.
<code>-scheduletype</code>	Type d'intervalle de planification. A spécifié l'option en utilisant une des quatre valeurs suivantes : « <code>daily</code> » - Pour les archives quotidiennes créées automatiquement. « <code>weekly</code> » - Pour les archives hebdomadaires créées automatiquement. Vous devez spécifier le paramètre « <code>-dayofweek</code> ». « <code>monthly</code> » - Pour les archives mensuellement créées automatiquement. Vous devez spécifier le paramètre « <code>-dayofmonth</code> ». Si un mois ne possède pas le jour précisé (par exemple « <code>31</code> ») alors l'archive n'aura pas lieu pour ce mois. « <code>lastdayofmonth</code> » - Pour automatiquement créer une archive le dernier jour de chaque mois.
<code>-dayofweek</code>	À utiliser uniquement pour l'option « <code>weekly</code> » du paramètre « <code>-scheduletype</code> ». Le jour de la semaine de création automatique de l'archive (par exemple, « <code>lundi</code> »).
<code>-dayofmonth</code>	À utiliser uniquement pour l'option « <code>month</code> » du paramètre « <code>-scheduletype</code> ». Le jour (numéro) du mois de création automatique de l'archive (par exemple, « <code>15</code> »).
<code>-time</code>	L'heure du jour de création d'une archive.
<code>-initialpause</code>	Facultatif. Spécifiez cette option si vous souhaitez suspendre initialement l'archivage après avoir configuré la planification de l'archivage.
<code>-id</code>	L'identificateur de l'archive planifiée que vous souhaitez modifier.

Exemple :

Modifiez une archive planifiée sur le Core local :

```
>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

La commande `Edit-VBVirtualStandby` permet d'utiliser PowerShell pour modifier une exportation virtuelle existante vers une machine virtuelle VirtualBox.

Utilisation

L'utilisation de la commande est la suivante :

```
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>]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Edit-VBVirtualStandby` :

Tableau 231. Options de la commande Edit-VBVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont les suivantes : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance de logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD de démarrage), 'diagnostics' (chargement de journaux), 'exchange' (vérification de fichiers Exchange Server), 'export' (exportation de point de restauration), 'pushinstall' (déploiement d'agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation de points de restauration), 'sqlattach' (vérifications de la capacité d'attachement de l'agent) et 'mount' (montage de logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent :

Option	Description
	#d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant)
	#h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant)
	"time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Edit-VMVirtualStandby

La commande `Edit-VMVirtualStandby` vous permet d'utiliser PowerShell pour apporter des modifications à une exportation virtuelle vers une machine virtuelle VMWare Workstation (VM).

Utilisation

L'utilisation de la commande est la suivante :

```

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

```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Edit-VMVirtualStandby` :

Tableau 232. Options de la commande Edit-VMVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le core et tous les serveurs protégés.
-number	Facultatif. Détermine combien d'enregistrements afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance de logithèque), 'replication' (Répliquions locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD d'amorçage), 'diagnostics' (Journaux de téléchargements), 'exchange' (vérification des fichiers Exchange Server), 'export' (exportation des points de restauration), 'pushinstall' (déploiement d'agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation des points de restauration), 'sqlattach' (vérification de la capacité d'attachement de l'agent), et 'mount' (montage d'une logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Get-ActiveJobs

La commande `Get-ActiveJobs` renvoie toutes les tâches actives depuis le Core. Le paramètre `-jobtype` peut être utilisé pour observer des tâches spécifiques.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ActiveJobs` :

Tableau 233. Options de la commande Get-ActiveJobs

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le Core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD d'amorçage), 'diagnostics' (charger les journaux), 'exchange' (vérification des fichiers Exchange Server), 'export' (exporter des points de restauration), 'pushinstall' (déployer des agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation des points de restauration), 'sqlattach' (vérification de la capacité d'attachement de l'agent) et 'mount' (monter une logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Get-Clusters

La commande `Get-Clusters` renvoie des informations sur les clusters de serveurs protégés sur le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Clusters` :

Tableau 234. Options de la commande Get-Clusters

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie les clusters de serveurs protégés sur le Core local :

```
>Get-Clusters
```

Get-CompletedJobs

La commande `Get-CompletedJobs` renvoie la liste des tâches terminées sur le Core. Le paramètre `-jobtype` peut être utilisé pour observer des tâches spécifiques.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-CompletedJobs` :

Tableau 235. Options de la commande `Get-CompletedJobs`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le Core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD d'amorçage), 'diagnostics' (charger les journaux), 'exchange' (vérification des fichiers Exchange Server), 'export' (exporter des points de restauration), 'pushinstall' (déployer des agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation des points de restauration), 'sqlattach' (vérification de la capacité d'attachement de l'agent) et 'mount' (monter une logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Liste toutes les tâches actives sur le Core local :

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

Liste toutes les tâches de création de logithèque terminées sur le Core :

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

Get-ExchangeMailStores

La commande `Get-ExchangeMailStores` renvoie des informations sur les magasins d'e-mails des serveurs Exchange protégés par le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ExchangeMailStores` :

Tableau 236. Options de la commande `Get-ExchangeMailStores`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Répertorie les magasins d'e-mails Exchange pour le serveur Exchange du Core local :

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

Get-Failed

La commande `Get-Failed` renvoie des informations sur les points de restauration ayant échoué sur le Core local.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Failed` :

Tableau 237. Options de la commande Get-Failed

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.

Exemple :

Répertorie tous les points de restauration ayant échoué :

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

Get-FailedJobs

La commande `Get-FailedJobs` renvoie toutes les tâches échouées depuis le Core local.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-FailedJobs` :

Tableau 238. Options de la commande `Get-FailedJobs`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-all	Affiche toutes les tâches, dont celles exécutées par le Core et tous les serveurs protégés.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
-jobtype	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD d'amorçage), 'diagnostics' (charger les journaux), 'exchange' (vérification des fichiers Exchange Server), 'export' (exporter des points de restauration), 'pushinstall' (déployer des agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation des points de restauration), 'sqlattach' (vérification de la capacité d'attachement de l'agent) et 'mount' (monter une logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
-time	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant)

Option	Description
	"time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Répertorie toutes les tâches échouées sur le Core local :

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

Liste tous les échecs de création de tâches de sauvegarde sur le Core :

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

Get-Mounts

La commande `Get-Mounts` renvoie tous les points de restauration montés sur le Core local.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Mounts` :

Tableau 239. Options de la commande Get-Mounts

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Montre tous les points de restauration montés :

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

Get-Passed

La commande `Get-Passed` renvoie des informations sur les points de restauration qui ont passé avec succès les vérifications sur le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Passed` :

Tableau 240. Options de la commande Get-Passed

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie tous les points de restauration sur le Core local ayant passé avec succès les vérifications :

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

La commande `Get-ProtectedServers` renvoie des informations sur les machines protégées sur le Core local.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ProtectedServers` :

Tableau 241. Options de la commande `Get-ProtectedServers`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie toutes les machines actuellement protégées sur le Core local :

```
>Get-ProtectedServers
```

Get-ProtectionGroups

La commande `Get-ProtectionGroups` renvoie des informations sur les groupes de protection du Core local.

Utilisation

L'utilisation de la commande est la suivante :

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |  
-protectedserver [server name or IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ProtectionGroups` :

Tableau 242. Options de la commande Get-ProtectionGroups

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Répertorie tous les groupes de protection sur le Core local :

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

La commande `Get-QueuedJobs` renvoie tous les travaux en attente depuis le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Get-ActiveJobs` :

Tableau 243. Options de la commande Get-ActiveJobs

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-protectedserver</code>	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
<code>-all</code>	Affiche toutes les tâches, dont celles exécutées par le core et tous les serveurs protégés.
<code>-number</code>	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont les suivantes : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.
<code>-jobtype</code>	Facultatif. Indique le filtre du type de tâche. Les valeurs disponibles sont : 'transfer' (transfert de données), 'repository' (maintenance de logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD de démarrage), 'diagnostics' (chargement de journaux), 'exchange' (vérification de fichiers Exchange Server), 'export' (exportation de point de restauration), 'pushinstall' (déploiement d'agents), 'rollback' (restauration à partir d'un point de restauration), 'rollup' (consolidation de points de restauration), 'sqlattach' (vérifications de la capacité d'attachement de l'agent) et 'mount' (montage de logithèque). Toutes les tâches, d'un type spécifié, sont retournées par défaut.
<code>-time</code>	Facultatif. Filtrer la sortie par date et heure auxquelles la tâche a démarré. Les types d'entrée d'entrées disponibles comprennent : #d ou DD (où # représente le nombre pour la période des jours écoulés avant maintenant jusqu'à maintenant) #h ou #H (où # représente le nombre pour la période des heures écoulées avant maintenant jusqu'à maintenant) "time date 1", "time date 2" (pour afficher une plage d'heures personnalisée à partir d'une date spécifique apparaissant avant la virgule jusqu'à une date spécifique après la virgule).

Exemple :

Répertorie toutes les tâches en attente sur le Core local :

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

La commande `Get-RecoveryPoints` renvoie des informations sur les points de restauration des machines protégées sur le Core local.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-RecoveryPoints` :

Tableau 244. Options de la commande `Get-RecoveryPoints`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-number	Facultatif. Détermine le nombre d'enregistrements à afficher. Les valeurs disponibles sont : all (afficher toutes les tâches); l[nombre] ou [nombre] (récupère les x tâches les plus récentes triées par exécution et par heure); f[nombre] (affiche les x premières tâches de restauration triées par exécution et par heure). Par défaut, ce sont les 20 tâches les plus récentes qui sont affichées.

Exemple :

Répertorie tous les points de restauration pour les machines protégées sur le Core local :

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

La commande `Get-ReplicatedServers` renvoie des informations sur les machines répliquées sur le Core local.

Utilisation

L'utilisation de la commande est la suivante :

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

Dell vous conseille de prendre des mesures de sécurité adéquates lors de l'utilisation de commandes permettant de renvoyer des valeurs. Par exemple, cette commande renvoie le mot de passe d'administrateur pour chaque serveur répliqué. Si vous l'utilisez sur la plateforme MSP du Core cible, le mot de passe de connexion de l'administrateur risque d'être compromis. Si les données des logithèques sont chiffrées sur votre plateforme, votre sécurité n'est pas en danger.

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ReplicatedServers` :

Tableau 245. Options de la commande `Get-ReplicatedServers`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie tous les serveurs répliqués sur le Core local :

```
>Get-ReplicatedServers
```

Get-Repositories

La commande `Get-Repositories` renvoie des informations sur les logithèques du Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Repositories` :

Tableau 246. Options de la commande `Get-Repositories`

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie les logithèques présentes sur le Core local :

```
>Get-Repositories
```

Get-ScheduledArchives

La commande `Get-ScheduledArchives` vous permet d'utiliser PowerShell pour afficher des informations sur les archives programmées Rapid Recovery associés à ce Core.

Utilisation

L'utilisation de la commande est la suivante :

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-ScheduledArchives` :

Tableau 247. Options de la commande Get-ScheduledArchives

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Obtenez des informations sur les archives planifiées sur ce Core :

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

La commande `Get-SqlDatabases` renvoie la liste des bases de données SQL à partir de la machine protégée spécifiée.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-SqlDatabases` :

Tableau 248. Options de la commande Get-SqlDatabases

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-protectedserver</code>	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Répertorie toutes les tâches des bases de données SQL sur le Core local :

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

La commande `Get-UnprotectedVolumes` renvoie des informations sur les volumes disponibles à la protection, mais non protégés actuellement sur le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-UnprotectedVolumes` :

Tableau 249. Options de la commande Get-UnprotectedVolumes

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-protectedserver</code>	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Répertorie tous les volumes disponibles à la protection (sauf les volumes protégés) sur l'agent spécifié :

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

La commande `Get-VirtualizedServers` renvoie des informations sur les serveurs virtualisés.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-VirtualizedServers` :

Tableau 250. Options de la commande `Get-VirtualizedServers`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Répertorie tous les serveurs virtualisés sur le Core local :

```
>Get-VirtualizedServers
```

Get-Volumes

La commande `Get-Volumes` renvoie des informations sur les volumes d'une machine spécifiée protégée par le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Get-Volumes` :

Tableau 251. Options de la commande `Get-Volumes`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.

Exemple :

Répertorie tous les volumes sur la machine spécifiée :

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

La commande `New-Base` force une nouvelle base d'images résultant d'un transfert de données vers la machine active protégée. Lorsque vous forcez une base d'images, le transfert démarre immédiatement ou est ajouté à la file d'attente. Seules les données qui ont changé depuis un point de restauration précédent seront transférées. S'il n'existe aucun point de restauration précédent, toutes les données des volumes protégés seront transférées.

Utilisation

L'utilisation de la commande est la suivante :

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -
password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-Base` :

Tableau 252. Options de la commande New-Base

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Base d'images pour tous les agents.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Forcer pour le nom de la machine protégée active.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Forcer une image de base pour toutes les machines protégées :

```
>New-Base -all
```

New-CloudAccount

La commande `New-CloudAccount` vous permet d'ajouter un nouveau compte cloud au Core Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display name] -type [cloud account type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] - authurl [authorization url]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-CloudAccount` :

Tableau 253. Options de la commande New-CloudAccount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-displayname	Le nom du compte cloud à afficher.
-type	Le type de compte cloud que vous souhaitez ajouter. Les valeurs disponibles sont : • Amazon • Openstack • Rackspace • Windowsazure • « Windows Azure » • Azure
-username	Le nom d'utilisateur du compte cloud que vous souhaitez ajouter. Il est utilisé dans le processus d'authentification. Cette propriété devient « Clé d'accès » pour Amazon™ cloud, « Nom d'utilisateur » pour Rackspace et OpenStack, et « Nom de compte de stockage » pour les comptes cloud de Windows Azure.
-key	La clé du compte cloud que vous souhaitez ajouter. Elle est utilisée dans le processus d'authentification. Cette propriété devient « Clé secrète » pour Amazon™ cloud, « Clé Api » pour Rackspace et OpenStack, et « Clé d'accès » pour les comptes cloud Windows Azure.
-region	La région du compte cloud que vous souhaitez ajouter. Cette propriété est nécessaire uniquement pour les comptes cloud RackSpace et OpenStack.
-tenantid	L'identificateur qui est utilisé dans le processus d'authentification d'un compte cloud OpenStack. Cette option est requise uniquement pour les comptes cloud OpenStack.
-authurl	L'URL qui est utilisée dans le processus d'authentification d'un compte cloud OpenStack. Cette option est requise uniquement pour les comptes cloud OpenStack.

Exemple :

Créez un nouveau compte cloud Amazon™ S3 nommé « Compte Amazon S3 » avec la clé d'accès « UNEclé » et la clé secrète « Sclé ».

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

La commande `New-EncryptionKey` vous permet de créer une nouvelle clé de chiffrement vous permettant de sécuriser vos données sauvegardées Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key  
name] -passphrase [pas  
sphrase] -comment [comment]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-EncryptionKey` :

Tableau 254. Options de la commande New-EncryptionKey

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-name	Le nom de la clé de chiffrement que vous souhaitez créer.
-passphrase	La phrase secrète de la clé de chiffrement que vous souhaitez créer.
-comment	Facultatif. La description de la clé de chiffrement.

Exemple :

Créez une clé de chiffrement sur le Core local :

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

La commande PowerShell `New-EsxiVirtualStandby` vous permet de créer une nouvelle machine avec disque de secours virtuel ESXi avec Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
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
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-EsxiVirtualStandby` :

Tableau 255. Options de la commande New-EsxiVirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-volumes	Facultatif. Listez les noms des volumes que vous souhaitez exporter. Si aucun n'est spécifié, tous les volumes des points de restauration seront exportés. Les valeurs doivent être entre guillemets doubles (") et séparées par un espace, par exemple : "c:", "d:".  REMARQUE : Ne pas utiliser de slashes dans les noms des volumes.
-vmname	Le nom de la machine virtuelle selon Microsoft Windows.
-hostname	Le nom d'utilisateur pour l'hôte du serveur virtuel.
-hostport	Le numéro de port à utiliser pour communiquer avec le serveur virtuel.
-hostusername	Nom d'utilisateur pour se connecter à l'hôte du serveur virtuel.

Option	Description
-hostpassword	Mot de passe pour se connecter à l'hôte du serveur virtuel.
-ram	Affecte une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-diskprovisioning	Facultatif. La quantité d'espace disque à affecter sur la machine virtuelle. Les valeurs disponibles sont : • Complet : pour rendre le disque virtuel aussi grand que le disque d'origine sur le serveur protégé. • Léger : pour allouer la quantité d'espace disque effective occupée sur le disque d'origine, plus quelques mégaoctets supplémentaires. Le provisionnement des disques par défaut est « Léger ».
-diskmapping	Facultatif. Détermine la manière d'adresser les disques du point de restauration vers la machine virtuelle. Les valeurs disponibles sont : • 'Auto' • 'Manuel' • 'Avec VM' Le paramètre par défaut est 'Auto'.
-initialexport	Facultatif. Spécifiez cette option si vous avez besoin de démarrer un export initial de machine virtuelle à la demande initiale après avoir configuré le Disque de secours virtuel.

Exemple :

Créez une nouvelle machine avec disque de secours virtuel ESXi :

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname 10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

La commande `New-HyperVVirtualStandby` PowerShell vous permet de créer une nouvelle machine virtuelle Hyper-V (VM) avec Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
    | -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
    hostpassword [virtual host password] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-HyperVVirtualStandby` :

Tableau 256. Options de la commande `New-HyperVVirtualStandby`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-volumes	Facultatif. Listez les noms des volumes que vous souhaitez exporter. Si aucun n'est spécifié, tous les volumes des points de restauration seront exportés. Les valeurs doivent être entre guillemets doubles (") et séparées par un espace, par exemple : "c:", "d:".
❗ REMARQUE : Ne pas utiliser de slashes dans les noms des volumes.	
-vmname	Le nom de la machine virtuelle selon Microsoft Windows.
-gen2	Facultatif. Spécifiez bien l'utilisation de la seconde génération de machine virtuelle. Si rien n'est spécifié, la première génération sera utilisée. Rapid Recovery est compatible avec la 2e génération de Windows Server 2012 R2 sous Windows 8.1 .
-usevhdx	Facultatif. Si vous spécifiez cette option, Rapid Recovery utilise le format de disque VHDX pour créer la VM. Si vous ne le spécifiez pas, il utilise le format de disque virtuel (VHD) . La 2e génération utilise uniquement le format VHDX.
-uselocalmachine	Facultatif. Se connecter au serveur Hyper-V local. Lorsque vous spécifiez cette valeur, Rapid Recovery ignore les options suivantes : • Nom d'hôte • hostport • hostusername • hostpassword
-hostname	Le nom d'utilisateur pour l'hôte du serveur virtuel.
-hostport	Le numéro de port à utiliser pour communiquer avec le serveur virtuel.
-hostusername	Nom d'utilisateur pour se connecter à l'hôte du serveur virtuel.
-hostpassword	Mot de passe pour se connecter à l'hôte du serveur virtuel.

Option	Description
-vmlocation	Chemin d'accès local ou réseau au dossier dans lequel vous souhaitez stocker les fichiers de la machine virtuelle.
-ram	Affecte une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-initialexport	Facultatif. Spécifiez cette option si vous avez besoin de démarrer un export initial de machine virtuelle à la demande initiale après avoir configuré le Disque de secours virtuel.

Exemple :

Créez une nouvelle machine avec disque de secours virtuel Hyper-V :

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver [name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] -rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

La commande `New-Mount` monte l'instantané d'un ou plusieurs volumes.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-Mount` :

Tableau 257. Options de la commande New-Mount

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-protectedserver	L'adresse IP du serveur protégé ou le nom de la machine (en fonction de la manière dont la machine particulière a été protégée).
-time	Facultatif. L'horodatage du point de restauration à monter. Devra être au format qui est défini par l'OS du PC actif. L'administrateur est capable de recevoir le dernier point de restauration en spécifiant le dernier point de restauration ou le dernier vérifié par la valeur transmise du paramètre. Par défaut, l'option de l'heure la plus récente est choisie.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-path	Chemin sur la machine Core vers laquelle les points de restauration seront montés.
-mounttype	Facultatif. Spécifie un mode de montage. Les options possibles sont : 'read' (lecture seule), 'readOnlyWithPreviousWrites' (lecture seule avec écritures précédentes), 'write' (accessible en écriture). Le mode par défaut est read-only (lecture seule).
-volumes	Facultatif. Liste des noms de volumes à monter séparés par des espaces. Si le nom du volume contient des espaces ou des caractères spéciaux, ils doivent être spécifiés en utilisant des guillemets. Si rien n'est spécifié, tous les volumes seront montés.
-drivers	Facultatif. Liste des noms de volumes à monter séparés par des virgules. Si rien n'est spécifié, tous les volumes seront montés. REMARQUE : Cette option est obsolète, utilisez plutôt ' -volumes '.
-rpn	Facultatif. Numéro attribué au point de restauration pour le montage. Vous pouvez l'obtenir en utilisant la commande <code>get-mounts</code> . Spécifiez plusieurs numéros pour le paramètre <code>rpn</code> afin de monter différents points à partir d'une seule commande. REMARQUE : Si vous définissez un tableau de points à monter, chaque point sera situé dans un répertoire enfant distinct. Le nom indique le moment où le point de restauration a été créé. Lorsque vous appelez la fonction démontage, tous les répertoires enfants seront retirés. Vous devez retirer le répertoire parent manuellement.

Exemple :

```
>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"
```

Monter un tableau de points de restauration :

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path "D:/Folder for mount"
```

Monter un point de restauration avec l'heure réelle de création :

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012 11:46 AM"
```

Resume-Replication

La commande `New-Replication` vous permet de configurer et de forcer la réplication d'un ou plusieurs serveurs protégés.

Utilisation

L'utilisation de la commande est la suivante :

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-Replication` :

Tableau 258. Options de la commande New-Replication

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-replicationname	Nom de la configuration de réplication sur le Core cible.
-targetserver	Le nom d'hôte, le nom d'utilisateur et mot de passe du Core cible.
-protectedserver	Le nom de la machine protégée et de la logithèque du Core cible pour configurer la réplication.

Exemple :

Créez une nouvelle réplication pour la machine protégée portant l'adresse IP 10.10.10.4 :

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

La commande `New-Repository` permet de créer une nouvelle logithèque DVM dans le Core Rapid Recovery. La taille spécifiée doit être comprise entre 250 Mo et 16 To.

Utilisation

L'utilisation de la commande est la suivante :

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-Repository` :

Tableau 259. Options de la commande New-Repository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-name	Nom de la logithèque.
-size	Taille de l'étendue de la logithèque. Les unités disponibles sont : o, Ko, Mo, Go, To et Po.
-datapath	Pour l'emplacement local uniquement. Détermine le chemin des données de l'étendue de la logithèque.
-metadatapath	Pour l'emplacement local uniquement. Détermine le chemin des métadonnées de l'étendue de la logithèque.
-uncpath	Pour l'emplacement partagé uniquement. Détermine les chemins des données et des métadonnées de l'étendue de la logithèque.
-shareusername	Pour l'emplacement partagé uniquement. Détermine l'identifiant de connexion à l'emplacement partagé.
-sharepassword	Pour l'emplacement partagé uniquement. Détermine le mot de passe de connexion à l'emplacement partagé.
-comment	Facultatif. Description de la logithèque.
-concurrent Operations	Facultatif. Le nombre maximal d'opérations qui peuvent être en attente à un moment donné. Valeur par défaut : 64.

Exemple :

Créez une nouvelle logithèque DVM d'une taille minimale sur le disque local E :

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:\Repository\Metadata
```

New-ScheduledArchive

La commande `New-ScheduledArchive` vous permet d'utiliser PowerShell pour apporter des modifications à un archivage programmé existant.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-ScheduledArchive` :

Tableau 260. Options de la commande New-ScheduledArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	La machine protégée ayant des points de restauration que vous souhaitez archiver. Vous pouvez spécifier plusieurs noms de machine entourés de guillemets doubles (") et séparés par des virgules.
-all	Points de restauration d'archive de toutes les machines protégées.
-path	Le chemin de l'emplacement pour enregistrer les données archivées. Par exemple : - Machine locale : « d: \work\archive » - Chemin d'accès au réseau : « \\servername\sharename » - Dossier dans un compte cloud : « nom du dossier »  REMARQUE : Le nombre de symboles ne doit pas être supérieur à 100 pour les emplacements locaux et réseaux, et ne doit pas être supérieur à 150 pour un emplacement cloud.
-archiveusername	Facultatif. Nom d'utilisateur pour se connecter à la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-archivepassword	Facultatif. Mot de passe pour se connecter à la machine distante. Obligatoire uniquement pour les chemins d'accès réseau.
-cloudaccountname	Facultatif. Utilisez uniquement pour l'archivage cloud. Le nom du compte cloud où vous souhaitez enregistrer l'archive.

Option	Description
-cloudcontainer	Facultatif. Utilisez uniquement pour l'archivage cloud. Le Nom du conteneur cloud dans le compte cloud choisi, où l'archive sera enregistrée. Lorsque vous utilisez cette option, vous devez également spécifier le paramètre « -cloudaccountname ».
-recycleaction	Le type d'action de recyclage. Spécifié avec une des quatre valeurs suivantes : « replacethiscore » - Remplace les données archivées existantes du Core, mais laisse intactes les données des autres Cores. « erasecompletely » - Efface toutes les données archivées dans le répertoire avant d'écrire une nouvelle archive. « incremental » - Permet d'ajouter des points de restauration à une archive existante. La fonction compare les points de restauration pour éviter de dupliquer les données qui existent déjà dans l'archive.
-scheduletype	Type d'intervalle de planification. Option spécifiée avec une des quatre valeurs suivantes : « daily » - Pour les archives quotidiennes créées automatiquement. « weekly » - Pour les archives hebdomadaires créées automatiquement. Vous devez spécifier le paramètre « -dayofweek ». « monthly » - Pour les archives mensuelles créées automatiquement. Vous devez spécifier le paramètre « -dayofmonth ». Si un mois n'a pas le jour précisé (par exemple : 31) l'archivage n'aura pas lieu ce mois. « lastdayofmonth » - Pour créer automatiquement une archive le dernier jour de chaque mois.
-dayofweek	Utilisez uniquement pour l'option « weekly » du paramètre « -scheduletype ». Le jour de la semaine pour créer automatiquement l'archive (par exemple, « lundi »).
-dayofmonth	Utilisez uniquement pour l'option « monthly » du paramètre « -scheduletype ». Le jour (numéro) du mois pour créer automatiquement l'archive (par exemple, « 15 »).
-time	L'heure pour créer une archive quotidienne.
-initialpause	Facultatif. Spécifiez cette option si vous souhaitez suspendre l'archivage après avoir configuré la planification.

Exemples :

Archivez tous les points de restauration créés à partir du 30/04/2012 à 14 h 55 pour toutes les machines sur le Core et remplacez les données archivées pré-existantes appartenant à ce 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
```

Archivez les points de restauration qui se situent dans une plage de dates pour deux machines protégées et effacez toutes les données archivées de la logthèque avant d'écrire la nouvelle 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
```

Créez une archive incrémentielle de tous les points de restauration créés à partir du 30/04/2012 à 14 h 55 pour toutes les machines sur le Core du compte cloud nommé « Amazon S3 » et un conteneur appelé « conteneur » :

```
>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

La commande `New-Snapshot` force un instantané entraînant un transfert de données pour la machine protégée active. Lorsque vous forcez un instantané, le transfert démarre immédiatement ou sera ajouté à la file d'attente. Seules les données qui ont changé depuis un point de restauration précédent seront transférées. S'il n'existe aucun point de restauration précédent, toutes les données des volumes protégés seront transférées.

Utilisation

L'utilisation de la commande est la suivante :

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-Snapshot` :

Tableau 261. Options de la commande New-Snapshot

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Forcer toutes les machines protégées.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Forcer pour le nom de la machine protégée active.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Forcer un instantané pour toutes les machines protégées.

```
>New-Snapshot -all
```

New-VBVirtualStandby

La commande `New-VBVirtualStandby` vous permet d'utiliser PowerShell pour créer une nouvelle exportation virtuelle pour une machine virtuelle VirtualBox(VM).

Utilisation

L'utilisation de la commande est la suivante :

```
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
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-VBVirtualStandby` :

Tableau 262. Options de la commande `New-VBVirtualStandby`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-volumes	Facultatif. Listez les noms des volumes que vous souhaitez exporter. Si aucun n'est spécifié, tous les volumes des points de restauration seront exportés. Les valeurs doivent être entre guillemets doubles (") et séparées par un espace, par exemple : "c:", "d:". REMARQUE : Ne pas utiliser de slashes dans les noms des volumes.
-vmname	Le nom de la machine virtuelle selon Microsoft Windows.
-ram	Affecte une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-linuxhostname	Le nom du serveur hôte VirtualBox Linux.
-hostport	Le port du serveur VirtualBox Linux.
-targetpath	Le chemin local, réseau ou Linux vers le dossier dans lequel vous souhaitez stocker les fichiers de la machine virtuelle.
-pathusername	Nom d'utilisateur pour la connexion à la machine réseau. Uniquement requis lorsque vous spécifiez un emplacement réseau pour le chemin cible.

Option	Description
<code>-pathpassword</code>	Le mot de passe de connexion pour la machine réseau. Uniquement requis lorsque vous spécifiez un emplacement réseau pour le chemin cible.
<code>-accountusername</code>	Facultatif. Vous pouvez spécifier un compte utilisateur pour enregistrer la machine virtuelle exportée. C'est le nom d'utilisateur pour la connexion au compte utilisateur. Utilisez cette option pour une machine locale ou en réseau uniquement.
<code>-accountpassword</code>	Facultatif. Vous pouvez spécifier un compte utilisateur pour enregistrer la machine virtuelle exportée. Il s'agit du mot de passe pour se connecter au compte utilisateur. Utilisez cette option pour une machine locale ou en réseau uniquement.
<code>-initialexport</code>	Facultatif. Spécifiez cette option si vous avez besoin de démarrer un export initial de machine virtuelle à la demande initiale après avoir configuré le Disque de secours virtuel.

Exemple :

Créez une machine avec disques de secours virtuels VirtualBox nommée MachineExportée1 à l'emplacement spécifié :

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

La commande PowerShell `New-VMVirtualStandby` vous permet de créer une nouvelle VMware Workstation avec Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
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
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `New-VMVirtualStandby` :

Tableau 263. Options de la commande New-VMVirtualStandby

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Affiche les tâches d'une machine protégée spécifique, indiquée par son adresse IP.
-volumes	Facultatif. Listez les noms des volumes que vous souhaitez exporter. Si aucun n'est spécifié, tous les volumes des points de restauration seront exportés. Les valeurs doivent être entre guillemets doubles (") et séparées par un espace, par exemple : "c:", "d:". REMARQUE : Ne pas utiliser de slashes dans les noms des volumes.
-vmname	Le nom de la machine virtuelle selon Microsoft Windows.
-ram	Affecte une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-pathusername	Nom d'utilisateur pour la connexion à la machine réseau. Uniquement requis lorsque vous spécifiez un emplacement réseau pour le chemin cible.
-pathpassword	Le mot de passe de connexion pour la machine réseau. Uniquement requis lorsque vous spécifiez un emplacement réseau pour le chemin cible.
-initialexport	Facultatif. Spécifiez cette option si vous avez besoin de démarrer un export initial de machine virtuelle à la demande initiale après avoir configuré le Disque de secours virtuel.

Exemple :

Créez un nouveau disque de secours virtuel VMware Workstation :

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

Le script se met en pause et l'utilisateur doit spécifier un numéro d'index pour le poste de travail approprié. Entrez le numéro d'index du script pour terminer (dans ce cas, 2). L'exemple continue :

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

La commande `Push-Replication` force la réplication pour une ou plusieurs machines protégées.

Utilisation

L'utilisation de la commande est la suivante :

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host
name] -all | -protectedserver [machine name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Push-Replication` :

Tableau 264. Options de la commande Push-Replication

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Forcer la réplication pour toutes les machines en cours de réplication sur le core cible.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Nom de la machine protégée sur le core cible qui doit être utilisé pour forcer la réplication.
-user	Facultatif. Identifiant de connexion pour la machine hôte du core distant. Si vous spécifiez un identifiant de connexion, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Force la réplication pour une seule machine protégée :

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd  
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

Force la réplication pour toutes les machines protégées :

```
>Push-Replication -all
```

Push-Rollup

La commande `Push-Rollup` force la consolidation pour une machine protégée.

Utilisation

L'utilisation de la commande est la suivante :

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine  
name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Push-Rollup` :

Tableau 265. Options de la commande Push-Rollup

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Forcer toutes les machines protégées.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Forcer pour le nom de la machine protégée active.
-user	Facultatif. Identifiant de connexion pour la machine hôte du core distant. Si vous spécifiez un identifiant de connexion, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Forcer la consolidation pour une seule machine protégée :

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

Forcer la consolidation pour toutes les machines protégées :

```
>Push-Rollup -all
```

Remove-Agent

La commande PowerShellRemove-Agent vous permet de retirer une machine de la protection de Core Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeRemove-MountAgent :

Tableau 266. Options de la commande Remove-Agent

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Démonter tous les points de restauration montés pour la machine protégée active.
-deleterecoverypoints	Facultatif. Supprime tous les points de restauration de cette machine protégée.
-all	Facultatif. Supprime toutes les machines protégées du Core.

Exemple :

Démontez toutes les machines protégées et leurs points de récupération :

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$$sdd -deleterecoverypoints -all
```

Remove-Mount

La commande `Remove-Mount` démonte un point de restauration spécifié selon le `/Path`. Démonte les points de la machine sélectionnée en utilisant le paramètre `-protectedserver` ou démonte tous les points de restaurations montés en utilisant le paramètre `-all`.

Utilisation

L'utilisation de la commande est la suivante :

```
Remove-Mount -core [host name] -user [user name] -password [password] [-protectedserver [machine name] | -path [mount path]]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Remove-Mount` :

Tableau 267. Options de la commande Remove-Mount

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Démonte tous les points de restauration montés.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-path	Démonter le point de montage sélectionné.
-protectedserver	Démonter tous les points de restauration montés pour la machine protégée active.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Démonter le point de restauration spécifié par son chemin :

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -path C:\mountedRecoveryPoint
```

Remove-Mounts

La commande `Remove-Mounts` démonte tous les points de restauration montés.

Utilisation

L'utilisation de la commande est la suivante :

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Remove-Mounts` :

Tableau 268. Options de la commande Remove-Mounts

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Exemple :

Démonter tous les points de restauration sur le core spécifié :

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd
```

Remove-RecoveryPoints

La commande `PowerShellRemove-RecoveryPoints` permet de supprimer les points de restauration d'une machine spécifique.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Remove-RecoveryPoints` :

Tableau 269. Options de la commande Remove-RecoveryPoints

Option	Description
<code>-?</code>	Affiche de l'aide sur la commande.
<code>-core</code>	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
<code>-user</code>	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-password</code>	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
<code>-protectedserver</code>	Démonter tous les points de restauration montés pour la machine protégée active.

Option	Description
-rpn	Facultatif. Uniquement pour la suppression de chaîne (image de base avec chaîne de points incrémentiels ou orphelins). Numéro d'un point de restauration à supprimer (utiliser la commande Get-RecoveryPoints pour obtenir les numéros). Vous pouvez spécifier plusieurs numéros séparés par des espaces pour supprimer plusieurs points de restauration à l'aide d'une seule commande.
-time	Cette option permet de supprimer une chaîne de points de restauration. Facultatif. Pour supprimer un seul point de restauration, sélectionnez-le en fonction de son heure de création. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre ordinateur. Obligatoire. Pour établir une plage de dates, spécifiez un intervalle de temps à l'aide de deux chaînes de temps séparées par une virgule et un espace pour sélectionner la plage de points de restauration à supprimer.
-range	Facultatif. Plage de points de restauration à supprimer en fonction d'un intervalle de temps.
-chain	Facultatif. Image de base incluant un ensemble incrémentiel ou séquentiel de points de restauration orphelins à supprimer en les sélectionnant en fonction de leur numéro ou du moment de leur création.
-all	Facultatif. Supprimer toutes les machines protégées du Core.

Exemple :

Supprimer le point de restauration spécifié en fonction de sa date :

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -time "2/24/2012 09:00 AM"
```

Remove-Repository

La commande PowerShell `Remove-Repository` supprime une logithèque Rapid Recovery ainsi que son contenu sur le Core.

Utilisation

L'utilisation de la commande est la suivante :

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

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Remove-Repository` :

Tableau 270. Options de la commande Remove-Repository

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-name	Le nom de la logithèque que vous souhaitez retirer.
-all	Retirer toutes les logithèques associées à ce Core.

Exemple :

Retirer les logithèques présentes sur le Core local :

```
>Remove-repository -all
```

Remove-ScheduledArchive

Si vous avez programmé Rapid Recovery pour que celui-ci archive régulièrement les points de restauration d'une machine particulière, vous pouvez utiliser la commande `PowerShellRemove-ScheduledArchive` pour supprimer cette archive planifiée depuis le Core.

Utilisation

L'utilisation de la commande est la suivante :

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Remove-ScheduledArchive` :

Tableau 271. Options de la commande Remove-ScheduledArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion.

Option	Description
	Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Supprimez toutes les archives associées à ce Core.
-id	L'identificateur de l'archive que vous souhaitez supprimer. Pour répertoire plus d'une archive, séparez chaque identifiant par un espace.

Exemple :

Supprimez plusieurs archives planifiées du Core local :

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Remove-VirtualStandby

Si vous avez programmé Rapid Recovery pour que celui-ci exporte des données de manière continue vers une machine virtuelle, vous pouvez ensuite utiliser la commande PowerShellRemove-VirtualStandby pour annuler et supprimer cette tâche planifiée.

Utilisation

L'utilisation de la commande est la suivante :

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP ad  
dress]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeRemove-VirtualStandby :

Tableau 272. Options de la commande Remove-VirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Retirez tous les tâches de disques de secours virtuels associées à ce Core.

Option	Description
- protectedserver	Le nom ou l'adresse IP de la machine protégée pour laquelle vous souhaitez supprimer le disque de secours virtuel.

Exemple :

Retirez toutes les tâches de disques de secours virtuels associées à ce Core :

```
>Remove-VirtualStandby -all
```

Resume-Replication

La commande `Resume-Replication` vous permet de reprendre la réplication. Voir [Suspend-Replication](#) pour plus d'informations.

Utilisation

L'utilisation de la commande est la suivante :

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -  
protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Resume-Replication` :

Tableau 273. Options de la commande Resume-Replication

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Tous les serveurs protégés.
- protectedserver	Reprendre la réplication pour la machine spécifiée.
-incoming	Nom d'hôte du core distant qui réplique sur la machine Core. La réplication est reprise pour toutes les machines protégées sur le core distant.
-outgoing	Nom d'hôte du core cible distant sur lequel les données sont répliquées. La réplication est reprise pour toutes les machines protégées sur le core distant.

Exemple :

Reprenez la réplication pour la machine protégée avec l'IP 10.10.10.128 pour le Core local, en spécifiant la logithèque utilisé :

```
>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:
```

Le script se met en pause, l'utilisateur doit alors spécifier un numéro d'index pour la logithèque concerné. Entrez le numéro d'index du script pour terminer (dans ce cas, 2). L'exemple continue ;

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

Un administrateur peut reprendre les instantanés, exporter vers des machines virtuelles ou effectuer une réplication. Voir [Start-VMExport](#) pour plus d'informations.

Utilisation

L'utilisation de la commande est la suivante :

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Resume-Snapshot` :

Tableau 274. Options de la commande Resume-Snapshot

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-all	Tous les serveurs protégés.
-protectedserver	Reprendre l'instantané pour la machine spécifiée.

Exemple :

Reprendre les instantanés pour la machine protégée avec l'IP 10.10.10.4 pour le Core local :

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

La commande PowerShell `Resume-VirtualStandby` vous permet de reprendre l'exportation interrompue des données vers un disque de secours virtuel Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Resume-VirtualStandby` :

Tableau 275. Options de la commande Resume-VirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Permet de reprendre toutes les exportations des disques de secours virtuels.
-protectedserver	Le ou les noms (séparés par une virgule et des espaces) des machines protégées comportant les disques de secours virtuels que vous voulez reprendre.

Exemple :

Reprenez les exportations du disque de secours virtuel d'une machine protégée :

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

Resume-VMExport

La commande `Resume-VMExport` permet à l'administrateur d'exporter vers des machines virtuelles. Voir [Suspend-VMExport](#) pour plus d'informations.

Utilisation

L'utilisation de la commande est la suivante :

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Resume-VMExport` :

Tableau 276. Options de la commande Resume-VMExport

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Tous les serveurs protégés.
-protectedserver	Reprendre l'instantané pour la machine spécifiée.

Exemple :

Reprendre l'exportation vers une machine virtuelle pour chacune des machines protégées sur le core local :

```
>Resume-VMExport -all
```

Start-Archive

Les entreprises utilisent souvent un stockage à long terme pour l'archivage des données conformes et non conformes. La fonction d'archivage dans Rapid Recovery est utilisée pour prendre en charge la rétention prolongée des données conformes et de non-conformes. L'administrateur peut sauvegarder et archiver sur le stockage local ou à un emplacement réseau en spécifiant la commande/Path et les identifiants.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core [host name] -user [user name] -password [password]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Start-Archive` :

Tableau 277. Options de la commande Start-Archive

Option	Description
-?	Affiche de l'aide sur la commande.
-path	Chemin d'accès de l'emplacement. Exemple de chemin : « D:\work\archive » ou le chemin réseau : « \servername\sharename ».
-all	Archiver tous les points de restauration pour toutes les machines sur le Core :
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-startdate	Date de début de la plage de dates pour les points de restauration créés. Devra être au format spécifié par l'OS du PC actif.
-enddate	Date de fin de la plage de dates. L'heure en cours est la valeur par défaut.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Archiver les points de restauration d'une machine spécifiée.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-archiveusername	Facultatif. Obligatoire uniquement pour les chemins d'accès réseau.
-archivepassword	Facultatif. Obligatoire uniquement pour les chemins d'accès réseau.
-comment	Facultatif. Exemple : <code>-comment 'Before install new application'</code> .

Exemple :

Archiver tous les points de restauration pour toutes les machines sur le Core :

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

La commande `Start-AttachabilityCheck` force une vérification de la capacité d'attachement pour toutes les bases de données des serveurs SQL protégées par le Core.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]  
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Start-AttachabilityCheck` :

Tableau 278. Options de la commande Start-AttachabilityCheck

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	La machine protégée à utiliser pour effectuer la vérification de la capacité d'attachement SQL.
-rpn	Facultatif. Le numéro d'un point de restauration à utiliser pour effectuer la vérification de la capacité d'attachement SQL. Vous pouvez utiliser la commande <code>-GetRecoveryPoints</code> pour obtenir les numéros des points de restauration. Spécifiez plusieurs numéros séparés par des espaces pour effectuer les vérifications sur plusieurs points de restauration à l'aide d'une seule commande.

 **REMARQUE :** Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est utilisé pour la vérification de la capacité d'attachement.

Option	Description
-time	Facultatif. Détermine le point de récupération à sélectionner pour la vérification de la capacité d'attachement. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA » (par exemple : « 24/04/2015 9 h 00 »). Spécifiez la date et l'heure correspondant au fuseau horaire défini sur la machine locale.
 REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.	

Exemple :

Effectuer une vérification de la capacité d'attachement SQL sur le point de restauration le plus récent pour le serveur SQL protégé spécifié :

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-ChecksumCheck

La commande PowerShellStart-ChecksumCheck vous permet de forcer une vérification de la somme de contrôle des points de restauration du serveur Exchange.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name  
| IP address] -rpn [number | numbers] | -time [time string]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeStart-ChecksumCheck :

Tableau 279. Options de la commande Start-ChecksumCheck

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Nom de la machine protégée.

Option	Description
-rpn	Facultatif. Uniquement pour la suppression de chaîne (image de base avec une chaîne de points incrémentiels ou orphelins). Le numéro d'un point de restauration à vérifier (utilisez la commande Get-RecoveryPoints pour obtenir les numéros). Vous pouvez spécifier plusieurs numéros séparés par des espaces pour supprimer plusieurs points de restauration à l'aide d'une seule commande.
-time	Facultatif. Sélectionnez le point de restauration à vérifier en utilisant son heure de création, au lieu de son numéro. Vous devez spécifier le moment exact au format "mm/jj/aaaa hh:mm tt" (par exemple, "2/24/2012 09:00 AM"). Pensez à bien spécifier la date et l'heure correspondant au fuseau horaire défini sur votre ordinateur.

Exemple :

Démarrez une vérification de somme de contrôle sur deux points de restauration :

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

La commande PowerShellStart-EsxiExport démarre le lancement d'une exportation virtuelle à partir du point de restauration Rapid Recovery sélectionné vers une machine virtuelle ESX(i).

Les paramètres obligatoires sont le nom de la machine protégée contenant les points de récupération à exporter, le nom de la machine virtuelle vers laquelle l'exportation se fait, la quantité de RAM à allouer sur la machine virtuelle, le nom d'hôte et le port du serveur hôte Linux, ainsi que le chemin vers le dossier local, réseau ou Linux où seront stockés les fichiers résultants de la machine virtuelle.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeStart-EsxiExport :

Tableau 280. Options de la commande Start-EsxiExport

Option	Description
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Machine protégée avec des points de restauration à exporter.
-volumes	Facultatif. Liste des noms de volumes à exporter. Si rien n'est spécifié, tous les volumes des points de restauration spécifiés seront exportés. Les valeurs doivent être entre guillemets, chacune séparée par un espace. N'utilisez pas de slashes dans les noms des volumes. Par exemple, spécifiez "C:" et non "C:/"
-rpn	Facultatif. Le numéro du point de restauration à exporter. Vous pouvez utiliser la commande <code>Get-RecoveryPoints</code> pour obtenir les numéros des points de restauration.
	REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le point de restauration à sélectionner pour l'exportation. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA » (par exemple : « 24/04/2015 9 h 00 »). Spécifiez la date et l'heure correspondant au fuseau horaire défini sur la machine locale.
	REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-vmname	Nom Windows de la machine virtuelle.
-hostname	Nom d'hôte du serveur virtuel.
-hostport	Numéro de port du serveur virtuel.
-hostusername	Nom d'utilisateur pour l'hôte du serveur virtuel.
-hostpassword	Mot de passe de connexion à l'hôte du serveur virtuel.
-ram	Alloue une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-diskprovisioning	Facultatif. La quantité d'espace disque à allouer sur la machine virtuelle. Spécifiez 'thick' pour rendre le disque virtuel aussi grand que le disque d'origine sur le serveur protégé, ou 'thin' pour allouer la quantité d'espace disque effective occupée sur le disque d'origine, plus quelques mégaoctets supplémentaires. Par défaut, c'est l'option 'thin' qui est sélectionnée.
-diskmapping	Facultatif. Choisissez entre 'auto,' 'manual,' ou 'withvm'. Par défaut, c'est le mappage automatique qui est activé.
-resetup	Facultatif. Recrée la machine virtuelle si elle est déjà présente sur l'emplacement spécifié.
-datacenter	Facultatif. Spécifie le datacenter à utiliser.
-resourcepool	Facultatif. Spécifie le pool de ressources à utiliser.
-datastore	Facultatif. Spécifie le magasin de données à utiliser.
-computeresource	Facultatif. Spécifie les ressources informatiques à utiliser.
-version	Facultatif. Spécifie la version de ESXi à utiliser.

Start-HypervExport

La commande PowerShellStart-HypervExport démarre le lancement d'une exportation virtuelle à partir du point de restauration Rapid Recovery sélectionné vers une machine virtuelle serveur Hyper-V.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commandeStart-HypervExport :

Tableau 281. Options de la commande Start-HypervExport

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Machine protégée avec des points de restauration à exporter.
-volumes	Facultatif. Liste des noms de volumes à exporter. Si rien n'est spécifié, tous les volumes des points de restauration spécifiés seront exportés. Les valeurs doivent être saisies entre guillemets doubles et séparées par un espace. Ne pas utiliser de slashes dans les noms des volumes. Par exemple, spécifiez "C:" et non "C:/"
-rpn	Facultatif. Le numéro du point de restauration à exporter. (Vous pouvez utiliser la commandeGet-RecoveryPoints pour obtenir les numéros des points de restauration.)  REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le point de restauration à sélectionner pour l'exportation. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA hh:mm tt » (par exemple : « 04/24/2015 09:00 AM »). Spécifiez les valeurs de temps du fuseau horaire défini sur votre machine locale.  REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.

Option	Description
-vmname	Nom Windows de la machine virtuelle.
-gen2	Facultatif. À spécifier pour utiliser la deuxième génération de machine virtuelle. À défaut, la génération 1 est utilisée. Rapid Recovery prend en charge la génération 2, de Windows Server 2012 R2 à Windows 8.1.
-usevhdx	Facultatif. Si vous spécifiez cette option, Rapid Recovery utilise le format de disque VHDX pour créer la machine virtuelle. Sinon, le format de disque VHD est utilisé. La génération 2 utilise uniquement le format VHDX.
-uselocalmachine	Facultatif. Se connecter au serveur Hyper-V local. Si ce paramètre est utilisé, les options suivantes sont ignorées : nom d'hôte, port de l'hôte, nom d'utilisateur de l'hôte, mot de passe de l'hôte.
-hostname	Nom d'hôte du serveur virtuel.
-hostport	Numéro de port du serveur virtuel.
-hostusername	Nom d'utilisateur pour l'hôte du serveur virtuel.
-hostpassword	Mot de passe de connexion à l'hôte du serveur virtuel.
-vmlocation	Chemin local ou réseau jusqu'au dossier dans lequel vous souhaitez stocker les fichiers de la machine virtuelle.
-ram	Alloue une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.

Start-LogTruncation

La commande `Start-LogTruncation` force la troncature de journal pour le serveur SQL protégé spécifié ou le serveur Microsoft Exchange spécifié.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -target [sql | exchange]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Start-LogTruncation` :

Tableau 282. Options de la commande Start-LogTruncation

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Archiver les points de restauration d'une machine spécifiée.
-target	Spécifier le type de troncature de journal (soit 'sql', soit 'exchange'). Si cette option n'est pas spécifiée, la troncature des journaux se fait pour toutes les bases de données.

Exemple :

Tronquer les journaux SQL :

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Tronquer les journaux du serveur Exchange : tous les points de restauration pour toutes les machines du core :

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

La commande `Start-MountabilityCheck` force la vérification de la montabilité pour les magasins d'e-mails Microsoft Exchange protégés.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -protectedserver [[machine name] or [IP address]] -rpn [number | numbers] | -time [time string]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Start-MountabilityCheck` :

Tableau 283. Options de la commande Start-MountabilityCheck

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Archiver les points de restauration d'une machine spécifiée.
-rpn	Facultatif. Le numéro du point de restauration à exporter. (Vous pouvez utiliser la commande-GetRecoveryPoints pour obtenir les numéros des points de restauration.) <i>i</i> REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le point de restauration à sélectionner pour l'exportation. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA » (par exemple : « 24/04/2015 à 9 h 00 »). Spécifiez la date et l'heure correspondant au fuseau horaire défini sur la machine locale. <i>i</i> REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.

Exemple :

Démarrer une vérification de la montabilité pour tous les points de restauration pour toutes les machines du core :

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

La commandeStart-Protect permet à l'administrateur d'ajouter un serveur sous la protection d'un Core.

Utilisation

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeStart-Protect :

Tableau 284. Options de la commande Start-Protect

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-repository	Le nom d'une logithèque sur le Core où les données de la machine protégée sont stockées.
-agentname	Nom de la machine protégée ou adresse IP.
-agentusername	Se connecter au serveur pour être protégé.
-agentpassword	Mot de passe du serveur afin d'être protégé.
-agentport	Numéro de port du serveur protégé.
-volumes	Liste des volumes à protéger. Les valeurs doivent être entre guillemets et séparées par un espace. Ne pas utiliser de slashes dans les noms des volumes. Par exemple : « c: » ou « d: ».

Exemple :

Mettre les volumes d'un serveur sous protection :

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

La commande Start-ProtectCluster permet à l'administrateur d'ajouter un cluster de serveurs sous la protection d'un Core.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande Start-ProtectCluster :

Tableau 285. Options de la commande Start-ProtectCluster

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-repository	Le nom d'une logithèque sur le Core où les données de la machine protégée sont stockées. Le nom doit être entouré de guillemets doubles ("").
-clustername	Nom du cluster à protéger.
-clusterusername	Nom d'utilisateur du cluster à protéger.
-clusterpassword	Mot de passe du cluster à protéger.
-clusterport	Numéro de port du cluster à protéger.
-clustervolumes	Liste des volumes à protéger. Les valeurs doivent être entre guillemets et séparées par un espace. Ne pas utiliser de slashes dans les noms des volumes. Par exemple : "c:", "d".
-clusternodes	Liste des nœuds de cluster avec des volumes à protéger. Tout d'abord, spécifiez le libellé "nodename" puis saisissez le nom du nœud. Puis spécifiez le libellé "volumes" et saisissez une liste de volumes pour le nœud. Par exemple : "nodename", "10.10.10.10", "volumes", "c:", "e:", "nodename", "10.10.10.11", "volumes", "c:"

Exemple :

Mettre les volumes d'un serveur sous 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-RepositoryCheck

La commande PowerShellStart-RepositoryCheck vous permet de vérifier l'intégrité d'une logithèque.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password [password] -force
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commandeStart-RepositoryCheck :

Tableau 286. Options de la commande Start-RepositoryCheck

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-repository	Requis. Le nom de la logithèque que vous souhaitez vérifier.
-all	Facultatif. Vérifiez toutes les logithèques associées à ce Core.
-force	Facultatif. Effectuer la vérification de la logithèque sans confirmation.

Exemple :

Démarrez la vérification d'une logithèque :

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -password 23WE@#$$dd
```

Start-RestoreArchive

Les entreprises utilisent souvent un stockage à long terme pour l'archivage des données conformes et non conformes. La fonction d'archivage de Rapid Recovery permet de prendre en charge la rétention prolongée des données conformes et non conformes. L'administrateur peut enregistrer une archive sur le stockage local ou à un emplacement réseau en spécifiant la commande `-Path` et les informations d'identification.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Start-RestoreArchive` :

Tableau 287. Options de la commande Start-RestoreArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Archiver les points de restauration de toutes les machines protégées.
-protectedserver	Machine protégée incluant les points de restauration à archiver. Vous pouvez spécifier plusieurs noms de machine en les mettant entre guillemets doubles (") et en les séparant par des espaces.
-repository	Nom de la logithèque sur laquelle vous souhaitez stocker les points de restauration restaurés. Vous devez mettre le nom entre guillemets doubles ; par exemple, "Logithèque1".
-archiveusername	Facultatif. Nom d'utilisateur permettant la connexion à la machine distante. Celui-ci est uniquement obligatoire pour un chemin d'accès réseau.
-archivepassword	Facultatif. Mot de passe permettant la connexion à la machine distante. Celui-ci est uniquement obligatoire pour un chemin d'accès réseau.
-path	Chemin de l'emplacement sur lequel enregistrer les données archivées. Par exemple : - Machine locale : "d:\travail\archive" - Chemin réseau : "\\nomserveur\nompartage" - Dossier d'un compte Cloud : "Nom du dossier" REMARQUE : Le nombre de symboles maximal est de 100 pour les emplacements locaux et réseau, et de 150 pour un emplacement Cloud.
-cloudaccountname	Facultatif. À utiliser uniquement pour l'archivage Cloud. Nom du compte Cloud sur lequel enregistrer l'archive.
-cloudcontainer	Facultatif. À utiliser uniquement pour l'archivage Cloud. Nom du conteneur Cloud dans le compte Cloud choisi, où l'archive doit être enregistrée. Lorsque vous utilisez cette option, vous devez également spécifier le paramètre « -cloudaccountname ».
-manifestcore	Facultatif. Spécifiez le Core à utiliser à partir du manifeste de l'archive restaurée.

Exemple :

Archiver tous les points de restauration de toutes les machines sur le Core et les stocker sur la machine locale :

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

La commande PowerShell `Start-ScheduledArchive` vous permet de forcer une archive planifiée Rapid Recovery à démarrer sur demande, quelle que soit la planification pré-établie.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Start-ScheduledArchive` :

Tableau 288. Options de la commande Start-ScheduledArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Forcez toutes les archives planifiées.
-id	Le numéro d'identification ou les identificateurs séparés par des espaces des archives planifiées que vous souhaitez forcer.

Exemple :

Démarrez plusieurs tâches d'archivage planifiés :

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

La commande `start-VBExport` démarre le lancement d'une exportation virtuelle à partir du point de restauration sélectionné vers une machine virtuelle serveur Oracle VirtualBox.

Les paramètres obligatoires sont le nom de la machine protégée contenant les points de récupération à exporter, le nom de la machine virtuelle vers laquelle l'exportation se fait, la quantité de RAM à allouer sur la machine virtuelle, le nom d'hôte et le port du serveur hôte Linux, ainsi que le chemin vers le dossier local, réseau ou Linux où seront stockés les fichiers résultants de la machine virtuelle.

Utilisation

L'utilisation de la commande est la suivante :

```
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]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Start-VBExport` :

Tableau 289. Options de la commande Start-VBExport

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Machine protégée avec des points de restauration à exporter.
-volumes	Facultatif. Liste des noms de volumes à exporter. Si rien n'est spécifié, tous les volumes des points de restauration spécifiés seront exportés. Les valeurs doivent être saisies entre guillemets doubles et séparées par un espace. Ne pas utiliser de slashes dans les noms des volumes. Par exemple, spécifiez "C:" et non "C:/"
-rpn	Facultatif. Le numéro du point de restauration à exporter. (Vous pouvez utiliser la commande <code>Get-RecoveryPoints</code> pour obtenir les numéros des points de restauration.) REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le point de restauration à sélectionner pour l'exportation. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA hh:mm tt » (par exemple : « 04/24/2015 09:00 AM »). Spécifiez les valeurs de temps du fuseau horaire défini sur votre machine locale. REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-vmname	Nom Windows de la machine virtuelle.
-ram	Alloue une quantité spécifique de RAM sur le serveur virtuel.

Option	Description
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-linuxhostname	Nom d'hôte du serveur VirtualBox Linux.
-hostport	Port du serveur VirtualBox Linux.
-targetpath	Chemin local, réseau ou Linux vers le dossier où les fichiers de la machine virtuelle doivent être stockés.
-pathusername	Nom d'utilisateur pour la machine réseau. Uniquement nécessaire lorsque vous spécifiez le chemin d'accès réseau dans le paramètre -targetpath.
-pathpassword	Mot de passe de connexion pour la machine réseau. Uniquement nécessaire lorsque vous spécifiez le chemin d'accès réseau dans le paramètre -targetpath.
-accountusername	Facultatif. À utiliser si vous spécifiez un compte d'utilisateur pour enregistrer la machine virtuelle exportée. Pour une machine locale ou réseau uniquement.
-accountpassword	Facultatif. À utiliser uniquement lorsque vous spécifiez un compte d'utilisateur pour enregistrer la machine virtuelle exportée à l'aide du paramètre -accountusername. Pour une machine locale ou réseau uniquement.

Exemple :

Exporter tous les volumes à partir du dernier point de restauration sur la machine 10.10.12.97 vers une machine virtuelle du nom de NewVirtualBoxVM :

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -targetpath D:/exports
```

Start-VirtualStandby

La commande PowerShellStart-VirtualStandby vous permet de forcer Rapid Recovery à exporter des données vers un disque de secours virtuel. Cette exportation à la demande peut se produire en-dehors des exportations de disques de secours virtuels régulièrement planifiées.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -protectedserver [name(s) | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande Start-VirtualStandby :

Tableau 290. Options de la commande Start-VirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Permet de forcer une exportation pour tous les disques de secours virtuels.
-protectedserver	Le ou les noms (séparés par une virgule et un espace) des machines protégées dont vous souhaitez forcer l'exportation.

Exemple :

Forcez une exportation de disque de secours virtuel d'une machine protégée :

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

Start-VMExport

La commande `Start-VMExport` démarre le lancement d'une exportation virtuelle à partir du point de restauration sélectionné vers une machine virtuelle serveur VMware Workstation.

Les paramètres obligatoires sont le nom de la machine protégée contenant les points de récupération à exporter, le nom de la machine virtuelle vers laquelle l'exportation se fait, la quantité de RAM à allouer sur la machine virtuelle et le chemin vers le dossier local ou réseau où seront stockés les fichiers résultants de la machine virtuelle.

Utilisation

L'utilisation de la commande est la suivante :

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or [IP address] -volumes [volume names] -rpn [number | numbers] |  
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |  
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]  
pathusername [user name] - pathpassword [password]
```

Options de la commande

Le tableau suivant présente les options disponibles pour la commande `Start-VMExport` :

Tableau 291. Options de la commande Start-VMExport

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Machine protégée avec des points de restauration à exporter.
-volumes	Facultatif. Liste des noms de volumes à exporter. Si rien n'est spécifié, tous les volumes des points de restauration spécifiés seront exportés. Les valeurs doivent être saisies entre guillemets doubles et séparées par un espace. Ne pas utiliser de slashes dans les noms des volumes. Par exemple, spécifiez "C:" et non "C:/"
-rpn	Facultatif. Le numéro du point de restauration à exporter. (Vous pouvez utiliser la commande Get-RecoveryPoints pour obtenir les numéros des points de restauration.)  REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-time	Facultatif. Détermine le point de restauration à sélectionner pour l'exportation. Vous devez spécifier l'heure exacte au format « MM/JJ/AAAA hh:mm tt » (par exemple : « 04/24/2015 09:00 AM »). Spécifiez les valeurs de temps du fuseau horaire défini sur votre machine locale.  REMARQUE : Si ni l'option 'time', ni l'option 'rpn' ne sont spécifiées dans cette commande, c'est alors le point de restauration le plus récent qui est exporté.
-vmname	Nom Windows de la machine virtuelle.
-ram	Alloue une quantité spécifique de RAM sur le serveur virtuel.
-usesourceram	Facultatif. Alloue la même quantité de RAM sur le serveur virtuel qu'il y en a sur la machine source protégée.
-targetpath	Chemin local, réseau ou Linux vers le dossier où les fichiers de la machine virtuelle doivent être stockés.
-pathusername	Nom d'utilisateur pour la machine réseau. Uniquement nécessaire lorsque vous spécifiez le chemin d'accès réseau dans -targetpath.
-pathpassword	Mot de passe de connexion pour la machine réseau. Uniquement nécessaire lorsque vous spécifiez le chemin d'accès réseau dans -targetpath.
-version	Version de VMware Tools à utiliser. Versions valides : 7, 8, 9 et 10.

Exemple :

Exporter tous les volumes à partir du dernier point de restauration sur la machine 10.10.12.97 vers une machine virtuelle du nom de NewVMwareVM :

```
>Start-VMExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath D:/exports
```


Stop-ActiveJobs

La commande `Stop-ActiveJobs` annule toutes les tâches actives pour une machine protégée spécifiée.

Utilisation

L'utilisation de la commande est la suivante :

```
Stop-ActiveJobs [-protectedserver [machine name | IP address]] [-core [host name]] -user [user name] -password [password] -jobtype [jobtype]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Stop-ActiveJobs` :

Tableau 292. Options de la commande Stop-ActiveJobs

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Sélectionne et annule des événements d'un type spécifié pour toutes les machines protégées.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Détermine la machine protégée sur laquelle les tâches doivent être annulées.
-jobtype	Facultatif. Indique le filtre de type de tâche. Les valeurs disponibles sont : 'transfer' (données de transfert), 'repository' (maintenance de logithèque), 'replication' (réplications locales et distantes), 'backup' (sauvegarde et restauration), 'bootcdbuilder' (création de CD d'amorçage), 'diagnostics' (chargement de journaux), 'exchange' (vérification des fichiers Exchange Server), 'export' (exporter des points de restauration), 'pushinstall' (déploiement du logiciel Agent sur les machines protégées), 'rollback' (restauration des données à partir d'un point de restauration), 'rollup' (consolidation des points de restauration), 'sqlattach' (vérifications de la capacité d'attachement pour l'agent) et 'mount' (ne concerne pas la logithèque). Toutes les tâches du type spécifié sont annulées par défaut.

Exemple :

Arrêter la tâche de transfert pour la machine protégée :

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

Arrêter toutes les tâches pour une machine protégée spécifique :

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

La commande `Suspend-Replication` permet à un administrateur de suspendre la réplication.

Un utilisateur peut suspendre une réplication de trois façons :

- Suspendre la réplication sur le Core maître pour toutes les machines protégées (`-outgoing` parameter)
L'administrateur doit spécifier le nom de la machine distante avec l'appairage de la réplication sortante pour suspendre la réplication sortante sur le Core maître.

```
>Suspend-replication -outgoing 10.10.12.10
```
- Suspendre la réplication sur le Core maître pour une seule machine protégée (paramètre `-protectedserver`)

```
>Suspend-replication -protectedserver 10.10.12.97
```
- Suspendre la réplication sur le Core cible (`-incoming` parameter)
Si le Core local est un Core cible, l'administrateur peut suspendre la réplication en spécifiant le Core maître et en utilisant le paramètre entrant.

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-Replication` :

Tableau 293. Options de la commande Suspend-Replication

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Suspend toutes les machines protégées sur le core sélectionné.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-pause	[snapshots],[replication] ou [vmexport].
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-protectedserver	Suspendre le serveur protégé actif.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-incoming	Nom d'hôte du core distant qui réplique sur la machine Core. La réplication est suspendue pour toutes les machines protégées sur le core distant.
-outgoing	Nom d'hôte du core cible distant sur lequel les données sont répliquées. La réplication est suspendue pour toutes les machines protégées sur le core distant.

Exemple :

Suspendre la réplication sortante sur le Core distant avec l'adresse IP : 10.10.1.15, pour la machine protégée portant l'adresse IP : 10.10.1.76 :

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

Suspendre les réplications sortantes à partir du Core local vers les cibles distantes avec l'adresse IP : 10.10.1.63 pour toutes les machines protégées :

```
>Suspend-replication -outgoing 10.10.1.63
```

Suspendre la réplication entrante à partir de 10.10.1.82 sur le Core distant portant l'adresse IP : 10.10.1.15 (l'administrateur peut uniquement suspendre la réplication entrante pour la totalité de la machine) :

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend-RepositoryActivity

La commande PowerShell `Suspend-RepositoryActivity` vous permet d'interrompre les activités d'une logithèque Rapid Recovery. L'interruption des activités place un verrou sur la logithèque, ce qui empêche l'entrée et la sortie de données.

Utilisation

L'utilisation de la commande est la suivante :

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -repository ["name" | "name1 " "name2"]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-RepositoryActivity` :

Tableau 294. Options de la commande Suspend-RepositoryActivity

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.

Option	Description
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Interrompez les activités de toutes les logithèques associées à ce Core.
-repository	Le nom de la logithèque que vous souhaitez verrouiller. Le nom doit être entouré de guillemets doubles (""). Vous pouvez spécifier plusieurs logithèques séparées par des espaces.

Exemples :

Suspendez des activités de plusieurs logithèques :

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

Suspendez les activités sur toutes les logithèques :

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

La commande PowerShell `Suspend-ScheduledArchive` vous permet de suspendre une archive planifiée Rapid Recovery. Cette commande empêche l'archive de se produire de la manière planifiée jusqu'à ce que vous la réactiviez..

Utilisation

L'utilisation de la commande est la suivante :

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-ScheduledArchive` :

Tableau 295. Options de la commande Suspend-ScheduledArchive

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.

Option	Description
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Suspend toutes les archives planifiées.
-id	Le numéro d'identification ou les numéros séparés par des espaces d'archives planifiées à mettre en pause.

Exemple :

Suspendre plusieurs archives planifiées :

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

La commande `Suspend-Snapshot` permet à un administrateur de suspendre des instantanés.

Utilisation

L'utilisation de la commande est la suivante :

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |  
-protectedserver [name | IP address] -time [time string]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-Snapshot` :

Tableau 296. Options de la commande Suspend-Snapshot

Option	Description
-?	Affiche de l'aide sur la commande.
-all	Suspend toutes les machines protégées sur le core sélectionné.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-time	L'heure au format 'Day-Hours-Minutes' où les instantanés seront repris (seulement pour les instantanés suspendus).

Exemple :

Suspendre les instantanés de la machine protégée avec l'IP 10.10.10.4 pour le Core local avec un temps défini pour reprendre :

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

La commande PowerShell `Suspend-VirtualStandby` vous permet de suspendre l'exportation des données vers un disque de secours virtuel Rapid Recovery.

Utilisation

L'utilisation de la commande est la suivante :

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -  
protectedserver [name(s) | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-VirtualStandby` :

Tableau 297. Options de la commande Suspend-VirtualStandby

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un identifiant de connexion. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Met en pause toutes les exportations des disques de secours virtuels.
- protectedserver	Le ou les noms (séparés par une virgule et des espaces) des machines protégées comportant les disques de secours virtuels que vous voulez interrompre.

Exemple :

Interrompez les exportations du disque de secours virtuel d'une machine protégée :

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#sdd -  
protectedserver 10.10.5.22
```

Suspend-VMExport

La commande `Suspend-VMExport` permet à l'administrateur de suspendre des exportations vers des machines virtuelles.

Utilisation

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -  
protectedserver [name | IP address]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Suspend-VMExport` :

Tableau 298. Options de la commande Suspend-VMExport

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-all	Suspend toutes les machines protégées sur le core sélectionné.
- protectedserver	Suspendre le serveur protégé actif.

Exemple :

Suspendre l'exportation de machine virtuelle pour la machine protégée avec l'adresse IP 10.10.10.4 pour le core local :

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

La commande `Update-Repository` ajoute une étendue à une logithèque DVM existante. La taille spécifiée doit être comprise entre 250 Mo et 16 To.

Utilisation

```
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]
```

Options de la commande

Le tableau suivant décrit les options disponibles pour la commande `Update-Repository` :

Tableau 299. Options de la commande `Update-Repository`

Option	Description
-?	Affiche de l'aide sur la commande.
-core	Facultatif. Adresse IP de la machine hôte du Core distant (avec un numéro de port optionnel). Par défaut, la connexion est faite avec le Core installé sur la machine locale.
-user	Facultatif. Nom d'utilisateur pour la machine hôte du Core distant. Si vous spécifiez un nom d'utilisateur, vous devez également fournir un mot de passe. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-password	Facultatif. Mot de passe de connexion à la machine hôte du Core distant. Si vous spécifiez un mot de passe, vous devez aussi fournir un nom d'utilisateur. Si aucun identifiant n'a été fourni, dans ce cas, ceux de l'utilisateur connecté seront utilisés.
-name	Le nom de la logithèque DVM.
-size	La taille de l'étendue de la logithèque DVM. Les unités disponibles sont : o, Ko, Mo, Go, To et Po.
-datapath	Pour l'emplacement local uniquement. Détermine le chemin des données de l'étendue de la logithèque DVM.
-metadatapath	Pour l'emplacement local uniquement. Détermine le chemin des métadonnées de l'étendue de la logithèque DVM.
-uncpath	Pour l'emplacement partagé uniquement. Détermine les chemins des données et des métadonnées de l'étendue de la logithèque DVM.
-shareusername	Pour l'emplacement partagé uniquement. Détermine l'identifiant de connexion à l'emplacement partagé.
-sharepassword	Pour l'emplacement partagé uniquement. Détermine le mot de passe de connexion à l'emplacement partagé.

Exemple :

Ajouter une étendue à la logithèque DVM d'une taille minimum de :

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:\repository\Metadata
```

Localisation

Lorsqu'il est exécuté sur la même machine que celle sur laquelle le Core Rapid Recovery est installé, le module PowerShell de Rapid Recovery utilise la langue d'affichage définie pour le Core. Les versions localisées de Rapid Recovery comme celle-ci prennent en charge l'anglais, le chinois (simplifié), le français, l'allemand, le japonais, le coréen, le portugais (Brésil) et l'espagnol.

Si un module PowerShell de Rapid Recovery est installé sur une machine distincte, l'anglais est la seule langue prise en charge.

Qualificateurs

Le tableau suivant décrit les qualificateurs disponibles pour le module Powershell de Rapid Recovery.

Tableau 300. Qualificateurs du module PowerShell de Rapid Recovery

Qualificateur	Utilisation
-core <Rapid Recovery Core Name>	Nom d'hôte du Core. Valeur par défaut :localhost
-ProtectedServer <Protected Server Name>	Nom de l'hôte/adresse IP de l'agent Rapid Recovery. Valeur par défaut :localhost si plusieurs serveurs sont protégés, sinon un seul serveur protégé.
-Mode <READ, READWRITE, WRITE>	Mode montage d'un point de restauration. Valeur par défaut :Read.
-Volumes <Snapshot Volume Letter>	Lettre du volume d'instantané de l'agent de Rapid Recovery. Valeur par défaut :All.
-User <User Name>	Nom d'utilisateur, utilisé pour la connexion au Core Rapid Recovery. Il s'agit généralement du service de l'utilisateur.
-Domain <Domain Name>	Domaine auquel l'utilisateur défini dans /User belongs.
-Password <Password>	Mot de passe de l'utilisateur défini dans /User.
-Path <Target path to mount, dismount recovery points or archive location>	Par exemple :C:\RapidRecoveryMount.

Extension des tâches Rapid Recovery avec des scripts

Rapid Recovery permet aux administrateurs d'automatiser l'administration et la gestion des ressources à certains moments en exécutant des commandes et des scripts. Le logiciel Rapid Recovery est compatible avec les scripts PowerShell pour Windows et les scripts Bourne Shell pour Linux.

Les tâches de Core sont créées automatiquement chaque fois que vous lancez sur le Core Rapid Recovery des opérations comme la réplication, l'exportation virtuelle ou la création d'un instantané de sauvegarde. Vous pouvez étendre ces tâches en exécutant un script avant ou après l'opération. On parle alors de pré-script ou de post-script, respectivement.

Cette section décrit les scripts pouvant être utilisés par les administrateurs à des moments déterminés dans Rapid Recovery pour Windows et Linux.

⚠ PRÉCAUTION : les exemples de scripts PowerShell et Bourne fournis dans ce document fonctionnent lorsqu'ils sont exécutés tels qu'ils sont définis par un administrateur qualifié. Modifiez avec précaution les scripts qui fonctionnent afin de conserver des versions fonctionnelles. Toute modification des exemples de scripts inclus ici, ou des scripts que vous créez vous-même, est considérée comme une personnalisation, normalement non couverte par le support technique de Dell.

Sujets :

- Utilisation des scripts PowerShell dans Rapid Recovery
- Paramètres d'entrée pour les scripts PowerShell
- Exemples de scripts PowerShell
- Utilisation des scripts Bourne Shell dans Rapid Recovery
- Paramètres d'entrée pour les scripts Bourne Shell
- Exemples de scripts Bourne Shell

Utilisation des scripts PowerShell dans Rapid Recovery

Windows PowerShell est un environnement connecté Microsoft .NET Framework conçu pour l'automatisation administrative. Rapid Recovery comprend des kits de développement de logiciels client (SDK) complets pour l'exécution de scripts PowerShell qui permettent aux utilisateurs administratifs d'exécuter des scripts PowerShell fournis par l'utilisateur à certains moments, par exemple, avant ou après un instantané, une vérification de la capacité d'attachement et de la montabilité, etc. Les administrateurs peuvent exécuter des scripts aussi bien depuis le Core de Rapid Recovery que depuis la machine protégée. Les scripts peuvent être paramétrés, et le résultat d'un script est écrit dans les fichiers journaux du core et de la machine protégée.

① REMARQUE : Pour les tâches nocturnes, il est nécessaire de conserver un fichier script, ainsi que le paramètre d'entrée **JobType** afin de distinguer les différentes tâches nocturnes.

Les fichiers de script sont situés dans le dossier **%ALLUSERSPROFILE%\AppRecovery\Scripts**.

- Sous Windows 7, le chemin pour localiser le dossier **%ALLUSERSPROFILE%** est le suivant : **C:\ProgramData**.
- Sous Windows 2003, le chemin pour localiser le dossier est : **Documents and Settings\All Users\Application Data**.

REMARQUE : Vous devez utiliser Windows PowerShell. Celui-ci doit être installé et configuré avant l'exécution des scripts de Rapid Recovery.

Pour plus d'informations sur l'utilisation des scripts PowerShell, voir [Exemples de scripts PowerShell](#), [Paramètres d'entrée pour les scripts PowerShell](#), [Paramètres d'entrée pour les scripts Bourne Shell](#) et [Exemples de scripts Bourne Shell](#).

Prérequis pour l'exécution de scripts PowerShell

Avant d'exécuter des scripts PowerShell pour Rapid Recovery, vous devez installer Windows PowerShell version 2.0 ou ultérieure. En raison de nouvelles fonctionnalités introduites dans PowerShell 3.0, notamment la facilitation de l'accès aux propriétés des objets, l'accès à PowerShell Web, et la prise en charge d'appels REST, Dell recommande l'utilisation de PowerShell version 3.0 ou ultérieure.

REMARQUE : Placez le fichier `powershell.exe.config` dans le répertoire de base PowerShell. Par exemple : 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>
```

Test des scripts PowerShell

Si vous souhaitez tester les scripts à exécuter, vous pouvez le faire à l'aide de l'éditeur graphique PowerShell, `powershell_is`. Vous devrez également ajouter le fichier de configuration, `powershell_ise.exe.config`, au même dossier de configuration, `powershell.exe.config`.

REMARQUE : Le fichier de configuration `powershell_ise.exe.config` doit avoir le même contenu que le fichier `powershell.exe.config`.

PRÉCAUTION : Si le pré ou post-script PowerShell échoue, la tâche échoue aussi.

Localisation

Lorsqu'il est exécuté sur la même machine que celle sur laquelle le Core de Rapid Recovery est installé, le module PowerShell de Rapid Recovery utilise la langue d'affichage définie pour le Core. Les versions localisées de Rapid Recovery comme celle-ci prennent en charge l'anglais, le chinois (simplifié), le français, le coréen, l'allemand, le japonais, le portugais (Brésil) et l'espagnol.

Si un module PowerShell de Rapid Recovery est installé sur une machine distante, l'anglais est la seule langue prise en charge.

Qualificateurs

Le tableau suivant décrit les qualificateurs disponibles pour le module Powershell de Rapid Recovery.

Tableau 301. Qualificateurs du module PowerShell de Rapid Recovery

Qualificateur	Utilisation
-core <Rapid Recovery Core Name>	Nom d'hôte du Core. Valeur par défaut :Localhost
-ProtectedServer <Protected Server Name>	Nom de l'hôte/adresse IP de l'agent Rapid Recovery. Valeur par défaut :Localhost si plusieurs serveurs sont protégés, sinon un seul serveur protégé.
-Mode <READ, READWRITE, WRITE>	Mode montage d'un point de restauration. Valeur par défaut :Read.
-Volumes <Snapshot Volume Letter>	Lettre du volume d'instantané de l'agent de Rapid Recovery. Valeur par défaut :All.
-User <User Name>	Nom d'utilisateur, utilisé pour la connexion au Core Rapid Recovery. Il s'agit généralement du service de l'utilisateur.
-Domain <Domain Name>	Domaine auquel l'utilisateur défini dans /User belongs.
-Password <Password>	Mot de passe de l'utilisateur défini dans /User.
-Path <Target path to mount, dismount recovery points or archive location>	Par exemple :C:\RapidRecoveryMount.

Paramètres d'entrée pour les scripts PowerShell

Tous les paramètres d'entrée disponibles sont utilisés dans les exemples de scripts. Les paramètres sont décrits dans les tableaux suivants :

❗ REMARQUE : les fichiers script doivent avoir le même nom que les fichiers des exemples de script.

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

Le tableau suivant présente les objets disponibles pour le paramètre AgentProtectionStorageConfiguration

Tableau 302. Objets du paramètre AgentProtectionStorageConfiguration

Méthode	Description
public Guid RepositoryId { get; set; }	Obtient ou définit l'identifiant de la logithèque dans laquelle seront stockés les points de restauration de l'agent.
public string EncryptionKeyId { get; set; }	Obtient ou définit l'identifiant de la clé de chiffrement des points de restauration de cet agent. Une chaîne vide signifie qu'il n'existe pas de chiffrement.

AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Le tableau suivant présente les objets disponibles pour le paramètre AgentTransferConfiguration.

Tableau 303. Objets du paramètre AgentTransferConfiguration

Méthode	Description
public uint MaxConcurrentStreams { get; set; }	Obtient ou définit le nombre maximum de connexions TCP simultanées que le core établit à l'agent pour le transfert de données.
public uint MaxTransferQueueDepth { get; set; }	Obtient ou définit le nombre maximal d'étendues de blocs qui peuvent être mises en file d'attente d'écriture. Lors de la lecture d'une plage de blocs depuis un flux de transfert, la plage est placée dans une file d'attente producteur/consommateur, où elle sera lue et écrite dans l'objet epoch par le fil consommateur. Si l'écriture par la logithèque est plus lente que la lecture par le réseau, cette file d'attente se remplit complètement. Le point de saturation de la file d'attente et d'arrêt des lectures s'appelle la longueur maximale de file d'attente de transfert.
public uint MaxConcurrentWrites { get; set; }	Obtient et définit le nombre maximum d'opérations d'écriture de blocs en attente dans un epoch à tout moment. Si des blocs supplémentaires sont reçus au-delà du nombre maximum d'opérations d'écriture spécifié dans ce paramètre, ces blocs supplémentaires sont ignorés jusqu'à ce qu'une des écritures en attente soit terminée.
public ulong MaxSegmentSize { get; set; }	Obtient et définit le nombre maximum de blocs contigus devant être transférés lors d'une même requête. Selon les tests, des valeurs plus élevées ou plus basses peuvent être optimales.
public Priority Priority { get; set; }	Obtient ou définit la priorité de requête de transfert.
public uint GetChangedBlocksRetries { get; set; }	Obtient ou définit le nombre de tentatives si la récupération initiale des blocs modifiés de l'agent a échoué.
public int MaxRetries { get; set; }	Obtient ou définit le nombre maximum de fois qu'un transfert défaillant peut être retenté avant d'être considéré comme un échec.
public bool UseDefaultMaxRetries { get; set; }	S'il est inclus, le nombre maximum par défaut de tentatives (spécifié dans la configuration du transfert) sera utilisé.
public Guid ProviderId { get; set; }	Obtient ou définit le GUID du fournisseur VSS à utiliser pour les instantanés sur cet hôte. Normalement, les administrateurs acceptent la valeur par défaut.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Obtient ou définit la collection d'identifiants des enregistreurs VSS qui doivent être exclus de cet instantané. L'identifiant d'enregistreur est entré en fonction du nom de l'enregistreur. Ce nom est attribué à des fins de documentation uniquement et ne correspond pas nécessairement au nom de l'éditeur.
public ushort TransferDataServerPort { get; set; }	Obtient ou définit une valeur contenant le port TCP sur lequel vous pourrez accepter des connexions depuis le Core du transfert de données de la machine protégée vers le Core. L'agent essaie d'écouter sur ce port, mais si celui-ci est en cours d'utilisation, la machine protégée peut utiliser un port différent. Le core doit utiliser le numéro de port spécifié dans les propriétés de BlockHashesUri et BlockDataUri de l'objet VolumeSnapshotInfo pour chaque volume dont un instantané a été pris.
public TimeSpan CleanSnapshotTimeout { get; set; }	Obtient ou définit le temps d'attente pour le nettoyage de l'instantané une fois le transfert terminé.

Méthode	Description
public TimeSpan SnapshotTimeout { get; set; }	Obtient ou définit le temps d'attente pour qu'une opération d'instantané VSS se termine avant abandon.
public TimeSpan TransferTimeout { get; set; }	Obtient ou définit le temps d'attente d'un nouveau contact depuis le core avant abandon de l'instantané.
public TimeSpan NetworkReadTimeout { get; set; }	Obtient ou définit le délai d'attente des opérations de lecture sur le réseau liées à ce transfert.
public TimeSpan NetworkWriteTimeout { get; set; }	Obtient ou définit le délai d'attente maximal des opérations d'écriture sur le réseau liées à ce transfert.
public uint InitialQueueSize { get; set; }	Obtient ou définit la taille de file d'attente initiale ou des requêtes.
public uint MinVolumeFreeSpacePercents { get; set; }	Obtient ou définit un montant minimum d'espace libre sur un volume, mesuré en pourcentage. Si l'espace libre est inférieur à celui spécifié dans ce paramètre, alors tous les journaux des modifications sont supprimés et une image de base est forcée.
public uint MaxChangeLogsSizePercents { get; set; }	Obtient ou définit la taille maximale des journaux des modifications apportées au pilote, dans le cadre de la capacité de volume mesurée en pourcentage. Si une partie des journaux des modifications est plus importante que cette valeur, alors tous les journaux des modifications sont supprimés et une image de base est forcée.
public bool EnableVerification { get; set; }	Obtient ou définit une valeur indiquant si une vérification de diagnostic de chaque bloc envoyé au Core doit être effectuée.

BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Le tableau suivant présente les objets disponibles pour le paramètre BackgroundJobRequest.

Tableau 304. Objets du paramètre BackgroundJobRequest

Méthode	Description
public AgentIdsCollection AgentIds { get; set; }	Obtient ou définit les identifiants des machines protégées.
public bool IsNightlyJob { get; set; }	Obtient ou définit la valeur indiquant si la tâche en arrière-plan est une tâche nocturne.
public Guid NightlyJobTransactionId { get; set; }	Obtient ou définit l'identifiant de transaction de tâches nocturnes.
public Guid JobId { get; set; }	Obtient ou définit l'identifiant de la tâche d'arrière-plan.
public bool Force { get; set; }	Obtient ou définit la valeur indiquant si la tâche a été forcée ou non.
public uint JobStartsCount { get; set; }	Obtient ou définit le nombre de tentatives de démarrage d'une tâche.
public virtual bool InvolvesAgentId(Guid agentId)	Détermine la valeur indiquant si l'agent concret est impliqué dans la tâche.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Hérite ses valeurs du paramètre DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Hérite ses valeurs du paramètre BackgroundJobRequest.

Tableau 305. Objets du paramètre DatabaseCheckJobRequestBase

Méthode	Description
public string RecoveryPointId { get; set; }	Obtient ou définit l'identifiant du point de restauration pour lequel les bases de données seront vérifiées.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Hérite ses valeurs du paramètre BackgroundJobRequest.

Le tableau suivant présente les objets disponibles pour le paramètre ExportJobRequest.

Tableau 306. Objets du paramètre ExportJobRequest

Méthode	Description
public uint RamInMegabytes { get; set; }	Obtient ou définit la taille de la mémoire pour la VM exportée. Spécifiez la valeur 0 pour utiliser la taille de mémoire de la machine source.
public ushort CpuCount { get; set; }	Obtient ou définit le nombre d'UC pour la VM exportée. Spécifiez la valeur 0 pour utiliser le nombre d'UC de la machine source.
public ushort CoresPerCpu { get; set; }	Obtient ou définit le nombre de Cores par UC pour la VM exportée. Spécifiez la valeur 0 pour utiliser le nombre de Cores par UC de la machine source.
public VirtualMachineLocation Location { get; set; }	Obtient ou définit l'emplacement cible de l'exportation. Il s'agit d'une classe de base abstraite.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Obtient ou définit les images de volumes devant être incluses dans l'exportation VM.
public ExportJobPriority Priority { get; set; }	Obtient ou définit la priorité de requête d'exportation.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Hérite ses valeurs du paramètre BackgroundJobRequest.

Tableau 307. Objets du paramètre NightlyAttachabilityJobRequest

Méthode	Description
public int SimultaneousJobsCount { get; set; }	Obtient ou définit le nombre de tâches pouvant être exécutées simultanément.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Hérite ses valeurs du paramètre BackgroundJobRequest.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

Le tableau suivant présente les objets disponibles pour le paramètre TakeSnapshotResponse.

Tableau 308. Objets du paramètre TakeSnapshotResponse

Méthode	Description
public Guid SnapshotSetId { get; set; }	Obtient ou définit le GUID attribué à cet instantané par VSS.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtient ou définit la collection des informations d'instantané pour chaque volume inclus dans l'instantané.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Hérite ses valeurs du paramètre BackgroundJobRequest.

Le tableau suivant présente les objets disponibles pour le paramètre TransferJobRequest.

Tableau 309. Objets du paramètre TransferJobRequest

Méthode	Description
public VolumeNameCollection VolumeNames { get; set; }	Obtient ou définit la collection de noms de volumes pour le transfert. VolumeNames est une structure de données qui contient les données suivantes : · GuidName. Guid associé au volume, utilisé comme nom si DisplayName n'est pas défini.

Méthode	Description
	DisplayName. Nom d'affichage du volume.
public VolumeNameCollection TransferredVolumes { get; set; }	Obtient ou définit la collection des volumes transférés.
public VolumeNameCollection DependentVolumeNames { get; set; }	Obtient ou définit la collection des volumes dépendants.
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	Obtient ou définit les quotas qui sont activés sur un volume.
public ShadowCopyType ShadowCopyType { get }	Obtient le type de copie pour le transfert. Les valeurs disponibles sont : - Copier - Plein
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtient ou définit la configuration du transfert. AgentTransferConfiguration est un objet qui aura les données suivantes : - MaxConcurrentStreams. Nombre maximum de connexions TCP simultanées que le core établira à l'agent pour le transfert de données. - MaxTransferQueueDepth. Nombre maximal d'étendues de blocs qui peuvent être mises en file d'attente d'écriture. - MaxConcurrentWrites. Nombre maximum d'opérations d'écriture de blocs en attente dans un epoch à tout moment. Si des blocs supplémentaires sont reçus lorsque ce nombre d'écritures de blocs est en attente, ces blocs supplémentaires sont ignorés jusqu'à ce qu'un des blocs en attente soit écrit. - MaxSegmentSize. Nombre maximum de blocs contigus devant être transférés lors d'une même requête. - Priority. Un objet qui aura les données suivantes : - Non défini - Un - Deux - Trois - Quatre - Cinq - Six - Sept - Huit - Neuf - Dix - Le plus élevé (égal à Un) - Le plus bas (égal à Dix) - Par défaut (égal à Cinq) - MaxRetries. Nombre maximum de fois qu'un transfert ayant échoué peut être retenté avant d'être considéré comme un échec. - UseDefaultMaxRetries. Valeur indiquant que le nombre maximal de nouvelles tentatives est la valeur par défaut. - ProviderId. GUID du fournisseur VSS à utiliser pour les instantanés sur cet hôte. Les utilisateurs utilisent généralement le paramètre par défaut.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtient ou définit la configuration du transfert.

Méthode	Description
public string Key { get; set; }	Génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier les requêtes de transfert.
public bool IsBaselImage { get; set; }	Obtient ou définit la valeur indiquant si l'image de base sera prise.
public bool IsForced { get; set; }	Obtient ou définit la valeur indiquant si le transfert a été forcé ou non.
public Guid ProtectionGroupId { get; set; }	Obtient ou définit l'identifiant du groupe de protection.
public TargetComponentTypes LogTruncationTargets { get; set; }	Obtient ou définit la valeur indiquant pour quelles bases de données la troncature des journaux sera effectuée (SQL ou Exchange).
public bool ForceBaselImage { get }	Obtient la valeur indiquant si l'image de base a été forcée ou non.
public bool IsLogTruncation { get }	Obtient la valeur indiquant si la tâche de troncature de journal est en cours ou non.

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Hérite ses valeurs du paramètre TransferScriptParameterBase.

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Le tableau suivant présente les objets disponibles pour le paramètre TransferPostscript. Hérite ses valeurs du paramètre TransferScriptParameterBase.

Tableau 310. Objets du paramètre TransferPostscript

Méthode	Description
public VolumeNameCollection VolumeNames { get; set; }	Obtient ou définit la collection des noms de volumes pour le transfert. VolumeNames est une structure de données qui contient les données suivantes : • GuidName. Guid associé au volume, utilisé comme nom si DisplayName n'est pas défini. • DisplayName. Nom d'affichage du volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtient ou définit le type de copie pour le transfert. ShadowCopyType est une énumération de valeurs. Les valeurs disponibles sont : • Inconnu • Copier • Plein
public AgentProtectionStorageConfigurationCom mon StorageConfiguration { get; set; }	Obtient ou définit la configuration du transfert.
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtient ou définit la configuration du transfert.

AgentTransferConfiguration est un objet qui aura les données suivantes :

- MaxConcurrentStreams. Nombre maximum de connexions TCP simultanées que le core établira à l'agent pour le transfert de données.
- MaxTransferQueueDepth. Nombre maximal d'étendues de blocs qui peuvent être mises en file d'attente d'écriture.
- MaxConcurrentWrites. Nombre maximum d'opérations d'écriture de blocs en attente dans un epoch à tout moment. Si des blocs supplémentaires sont reçus lorsque ce nombre d'écritures de blocs est en attente, ces blocs supplémentaires sont ignorés jusqu'à ce qu'un des blocs en attente soit écrit.
- MaxSegmentSize. Nombre maximum de blocs contigus devant être transférés lors d'une même requête.
- Priority. Un objet qui a les données suivantes :
 - "Non défini
 - "Un
 - "Deux
 - "Trois
 - "Quatre
 - "Cinq
 - "Six
 - "Sept
 - "Huit
 - "Neuf
 - "Dix
 - "Le plus élevé (égal à Un)
 - "Le plus bas (égal à Dix)
 - "Par défaut (égal à Cinq)
- MaxRetries. Nombre maximum de fois qu'un transfert ayant échoué peut être retenté avant d'être considéré comme un échec.
- UseDefaultMaxRetries. Valeur indiquant que le nombre maximal de nouvelles tentatives est la valeur par défaut.
- ProviderId. GUID du fournisseur VSS à utiliser pour les instantanés sur cet hôte. Normalement, les administrateurs acceptent la valeur par défaut.

public AgentTransferConfiguration
TransferConfiguration { get; set; } (cont.)

- ExcludedWriterIds. Collection d'identifiants des enregistreurs VSS qui devront être exclus de cet instantané. L'identifiant d'enregistreur est entré en fonction du nom de l'enregistreur. Ce nom sert à des fins de documentation uniquement et il n'est pas nécessaire qu'il corresponde exactement au nom réel de l'enregistreur.
- TransferDataServerPort. Valeur contenant le port TCP sur lequel vous pouvez accepter des connexions depuis le core pour le transfert de données effectif de l'agent vers le core.
- SnapshotTimeout. Délai d'attente qu'une opération d'instantané VSS se termine avant d'être abandonnée.
- TransferTimeout. Délai d'attente d'un nouveau contact depuis le core avant abandon de l'instantané.
- NetworkReadTimeout. Délai d'attente maximal des opérations de lecture sur le réseau liées à ce transfert.
- NetworkWriteTimeout. Délai d'attente maximal des opérations d'écriture sur le réseau liées à ce transfert.
- InitialQueueSize. Taille de la file d'attente initiale des requêtes.
- MinVolumeFreeSpacePercents. Quantité minimale d'espace disponible sur un volume, en pourcentage.
- MaxChangeLogsSizePercents. Taille maximale des journaux répertoriant les modifications apportées au pilote, dans le cadre de la capacité de volume mesurée en pourcentage.

Méthode	Description
	· EnableVerification. Valeur indiquant si une vérification diagnostique de chacun des blocs envoyés au core doit être effectuée.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtient ou définit la configuration du stockage. L'objet AgentProtectionStorageConfiguration contient les données suivantes : · RepositoryId. Identifiant de la logithèque dans laquelle seront stockés les points de restauration de cet agent. · EncryptionKeyId. Identifiant de la clé de chiffrement des points de restauration de cet agent. Une chaîne vide signifie qu'il n'existe pas de chiffrement.
public string Key { get; set; }	La méthode Key génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier les requêtes de transfert.
public bool ForceBaseImage { get; set; }	Obtient ou définit la valeur indiquant si le transfert était la capture d'une image de base forcée.
public bool IsLogTruncation { get; set; }	Obtient ou définit la valeur indiquant si une troncature des journaux est en cours d'exécution ou non.
public uint LatestEpochSeenByCore { get; set; }	Obtient ou définit la valeur de la dernière epoch. La méthode LatestEpochSeenByCore est le nombre ordinal du dernier instantané créé par le core. Il s'agit du 'numéro epoch' attribué par le pilote filtre à cet instantané au moment où il est créé avec VSS.
public Guid SnapshotSetId { get; set; }	Obtient ou définit le GUID attribué à cet instantané par VSS.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtient ou définit la collection des informations sur l'instantané pour chaque volume inclus dans l'instantané.

TransferScriptParameterBase (namespace Replay.Common.Contracts.PowerShellExecution)

Le tableau suivant présente les objets disponibles pour le paramètre TransferScriptParameterBase.

Tableau 311. Objets du paramètre TransferScriptParameterBase

Méthode	Description
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtient ou définit la configuration du transfert.
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Obtient ou définit la configuration du transfert.

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

Le tableau suivant présente les objets disponibles pour le paramètre VirtualMachineLocation.

Tableau 312. Objets du paramètre VirtualMachineLocation

Méthode	Description
public string Description { get; set;}	Obtient ou définit pour cet emplacement une description lisible par l'utilisateur.
public string Name { get; set;}	Obtient ou définit le nom de la VM.

VolumelmageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Hérite des valeurs du paramètre System.Collections.ObjectModel.Collection<string>.

VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

Le tableau suivant présente les objets disponibles pour le paramètre VolumeName.

Tableau 313. Objets du paramètre VolumeName parameter

Méthode	Description
public string GuidName { get; set;}	Obtient ou définit l'identifiant du volume.
public string DisplayName { get; set;}	Obtient ou définit le nom de la VM.
public string UrlEncode()	Obtient une version codée par URL du nom pouvant être transmise proprement dans une URL.
	REMARQUE : Il existe un problème connu dans .NET 4.0 WCF (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312), qui empêche les caractères d'échappement de chemin de fonctionner correctement dans un modèle d'URI. Puisqu'un nom de volume contient les caractères spéciaux « \ » et « ? », vous devez les remplacer par d'autres caractères spéciaux.
public string GetMountName()	Retourne un nom pour ce volume. Ce nom est valide pour le montage de l'image de volume sur certains dossiers.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Hérite des valeurs du paramètre System.Collections.ObjectModel.Collection<VolumeName>.

Le tableau suivant présente les objets disponibles pour le paramètre VolumeNameCollection.

Tableau 314. Objets du paramètre VolumeNameCollection

Méthode	Description
public override bool Equals(object obj)	Détermine si cette instance et un objet spécifié, qui doit également être un objet volumeNameCollection, ont la même valeur. (Overrides Object.Equals(Object).)
public override int GetHashCode()	Retourne le code de hachage de VolumeNameCollection. (Overrides Object.GetHashCode().)

VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer)

Le tableau suivant présente les objets disponibles pour le paramètre VolumeSnapshotInfo.

Tableau 315. Objets du paramètre VolumeSnapshotInfo

Méthode	Description
public Uri BlockHashesUri { get; set;}	Obtient ou définit l'URI sur lequel les hachages MD5 des blocs de volumes peuvent être lus.
public Uri BlockDataUri { get; set;}	Obtient ou définit l'URI sur lequel les blocs de données de volumes peuvent être lus.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Hérite ses valeurs du paramètre System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Exemples de scripts PowerShell

Les modèles de script suivants sont fournis pour assister les utilisateurs administratifs dans l'exécution de scripts PowerShell.

Liens connexes

[PreTransferScript.sh](#)
[PostTransferScript.ps1](#)
[PreExportScript.ps1](#)
[PostExportScript.ps1](#)
[PreNightlyJobScript.ps1](#)
[PostNightlyJobScript.ps1](#)

PreTransferScript.ps1

PreTransferScript s'exécute sur la machine protégée avant le transfert d'un instantané.

Exemple 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

PostTransferScript s'exécute sur la machine protégée après le transfert d'un instantané.

Exemple TransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal) | out-null
# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
    echo 'TransferPostscriptParameterObject parameter is null'
}
else {
    echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
        echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
        echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

PreExportScript s'exécute sur le core avant toute tâche d'exportation.

Exemple 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

PostExportScript s'exécute sur le core après toute tâche d'exportation.

REMARQUE : Il n'existe pas de paramètres d'entrée pour PostExportScript lorsqu'il est exécuté une fois sur la machine protégée exportée après le démarrage initial. La machine protégée régulière doit contenir ce script dans le dossier des scripts PowerShell sous le nom PostExportScript.ps1.

Exemple 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

PreNightlyJobScript s'exécute avant chaque tâche nocturne sur le core. Il contient le paramètre \$JobClassName qui facilite la gestion de ces tâches enfant séparément.

Exemple 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.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results: ';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List`1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
            echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
            }
        }
        break;
    }
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results: ';
        if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];

```

```

echo 'Transfer job results: ';
if($TransferJobRequestObject -eq $null) {
    echo 'TransferJobRequestObject parameter is null';
}
else {
    echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
    echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
}
echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
break;
}
}

```

PostNightlyJobScript.ps1

PostNightlyJobScript s'exécute après chaque tâche nocturne sur le core. Il contient le paramètre \$JobClassName qui facilite la gestion de ces tâches enfant séparément.

Exemple 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.TransferConfiguration;
        echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
    }
    echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
    $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
    if($TakeSnapshotResponseObject -eq $null) {
        echo 'TakeSnapshotResponseObject parameter is null';
    }
    else {
        echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
        echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
    }
    break;
}
}

```

Utilisation des scripts Bourne Shell dans Rapid Recovery

Bourne shell (sh) est un langage shell ou interpréteur en ligne de commande utilisé pour les systèmes d'exploitation Unix. Bourne shell est utilisé dans Rapid Recovery avec Linux pour personnaliser les environnements et spécifier l'occurrence de certaines opérations dans un ordre prédéterminé. .sh est l'extension de fichier et la convention utilisée pour nommer les fichiers Bourne Shell.

Bourne Again Shell (BASH) est un langage shell similaire qui implémente la même syntaxe, les mêmes paramètres, la même expansion des variables d'environnement, la même redirection et le même mécanisme de mise entre guillemets. BASH utilise également la même extension de fichier .sh. Les informations présentées ici s'appliquent également à BASH.

En utilisant des hooks de script de pré et post transfert et d'exportation, vous pouvez effectuer des opérations système avant et après un transfert ou une exportation. Par exemple, vous pouvez avoir besoin de désactiver une tâche cron pendant qu'un transfert est en cours, et de la réactiver une fois le transfert terminé. Vous pouvez également devoir exécuter des commandes pour purger des données spécifiques à une application sur le disque. Le contenu est écrit sur un fichier temporaire et exécuté avec `exec`. Le script s'exécute alors à l'aide de l'interpréteur défini dans la première ligne du script, par exemple (`#!/usr/bin/env bash`). Si l'interpréteur spécifié n'est pas disponible, le script utilise le shell par défaut défini dans la variable d'environnement `$SHELL`.

Vous pouvez substituer et utiliser n'importe quel interpréteur. Par exemple, dans la ligne `#!` du script, vous pouvez remplacer « `bash` » par « `zsh` » (Z shell), « `tcsh` » (tee shell), etc., selon votre préférence.

Vous pouvez ajouter des objets à partir du paramètre `TransferPrescript` ou vos propres commandes aux scripts `PreTransferScript.sh` et `PostTransfer.sh` pour les personnaliser.

Cette section décrit les scripts qui peuvent être utilisés par les administrateurs à des moments déterminés dans Rapid Recovery pour Windows et Linux. Il inclut les rubriques suivantes :

- [Paramètres d'entrée pour les scripts Bourne Shell](#)
- [Exemples de scripts Bourne Shell](#)

Prérequis pour l'exécution de scripts Bourne Shell

Rapid Recovery offre la possibilité d'exécuter des scripts Bourne Shell sur la machine agent Linux avant et après un transfert. Les machines Linux protégées par le logiciel agent Rapid Recovery prennent en charge les scripts suivants.

❗ REMARQUE : si un script n'est pas exécutable, la tâche de transfert va échouer.

- `PreTransferScript.sh`
- `PostTransferScript.sh`
- `PostExportScript.sh`

Pour utiliser ces scripts, vérifiez qu'ils se trouvent bien dans le répertoire `/opt/apprecovery/scripts/`.

Paramètres des scripts de transfert et de post-transfert pris en charge

Les paramètres suivants sont pris en charge sur Linux pour les scripts de transfert. Pour en savoir plus, voir [Exemples de scripts Bourne Shell](#).

- `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`

Les paramètres suivants sont pris en charge sur Linux pour les scripts de post-transfert.

- `TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames`
- `TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType`
- `TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration`

- `TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration`
- `TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key`
- `TransferPostscriptParameter_ForceBaselImage=$TransferPostscriptParameter_ForceBaselImage`
- `TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation`
- `TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestEpochSeenByCore`

Test des scripts Bourne Shell

Vous pouvez tester les scripts que vous souhaitez exécuter à l'aide de l'éditeur des fichiers de script (.sh).

REMARQUE : si le pré ou post-script Bourne Shell échoue, la tâche échoue aussi. Des informations sur cette tâche sont disponibles dans le fichier `/var/log/apprecovery/apprecovery.log`.
Les scripts correctement exécutés renvoient le code de sortie 0.

Paramètres d'entrée pour les scripts Bourne Shell

Les tableaux suivants décrivent les paramètres des scripts Bourne Shell dans Rapid Recovery.

TransferPrescriptParameters_VolumeNames

Le tableau suivant présente les objets disponibles pour le paramètre `TransferPrescript`.

Tableau 316. Objets TransferPrescript

Méthode	Description
<pre>public VolumeNameCollection VolumeNames (get; set;)</pre>	Obtient ou définit la collection des noms de volumes pour le transfert. <code>VolumeNames</code> est une structure de données qui contient les données suivantes : • <code>GuidName</code>. Guid associé au volume, utilisé comme nom si <code>DisplayName</code> n'est pas défini. • <code>DisplayName</code>. Nom d'affichage du volume.
<pre>public ShadowCopyType ShadowCopyType { get; set; }</pre>	Obtient ou définit le type de copie pour le transfert. <code>ShadowCopyType</code> est une énumération de valeurs. Les valeurs disponibles sont : • Inconnu • Copier • Plein
<pre>public string Key { get; set; }</pre>	La méthode <code>Key</code> génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier les requêtes de transfert.
<pre>public bool ForceBaselImage { get; set; }</pre>	Obtient ou définit la valeur indiquant si le transfert était la capture d'une image de base forcée.
<pre>public bool IsLogTruncation { get; set; }</pre>	Obtient ou définit la valeur indiquant si une troncature des journaux est en cours d'exécution ou non.
<pre>public uint LatestEpochSeenByCore { get; set; }</pre>	Obtient ou définit la valeur de la dernière epoch.

Méthode	Description
	La méthode LatestEpochSeenByCore est le nombre ordinal du dernier instantané créé par le Core. Il s'agit du 'numéro epoch' attribué par le pilote filtre à cet instantané au moment où il est créé avec VSS.

TransferPostscriptParameter

Le tableau suivant présente les objets disponibles pour le paramètre TransferPostscript.

Tableau 317. Objets TransferPostscript

Méthode	Description
public VolumeNameCollection VolumeNames (get; set;)	Obtient ou définit la collection des noms de volumes pour le transfert. VolumeNames est une structure de données qui contient les données suivantes : - GuidName. Guid associé au volume, utilisé comme nom si DisplayName n'est pas défini. - DisplayName. Nom d'affichage du volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtient ou définit le type de copie pour le transfert. ShadowCopyType est une énumération de valeurs. Les valeurs disponibles sont : - Inconnu - Copier - Plein
public string Key { get; set; }	La méthode Key génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier les requêtes de transfert.
public bool ForceBaseImage { get; set; }	Obtient ou définit la valeur indiquant si le transfert était la capture d'une image de base forcée.
public bool IsLogTruncation { get; set; }	Obtient ou définit la valeur indiquant si une troncature des journaux est en cours d'exécution ou non.
public uint LatestEpochSeenByCore { get; set; }	Obtient ou définit la valeur de la dernière epoch. La méthode LatestEpochSeenByCore est le nombre ordinal du dernier instantané créé par le Core. Il s'agit du 'numéro epoch' attribué par le pilote filtre à cet instantané au moment où il est créé avec VSS.

Exemples de scripts Bourne Shell

Cette section présente des exemples de scripts Bourne Shell proposés aux utilisateurs administratifs pour être exécutés sur les machines protégées.

⚠ PRÉCAUTION : Les exemples de scripts Bourne fournis dans ce document fonctionnent lorsqu'ils sont exécutés tels qu'ils sont définis par un administrateur qualifié. Modifiez avec précaution les scripts qui fonctionnent afin de conserver des versions fonctionnelles. Toute modification des exemples de scripts inclus ici, ou des scripts que vous créez vous-même, est considérée comme une personnalisation, qui n'est normalement pas couverte par le support Dell.

REMARQUE : Les machines protégées utilisent la commande shell 'exec' pour lancer le script. Vous pouvez indiquer quel interpréteur doit exécuter le script en définissant cette information dans la première ligne du script. Si vous ne spécifiez pas l'interprète, c'est le shell par défaut qui interprète le script. Si vous choisissez autre chose que le shell par défaut, vous devez vérifier que l'interpréteur spécifié est disponible sur toutes les machines protégées.

Les exemples de scripts utilisés pour les machines protégées comprennent :

PreTransferScript.sh

PreTransferScript s'exécute sur la machine protégée avant le transfert d'un instantané.

Le script suivant stocke les valeurs des paramètres d'entrée indiqués dans Pre(Post)TransferScriptResult.txt, qui est situé et stocké dans le répertoire racine.

Exemple 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

PostTransferScript s'exécute sur la machine protégée après le transfert d'un instantané.

Le script suivant stocke les valeurs des paramètres d'entrée indiqués dans Pre(Post)TransferScriptResult.txt, qui est situé et stocké dans le répertoire racine.

Exemple TransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

PostExportScript s'exécute sur la machine protégée après le transfert.

Le script suivant stocke les valeurs des paramètres d'entrée indiqués dans Pre(Post)ExportScriptResult.txt, qui est situé et stocké dans le répertoire racine.

Exemple PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```


Les API Rapid Recovery

Le but de cette section est de fournir une présentation et un aperçu de la technologie REST (Representational State Transfer) de Rapid Recovery, des interfaces de programmes d'application (API), leur utilisation et leur fonction.

Les API du service Web Rapid Recovery sont des API RESTful qui vous permettent d'automatiser et de personnaliser certaines fonctions et tâches au sein de la solution logicielle Rapid Recovery, afin de vous aider à atteindre vos objectifs professionnels.

Ces API sont accessibles à partir de la page **Téléchargements** du Portail des licences Dell Data Protection | Rapid Recovery.

Sujets :

- [Public visé](#)
- [Utilisation des API REST Rapid Recovery](#)
- [Téléchargement et affichage des API du Core et de l'Agent](#)
- [Lectures complémentaires conseillées](#)

Public visé

Les API Rapid Recovery sont prévues pour être utilisées par les développeurs d'applications qui souhaitent intégrer et étendre Rapid Recovery dans leurs applications, ainsi que pour les administrateurs qui souhaitent exécuter des scripts d'interaction avec le serveur Core Rapid Recovery.

Utilisation des API REST Rapid Recovery

Les API Rapid Recovery sont des API de style REST, ce qui signifie qu'elles utilisent des requêtes HTTP pour fournir un accès aux ressources (entités de données) par le biais de chemins URI. Les API Rapid Recovery utilisent les méthodes HTTP standard, comme GET, PUT, POST et DELETE. Vu que les API REST sont basées sur des standards ouverts, vous pouvez utiliser n'importe quel(le) langage ou outil prenant en charge les requêtes HTTP.

Il existe deux façons pour les développeurs et les administrateurs de travailler avec les API Rapid Recovery. À savoir :

- Utiliser C# ou d'autres langages .NET pour directement utiliser des fichiers DLL client .NET Rapid Recovery.
- Communiquer directement avec le point de terminaison HTTP pour générer votre propre XML.

La première approche est préférable. Les DLL du client sont inclus dans le SDK Rapid Recovery. La méthode d'appel des API Rapid Recovery est semblable à la façon dont vous consommeriez n'importe quel service WCF Windows 4.5X .NET.

Téléchargement et affichage des API du Core et de l'Agent

Le *Dell Data Protection | Rapid Recovery Kit de développement logiciel (SDK)* inclut les API REST pour le Core Rapid Recovery et les composants de l'Agent Rapid Recovery, les échantillons et les fichiers pris en charge. Ces contenus sont intégrés dans les dossiers suivants, puis compressés dans une archive qui inclut les composants suivants :

Tableau 318. Composants inclus dans l'archive du SDK

Nom du dossier	Contenu	Description
Core.Contracts	API du Core Rapid Recovery	Contient des API pour aider les développeurs ou les administrateurs à exécuter des scripts de fonctions dans le Core Rapid Recovery. 2 ensembles d'accords de service sont disponibles. - Ouvrez le fichier HTML CoreWeb.Client dans un navigateur Web pour afficher les informations des standards REST généraux. Les accords de service sont répertoriés. Lorsque vous cliquez sur un URI (Uniform Resource Identifier) avec lien hypertexte correspondant, le navigateur ouvre les informations dans le dossier Core.Contracts/docWeb/. La page obtenue affiche les informations des opérations de service REST générales, celles-ci incluent les méthodes et les descriptions. - Ouvrez le fichier Core.Client HTML dans un navigateur Web pour afficher des informations détaillées C#. Lorsque vous cliquez sur un accord de service avec lien hypertexte (classe), le navigateur ouvre les informations dans le répertoire Core.Contracts/doc/. La page obtenue affiche des informations détaillées sur toutes les méthodes C# de la classe sélectionnée.
Agent.Contracts	API de l'Agent Rapid Recovery (déconseillées)	Contient les API que les développeurs ou administrateurs peuvent utiliser pour manipuler l'Agent Rapid Recovery sur des machines protégées. ⚠ PRÉCAUTION : Les API d'Agent sont déconseillées et vont être supprimées des versions ultérieures du SDK. La manipulation directe des API d'agent est déconseillée. L'utilisation de ces API est considéré comme une personnalisation et ne sera pas prise en charge. Les informations sont fournies dans la documentation à des fins de documentation. - Ouvrez le fichier AgentWeb.Client dans un navigateur Web pour afficher les informations des standards REST généraux. - Ouvrez le fichier HTML Agent.Client dans un navigateur Web pour afficher des informations C# détaillées.
AppRecoveryAPISamples	Exemples de code et bibliothèques de liens dynamiques	AppRecoveryAPISamples contient des échantillons du code qui sont écrits en langage de programmation C#. Ces fichiers représentent un bon point de départ pour afficher les extraits de code si vous utilisez les API pour personnaliser votre interface GUI, des systèmes de gestion, et ainsi de suite. AppRecoveryAPISamples\Dependencies contient des fichiers de bibliothèques de liens dynamiques (DLL) qu'utilise le Core Rapid Recovery. Les DLL contiennent des accords de données (les types de données dont le Core est familier) et les accords de service (méthodes de gestion et opérations qui peuvent être utilisées pour forcer le Core à faire quelque chose). Si vous souhaitez personnaliser votre propre interface utilisateur graphique, ou utiliser un système de gestion pour travailler avec le Core Rapid Recovery, ces DLL sont requis. ❗ REMARQUE : La version du DLL utilisé doit correspondre à la version du Core.

Vous pouvez télécharger le SDK en tant qu'archive (API-Reference-x.x.x-xxxx). Chaque x représente un chiffre du numéro de build de la version correspondante.

Effectuez les étapes de cette procédure pour obtenir le SDK, téléchargez-le sur votre destination spécifiée, puis décompressez les fichiers en vue de préparer l'utilisation des API Core et Agent.

- Connectez-vous au Portail des licences Dell Data Protection | Rapid Recovery à l'adresse <https://licenseportal.com>.
- Dans la zone gauche de navigation du Portail des licences, cliquez sur **Téléchargements**.
La page **Téléchargements** du Portail des licences s'affiche.
- Dans la page **Téléchargements**, dans la section des applications Windows, faites défiler les options vers le bas jusqu'à la description pour le SDK et cliquez sur **Télécharger**.

- 4 Enregistrez l'archive téléchargée dans votre emplacement préféré.
- 5 Décompressez l'archive.
Dans le nouveau dossier API-Reference-x.x.x-xxxx, vous voyez les ensembles de fichiers distincts décrits dans le tableau précédent.
- 6 Ouvrez les fichiers HTML clés décrits dans le tableau précédent sous un navigateur Web pour afficher les conseils sur les API.

Lectures complémentaires conseillées

Le Guide d'installation et de mise à jour de *Dell Data Protection | Rapid Recovery* contient une présentation de l'architecture Rapid Recovery et décrit les étapes nécessaires pour l'installation des composants Rapid Recovery, ainsi que pour la mise à niveau des composants du Core ou de l'agent depuis des versions antérieures.

Vous pouvez afficher ou télécharger ce guide depuis l'adresse <https://support.software.dell.com/rapid-recovery/release-notes-guides/>.

À propos de Dell

Dell est à l'écoute de ses clients et leur offre des technologies innovantes dans le monde entier, ainsi que des solutions et des services métier reconnus pour leur fiabilité et leur qualité. Pour plus d'informations, rendez-vous sur <http://software.dell.com>.

Contacteur Dell

Pour des questions commerciales ou autres demandes, rendez-vous sur <http://software.dell.com/company/contact-us.aspx> ou appelez le + 1-949-754-8000.

Ressources du support technique

Le support technique est accessible aux clients ayant acheté un logiciel Dell et disposant d'un contrat de maintenance valide, ainsi qu'aux clients utilisant des versions d'évaluation. Pour accéder au Portail de support, rendez-vous sur <https://support.software.dell.com>.

Le portail du support fournit des outils d'auto-assistance que vous pouvez utiliser pour résoudre rapidement et de manière indépendante des problèmes 24 heures/24 toute l'année. En outre, il permet d'accéder directement aux techniciens du support des produits via un système en ligne de demande de service.

Le Portail de support vous permet d'effectuer les opérations suivantes :

- créer, mettre à jour et gérer les demandes de service (dossiers).
- consulter les articles dans la base de connaissances.
- obtenir des notifications sur les produits.
- télécharger des logiciels. Pour obtenir la version d'évaluation du logiciel, rendez-vous sur <http://software.dell.com/trials>.
- participer à des discussions avec la communauté.

Agent

L'Agent Rapid Recovery est un logiciel installé sur une machine physique ou virtuelle qui permet d'ajouter celle-ci à la protection par Core Rapid Recovery.

API REST

La technologie REST (Representational State Transfer) est une architecture logicielle simple et sans état conçue pour l'évolutivité. Rapid Recovery utilise cette architecture pour ses interfaces de programmes d'application (API) pour automatiser et personnaliser certaines fonctions et tâches. Un ensemble séparé d'API REST pour les fonctionnalités principales et pour les fonctionnalités des machines protégées (agent).

capacité d'attachement SQL

La vérification de la capacité d'attachement SQL est un test effectué dans le Core Rapid Recovery afin de vérifier que les points de restauration SQL sont exempts d'erreurs et disponibles pour une sauvegarde en cas de défaillance.

caractères interdits

Les caractères interdits sont des caractères qui ne doivent pas être utilisés pour donner un nom à un objet de la console Core Rapid Recovery. Par exemple, lors du choix du nom d'affichage d'une machine protégée, il ne faut utiliser aucun des caractères spéciaux suivants :

Tableau 319. Caractères interdits

Caractère	Nom du caractère	Interdit pour
?	point d'interrogation	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
	barre verticale	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
:	deux points	nom d'affichage d'une machine, clé de chiffrement, logithèque L'utilisation de ce symbole est prise en charge lorsque vous spécifiez un chemin, par exemple, c:\data .
/	barre oblique avant	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
\	barre oblique arrière	nom d'affichage d'une machine, clé de chiffrement, logithèque L'utilisation de ce symbole est prise en charge lorsque vous spécifiez un chemin local ou réseau, par exemple, c:\data ou \\ComputerName\SharedFolder\
*	astérisque	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
"	guillemet anglais	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
<	crochet angulaire ouvrant	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
>	crochet angulaire fermant	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin

Central Management Console

La Central Management Console Rapid Recovery est un composant facultatif destiné aux environnements ayant deux ou plusieurs Cores Rapid Recovery. Ce composant est un portail Web fournissant une interface centrale où vous pouvez grouper, gérer et générer les rapports de plusieurs Cores à l'aide d'une interface Web unique.

chiffrement

Les données sont chiffrées en vue de les rendre accessibles uniquement aux utilisateurs autorisés possédant la clé de chiffrement appropriée. Les données sont chiffrées avec AES 256-bits en mode CBC (Cipher Block Chaining). En mode CBC, chaque bloc des données en mettant XOR en relation avec le bloc de texte chiffré précédent avant le chiffrement, de façon à ce que chaque nouveau bloc de texte chiffré dépende de tous les blocs de texte brut antérieurs. Une phrase secrète sert de vecteur d'initialisation.

clé de licence

Une clé de licence est une méthode utilisée pour enregistrer votre logiciel ou votre appliance Rapid Recovery. (Vous pouvez également utiliser un fichier de licence.) Vous pouvez obtenir des clés de licence ou des fichiers en ouvrant un compte sur le Portail des licences Dell Data Protection | Rapid Recovery. Pour plus d'informations, voir le [Portail des licences](#).

cluster

Voir [Cluster de basculement Windows](#).

cluster à copie unique

Solution de cluster de basculement de stockage partagé qui utilise une copie unique d'un groupe de stockage situé dans un stockage partagé entre les nœuds du cluster. Il s'agit de l'un de deux types de déploiement de serveur de messagerie en cluster (CMS) disponibles dans Exchange 2007.

cluster de basculement Windows

Groupe de machines indépendantes qui fonctionnent conjointement pour augmenter la disponibilité des applications et des services. Les serveurs en cluster (appelés nœuds) sont connectés par des câbles physiques et par un logiciel. Si l'un des nœuds de cluster est défaillant, un autre nœud prend le relais (c'est le processus de basculement). Les utilisateurs subissent un minimum de perturbation dans le service. Rapid Recovery prend en charge la protection d'un certain nombre de types de clusters de serveurs SQL et Exchange.

cluster de serveurs

Voir [Cluster de basculement Windows](#).

compression

SNIA (Storage Networking Industry Association) définit la compression comme le processus de codage des données afin d'en réduire leur taille.

console Core

La console Core Rapid Recovery est une interface Web qui vous permet d'entièrement gérer le Core Rapid Recovery.

Core

Le Core Rapid Recovery Core constitue le composant central de l'architecture Rapid Recovery. Le core fournit les services essentiels pour la sauvegarde, la restauration, la rétention, la réplication, l'archivage et la gestion. Dans le contexte de la réplication, le Core s'appelle également le core source. Le Core source correspond au Core d'origine et le Core cible est la destination (un autre Core Rapid Recovery sur son propre serveur dédié, où les clusters ou les machines protégés sont répliqués).

Core cible

Le Core cible, appelé parfois réplique du Core, est le Core Rapid Recovery qui reçoit les données répliquées (points de restauration) depuis le Core source.

core distant

Un Core distant représente un Core Rapid Recovery auquel accède une machine non Core à l'aide de l'utilitaire de montage local ou de la Central Management Console.

database availability group (DAG)

Ensemble pouvant comprendre jusqu'à 16 serveurs de messagerie Microsoft Exchange Server 2010 qui fournissent au niveau de la base de données une récupération automatique de la base de données, du serveur ou du réseau défaillant. Les groupes DAG utilisent la réplication continue et un sous-ensemble de technologies en cluster de basculement Windows afin de fournir une haute disponibilité et une résilience de site. Les serveurs de messagerie dans un groupe DAG surveillent mutuellement leurs défaillances. Lorsque vous ajoutez un serveur de messagerie à un groupe DAG, il fonctionne avec d'autres serveurs dans le groupe pour pouvoir restaurer automatiquement les bases de données défaillantes.

déduplication globale

La SNIA (Storage Networking Industry Association) définit la déduplication de données comme le remplacement de plusieurs copies de données à plusieurs niveaux de références avec granularité vers une copie partagée pour sauvegarder un espace de stockage ou une bande passante. Le gestionnaire de volumes Rapid Recovery effectue une déduplication globale des données dans un volume logique. Le degré de granularité de déduplication est 8 Ko. L'étendue de la déduplication dans Rapid Recovery est limitée aux machines protégées utilisant la même logithèque et la même clé de chiffrement.

disque de secours virtuel

Le disque de secours virtuel est un processus qui crée une machine virtuelle clone d'une machine protégée. La machine source d'origine peut être physique ou virtuelle, mais le produit est toujours virtuel. Vous pouvez créer un disque de secours virtuel une fois sur demande, ou vous pouvez définir les exigences pour créer la machine virtuelle amorçable et la mettre à jour en permanence une fois chaque instantané capturé sur la machine protégée d'origine.

événement

Un événement est un processus qui est enregistré par le Core. Vous pouvez voir les événements dans la Core Console en cliquant sur



l'icône (Événements) de la barre d'icônes. Lorsque vous cliquez sur l'icône (Événements), la page **Tâches** s'affiche par défaut. Cette vue affiche les événements liés à une tâche. Vous pouvez voir les événements prioritaires dont vous êtes informé sur la page **Alertes**. Le journal de tous les événements s'affiche sur la page **Journal**. En configurant ou en modifiant des groupes de notification, vous pouvez personnaliser la notification de n'importe quel événement. Cette action donne la priorité à l'événement en l'affichant sur la page **Alertes**. Les membres d'un groupe de notification sont informés des événements à l'aide des méthodes de notification définies dans les options de notification du groupe.

expressions interdites

Les expressions interdites sont des expressions (ou associations de caractères) qui ne doivent pas être utilisées pour nommer un objet dans la console Core Rapid Recovery, parce qu'elles sont réservées à l'usage des systèmes d'exploitation. Il est recommandé de systématiquement éviter l'utilisation de ces expressions, lorsque c'est possible. Par exemple, lors du choix du nom d'affichage d'une machine protégée, il ne faut utiliser aucune des expressions suivantes :

Tableau 320. Expressions interdites

Expression	Utilisation générale	Interdit pour
con	console	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin
prn	port imprimante	nom d'affichage d'une machine, clé de chiffrement
aux	port auxiliaire	nom d'affichage d'une machine, clé de chiffrement
nul	valeur nulle	nom d'affichage d'une machine, clé de chiffrement
com1, com2 ... jusqu'à com9	port de communication	nom d'affichage d'une machine, clé de chiffrement
lpt1, lpt2... jusqu'à lpt9	port du terminal de	nom d'affichage d'une machine, clé de chiffrement, logithèque, description du chemin

Expression	Utilisation générale	Interdit pour
	l'imprimante en ligne	

Gestionnaire de volume

Le gestionnaire de volumes Rapid Recovery gère les objets, puis les stocke et les présente en tant que volume logique. Il tire parti de l'architecture en pipeline dynamique pour fournir l'évolutivité, le parallélisme et le modèle E/S de TruScale™ pour un haut débit et une latence E/S minimale.

image de base

Le premier transfert de sauvegarde enregistré sur le Core s'appelle l'instantané d'image de base. Toutes les données (le système d'exploitation, les applications et les paramètres) sont sauvegardés dans le core. Pour plus d'informations, voir [Instantanés](#).

implantation

Dans une réplication, il s'agit du transfert initial d'images de base dédoublées et des instantanés incrémentiels d'agents protégés, pouvant atteindre des centaines ou des milliers de gigaoctets de données. La réplication initiale peut être implantée dans le core cible à l'aide de supports externes. Cela est utile pour de grands ensembles de données ou les grands sites ayant une liaison lente.

Instantané

Un instantané est un terme commun à l'industrie qui définit la capacité à capturer et à stocker l'état d'un volume de disques à un moment donné, pendant l'exécution des applications. L'instantané est critique si la restauration du système est nécessaire suite à une coupure de courant ou à une panne du système. Les instantanés Rapid Recovery sont sensibles aux applications, ce qui signifie que toutes les transactions ouvertes et tous les journaux de transactions en cours se terminent et les caches se vident avant la création de l'instantané. Rapid Recovery utilise Microsoft VSS (Volume Shadow Services) pour faciliter la création d'instantanés créés au plantage des applications.

instantané incrémentiel

Les instantanés incrémentiels sont des sauvegardes constituées uniquement des données modifiées sur la machine protégée depuis la dernière sauvegarde. Ils sont sauvegardés sur le core de façon régulière, sur la base de l'intervalle défini (par exemple, toutes les 60 minutes). Pour plus d'informations, voir [Instantanés](#).

Live Recovery

Live Recovery de Rapid Recovery est une technologie de restauration instantanée pour les machines virtuelles ou les serveurs. Cette technologie fournit un accès quasi continu aux volumes de données dans un serveur virtuel ou physique, permettant la restauration d'un volume entier avec un RTO (temps de restauration) quasiment inexistant et un RPO (objectifs de point de restauration) de quelques minutes seulement.

Local Mount Utility

L'utilitaire LMU (Local Mount Utility) est une application téléchargeable qui permet de monter un point de restauration sur un Core Rapid Recovery distant depuis n'importe quelle machine.

logithèque

Une logithèque est une collection d'images de base et d'instantanés incrémentiels capturés depuis les machines protégées d'un Core Rapid Recovery. Les logithèques doivent être créées dans un dispositif de stockage principal rapide. L'emplacement de stockage d'une logithèque DVM peut être local pour le Core (dans ce cas, il est uniquement hébergé sur un système d'exploitation Windows pris en charge). Il peut utiliser un stockage à connexion directe, un réseau de zone de stockage, ou un serveur relié à un réseau et adéquat.

machine protégée

Une machine protégée, dénommée parfois « agent », est une machine physique ou virtuelle protégée par le Core Rapid Recovery. Les données de sauvegarde sont transmises depuis la machine protégée vers la logithèque spécifiée dans le Core à l'aide d'un intervalle de protection prédéfini. L'image de base transmet toutes les données à un point de restauration (celles-ci incluent le système d'exploitation, les applications et les paramètres). Chaque instantané incrémentiel suivant valide uniquement les blocs modifiés sur les

volumes du disque spécifié de la machine protégée. Les machines protégées basées sur les logiciels disposent d'un logiciel agent Rapid Recovery déjà installé. Certaines machines virtuelles peuvent aussi être protégées sans agent, avec certaines restrictions.

machines comportant uniquement des points de restauration

Une machine comportant uniquement des points de restauration est la représentation sur le Core des points de restauration provenant d'une machine qui a été préalablement protégée sur le Core et retirée depuis. Si vous supprimez une réplication tout en conservant les points de restauration, cela crée également une machine comportant uniquement des points de restauration. Les informations peuvent être affichées et récupérées à un niveau des fichiers. Vous ne pouvez pas utiliser une machine comportant uniquement des points de restauration pour effectuer des BMR ou restaurer des volumes entiers, ni ajouter davantage de données sur une machine comportant uniquement des points de restauration.

marque blanche

Rapid Recovery offre aux fournisseurs de services de sauvegarde et de récupération après sinistre la possibilité de proposer en marque blanche ou de renommer Rapid Recovery en utilisant leur propre identité, puis de le revendre ou le distribuer comme leur propre produit ou service.

montabilité

La montabilité d'Exchange est une fonction de détection de corruption qui alerte les administrateurs de pannes potentielles et vérifie que toutes les données sur les serveurs Exchange sont restaurées avec succès en cas de panne.

nœud de cluster

Machine individuelle qui fait partie d'un cluster de basculement Windows.

phrase secrète

Une phrase secrète est une clé qui est utilisée dans le chiffrement des données. Si vous perdez la phrase secrète, les données ne sont plus récupérables.

points de restauration

Les points de restauration forment une collection d'instantanés de divers volumes de disques. Par exemple : C:, D: et E:.

Portail des licences

Le Portail des licences Dell Data Protection | Rapid Recovery est une interface Web où les utilisateurs et partenaires peuvent télécharger des logiciels, inscrire des appliances Rapid Recovery et gérer les abonnements aux licences. Depuis le portail des licences, les utilisateurs peuvent enregistrer leurs comptes, télécharger les logiciels Core et Agent Rapid Recovery, administrer des groupes, suivre l'activité des groupes, enregistrer des machines et des appliances, inviter des utilisateurs et générer des rapports. Pour plus d'informations, voir le Guide *Portail des licences Dell Data Protection | Rapid Recovery*.

PowerShell Scripting

Windows PowerShell est un environnement connecté Microsoft .NET Framework conçu pour l'automatisation administrative. Rapid Recovery comprend des kits de développement logiciels clients complets pour l'exécution de scripts PowerShell permettant aux administrateurs d'automatiser l'administration et la gestion des ressources Rapid Recovery en exécutant des commandes directement ou via des scripts.

quorum

Pour un cluster de basculement, il s'agit du nombre d'éléments devant se trouver en ligne pour qu'un cluster puisse continuer à fonctionner. Les éléments pertinents dans ce contexte sont des nœuds de cluster. Ce terme peut également faire référence aux ressources de quorum sélectionnées pour conserver les données de configuration nécessaires à la restauration du cluster. Ces données contiennent les détails de toutes les modifications qui ont été apportées à la base de données de cluster. Les ressources de quorum sont généralement accessibles à d'autres ressources de cluster de manière qu'un nœud de cluster ait accès aux dernières modifications de la bases de données. Par défaut, il existe une seule ressource de quorum par cluster de serveur. Une configuration de quorum particulière (paramètres de cluster de basculement) détermine le point à partir duquel un trop grand nombre de défaillances arrête le fonctionnement du cluster.

Rapid Recovery

Rapid Recovery établit un nouveau standard en matière de protection unifiée des données en combinant la sauvegarde, la réplication et la restauration dans une même solution réputée la plus fiable et la plus rapide pour protéger les machines virtuelles (VM), ainsi que les environnements physiques et Cloud.

réplication

La réplication est le processus qui consiste à copier des points de restauration depuis un Core Rapid Recovery et de les transmettre à un autre Core Rapid Recovery en vue de les récupérer après sinistre. Le processus exige une relation d'appariement source-cible entre deux Cores ou plus. La réplication est gérée en fonction des machines protégées. Toute machine (ou toutes les machines) protégée ou répliquée sur un Core source peut être configurée pour être répliquée vers un Core cible. Ce sont les points de restauration qui sont copiés vers le Core cible.

réplication de cluster continue (CCR)

Solution de cluster de basculement non partagée qui utilise une technologie d'envoi asynchrone intégrée pour créer et conserver une copie de chaque groupe de stockage sur un second serveur dans un cluster de basculement. CCR est une solution à un ou deux centres de données offrant à la fois une haute disponibilité et une résilience du site. Il s'agit de l'un de deux types de déploiement de serveur de messagerie en cluster (CMS) disponible dans Exchange 2007.

restauration

Le processus consistant à restaurer un ou plusieurs volumes de stockage sur une machine à partir des points de restauration sauvegardés sur le Core Rapid Recovery porte le nom d'opération de restauration. Précédemment, le terme anglais de « rollback » a également été utilisé pour désigner cette opération.

rétenition

La rétenition définit la période pendant laquelle les instantanés de sauvegarde des machines protégées sont stockés dans le Core Rapid Recovery. La stratégie de rétenition s'applique aux points de restauration par l'intermédiaire du processus de consolidation.

rôles d'administration

La Central Management Console de Rapid Recovery présente un nouveau concept de rôles d'administration qui permet de partager la responsabilité des tâches administratives entre des administrateurs de service et de données de confiance. Elle prend également en charge le contrôle d'accès pour assurer une délégation et une administration efficace et sécurisée.

rollup

Le processus de consolidation est une procédure de maintenance nocturne qui applique la stratégie de rétenition en réduisant et en éliminant les points de restauration obsolètes. Rapid Recovery réduit les opérations de consolidation aux métadonnées uniquement.

sauvegarde différentielle SQL

La sauvegarde différentielle d'une base de données est une copie regroupant toutes les modifications apportées aux données depuis la dernière sauvegarde complète de la base de données SQL. Les sauvegardes différentielles sont généralement plus rapides à créer que les sauvegardes complètes de la base de données, et elles réduisent le nombre de journaux des transactions nécessaires pour récupérer la base de données.

Sauvegarde SharePoint

Une sauvegarde SharePoint est une copie de données utilisée pour restaurer ou récupérer ces données sur un serveur SharePoint après une panne système. À partir de la sauvegarde SharePoint, vous pouvez choisir d'effectuer une récupération complète de la ferme SharePoint, ou une récupération d'un ou plusieurs éléments constitutifs de la ferme.

sauvegarde SQL

Une sauvegarde SQL est une copie de données utilisée pour restaurer ou récupérer ces données sur un serveur SQL après une panne système. À partir de la sauvegarde SQL, vous pouvez choisir d'effectuer une récupération complète de la base de données SQL, ou une récupération d'un ou plusieurs éléments constitutifs de la base de données.

Smart Agent

Le Smart Agent Rapid Recovery s'installe sur les machines protégées par le Core Rapid Recovery. Smart Agent suit les blocs modifiés sur le volume de disque et crée des instantanés des blocs modifiés à une fréquence prédéfinie de protection.

somme de contrôle

Une somme de contrôle est une fonction qui crée des blocs de données servant à détecter des erreurs accidentelles qui sont créées pendant la transmission ou le stockage.

Système de fichiers objet

Le Scalable Object Store de Rapid Recovery est un composant du système de fichiers objet. Il traite tous les blocs de données dont sont issus les instantanés en tant qu'objets. Il stocke, récupère, conserve et réplique ces objets. Il fournit des performances d'entrée/sortie évolutives en conjonction avec déduplication globale des données, le chiffrement et la gestion de la rétention. Le système de fichiers objet communique directement avec les technologies de stockage standard du secteur.

Transport Layer Security

Transport Layer Security (TLS) est un protocole réseau cryptographique actuel qui protège les communications sur Internet. Ce protocole, défini par l'Internet Engineering Task Force (IETF), est le successeur de Secure Sockets Layer (SSL). Le terme SSL est toujours largement utilisé, et les protocoles sont interchangeableables (un client TLS peut être rétrogradé pour pouvoir communiquer avec un serveur SSL).

troncature de journal

La troncature de journal est une fonction qui supprime des enregistrements du journal des transactions. Pour une machine SQL Server, le forçage de la troncature des journaux SQL Server identifie l'espace libre sur le serveur SQL. Pour une machine Exchange Server, vous pouvez forcer la troncature des journaux Exchange Server, ce qui libère de l'espace sur un serveur Exchange.

True Scale

TrueScale est l'architecture évolutive de Rapid Recovery.

Universal Recovery

La technologie Universal Recovery de Rapid Recovery offre une flexibilité illimitée de restauration des machines. Elle permet d'effectuer une restauration monolithique vers et depuis toute plate-forme physique et virtuelle de votre choix, ainsi que des mises à jour de restauration incrémentielle vers des machines virtuelles à partir de n'importe quelle source physique ou virtuelle. Elle vous permet également d'effectuer une restauration de fichiers individuels, des dossiers, des e-mails, des éléments de calendrier, des bases de données et des applications, au niveau des applications, des éléments et des objets.

Verified Recovery

La technologie Verified Recovery permet d'effectuer des tests de restauration et des vérifications automatiques des sauvegardes. Elle prend en charge divers systèmes de fichiers et serveurs.