Appliance Dell DL4300
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.

2015 - 12

Rév. A01

Table des matières

1

Présentation de l'appliance Dell DL4300

Ce chapitre fournit une présentation et un aperçu de DL4300. Il décrit les fonctions, les fonctionnalités et l'architecture et il couvre les sujets suivants :

- Technologies de base
- Architecture True Scale
- Architecture de déploiement
- Caractéristiques du produit

Votre appliance définit une nouvelle norme de protection unifiée des données en combinant la sauvegarde, la réplication et la restauration en une solution unique conçue pour être la méthode de sauvegarde la plus rapide et la plus fiable pour la protection des machines virtuelles (VM) et physiques ainsi que des environnements informatiques.

Votre appliance peut gérer jusqu'à des péta-octets de données avec la déduplication globale intégrée, la compression, le chiffrement et la réplication vers toute infrastructure de cloud privé ou public. Les applications et données des serveurs peuvent être restaurées en quelques minutes pour la rétention et la conformité des données (DR).

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

Votre appliance combine les technologies suivantes :

- Live Recovery
- Verified Recovery
- Universal Recovery
- Déduplication globale réelle

Ces technologies sont conçues pour une intégration sécurisée à des fins de restauration après sinistre dans le cloud et de restauration fiable et rapide. Grâce à son magasin d'objets évolutif, votre appliance est particulièrement capable de gérer jusqu'à des péta-octets de données très rapidement avec la déduplication globale intégrée, la compression, le chiffrement et la réplication vers toute infrastructure de cloud privé ou public.

AppAssure traite le problème d'inefficacité et de complexité des outils hérités grâce à sa technologie de base et à la prise en charge d'environnements multi-hyperviseurs notamment ceux qui s'exécutent sur VMware vSphere et Microsoft Hyper-V, qui comprennent tant des clouds privés que des clouds publics. AppAssure offre ces technologies de pointe tout en réduisant de façon significative les coûts de stockage et de gestion informatique.

Technologies de base

Les rubriques suivantes contiennent des informations sur les technologies de base AppAssure.

Live Recovery

Live Recovery (Restauration en direct) est une technologie de restauration instantanée des VM ou serveurs. Elle vous donne un accès quasi continu aux volumes de données sur des serveurs virtuels ou physiques. Vous pouvez restaurer la totalité d'un volume avec des valeurs RTO pratiquement égales à zéro et un RPO en minutes.

La technologie de réplication et de sauvegarde enregistre des instantanés simultanés de plusieurs VM ou serveurs, offrant une protection quasi-instantanée des données et des systèmes. Vous pouvez reprendre l'utilisation du serveur directement depuis le fichier de sauvegarde sans attendre une restauration complète sur le stockage de production. Les utilisateurs maintiennent leur productivité et les services IT réduisent leurs délais de restauration pour satisfaire aux accords de niveau de service RTO (Recovery Time Objective, Objectif de temps de restauration) et RPO (Recovery Point Objective, Objectif de point de renaturation) actuels toujours plus rigoureux.

Verified Recovery

L'utilitaire Verified Recovery vous permet d'effectuer automatiquement des tests de restauration et la vérification des sauvegardes. Ceci inclut, sans s'y limiter, les systèmes de fichiers, Microsoft Exchange 2007, 2010 et 2013, ainsi que différentes versions de Microsoft SQL Server 2005, 2008, 2008 R2, 2012 et 2014. Verified Recovery permet la restauration des applications et des sauvegardes dans des environnements virtuels et physiques. Il inclut un algorithme complet de vérification de l'intégrité basé sur des clés SHA 256 bits qui contrôlent que chaque bloc de disque est correct dans la sauvegarde pendant l'archivage, la réplication et la génération des données de départ. Cela garantit que la corruption des données est identifiée très tôt et empêche le maintien ou le transfert de blocs de données corrompus pendant le processus de sauvegarde.

Universal Recovery

La technologie Universal Recovery vous offre une flexibilité de restauration d'ordinateur illimitée. Vous pouvez restaurer vos sauvegardes depuis des systèmes physiques vers des machines virtuelles, de machine virtuelle à machine virtuelle, de machine virtuelle à système physique ou de système physique à système physique et effectuer des restaurations sans système d'exploitation sur du matériel différent. Par exemple, P2V, V2V, V2P, P2P, P2C, V2C, C2P et C2V.

La technologie Universal Recovery accélère aussi les déplacements sur plusieurs plateformes parmi les machines virtuelles. Par exemple, le déplacement de VMware à Hyper-V ou de Hyper-V à VMware. Universal Recovery effectue des constructions dans des restaurations au niveau de l'application, au niveau de l'élément et au niveau de l'objet (fichiers, dossier, e-mail, éléments de calendrier, bases de données et applications individuels). Avec AppAssure, vous pouvez restaurer ou exporter de physique à cloud ou de virtuel à cloud.

Déduplication globale réelle

Votre appliance offre une fonction de déduplication réellement globale qui réduit les exigences de capacité du disque physique en proposant des ratios de réduction de l'espace excédant 50:1, tout en continuant à satisfaire aux exigences de stockage des données. La compression au niveau du bloc inline

d'AppAssure True Scale et les performances de déduplication de vitesse de ligne, alliées aux vérifications d'intégrité intégrées, empêchent la corruption des données d'affecter la qualité des processus de sauvegarde et d'archivage.

Architecture True Scale

Votre appliance repose sur l'architecture AppAssure True Scale. Elle tire parti de cette architecture dynamique de canaux à plusieurs cores, optimisée pour offrir en continu des performances robustes pour vos environnements d'entreprise. True Scale est conçu de toutes pièces pour une évolutivité linéaire, et pour le stockage et la gestion efficaces de grands volumes de données. Cette architecture offre des RTO et RPO de quelques minutes sans nuire aux performances. Elle comprend un objet prévu à cet effet et un gestionnaire de volume, qui intègre la déduplication globale, la compression, le cryptage, la réplication et la rétention. Le diagramme suivant décrit l'architecture AppAssure True Scale.

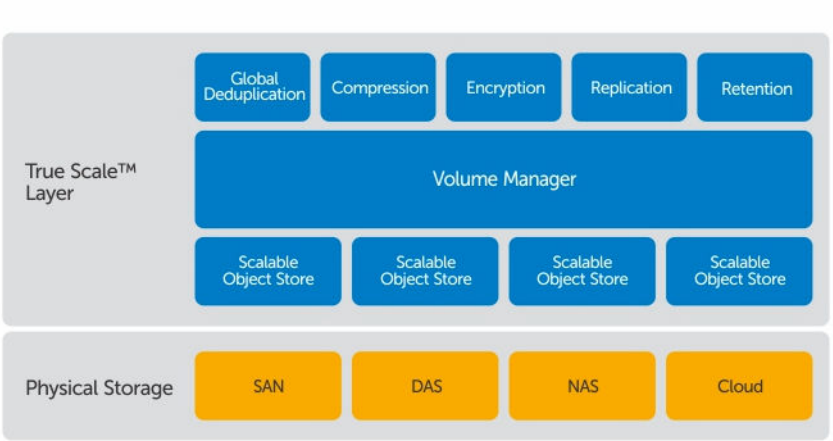


Figure 1. Architecture AppAssure True Scale

AppAssure Volume Manager et un magasin d'objets évolutif servent de base à l'architecture AppAssure True Scale. Le magasin d'objets évolutif stocke des instantanés au niveau du bloc qui sont capturés à partir de serveurs virtuels et physiques. Le Gestionnaire de volumes gère les nombreux magasins d'objets, en fournissant un référentiel commun ou un stockage « juste à temps » adapté aux besoins. Le magasin d'objets prend tout en charge simultanément avec des E/S asynchrones qui offrent un haut débit avec une latence minimale et optimisent l'utilisation du système. Le référentiel réside sur différentes technologies de stockage telles que SAN (Storage Area Network), DAS(Direct Attached Storage) ou NAS (Network Attached Storage).

Le gestionnaire de volumes AppAssure joue un rôle semblable à celui du gestionnaire de volumes d'un système d'exploitation. Il regroupe divers périphériques de stockage, parfois de tailles et de types différents, et les combine pour former des volumes logiques à l'aide de stratégies d'allocation en bandes ou séquentielle. La banque d'objets enregistre, récupère les objets dérivés d'instantanés avec reconnaissance de l'application, en assure la maintenance, puis les réplique. Le gestionnaire de volumes offre des performances d'E/S évolutives alliées à la déduplication globale des données, au cryptage et à la gestion de la rétention.

Architecture de déploiement

Votre appliance est un produit de sauvegarde et de restauration évolutif qui se déploie souplement 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.

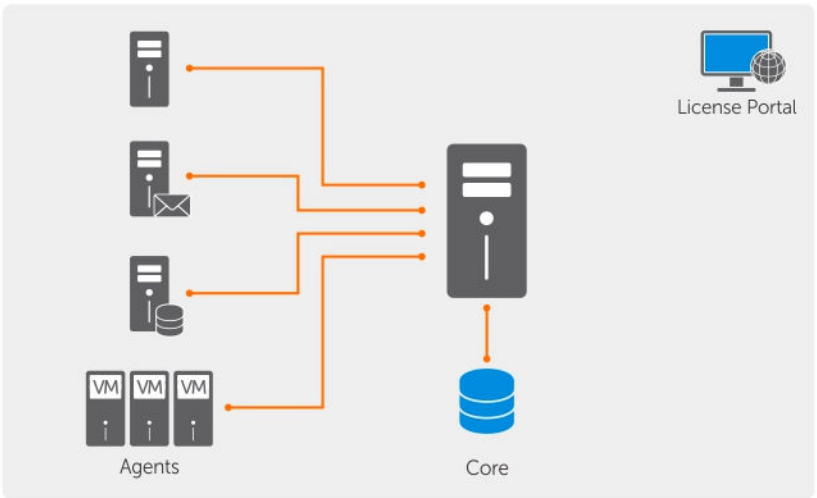


Figure 2. Architecture de déploiement de base

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

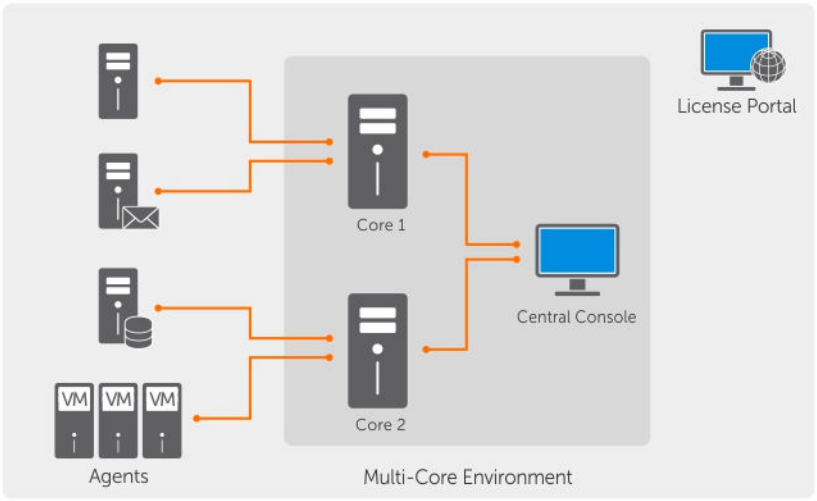


Figure 3. Architecture de déploiement avec plusieurs Cores

Smart Agent

Smart Agent effectue le suivi des modifications apportées aux blocs du volume de disque, puis prend un instantané des blocs modifiés selon l'intervalle de protection prédéfini. L'approche qui consiste à créer systématiquement des instantanés de niveau bloc empêche la copie répétée des mêmes données depuis la machine protégée vers le Core. Le Smart Agent s'installe sur les machines devant être protégées par le Core.

Le Smart Agent reconnaît l'application et reste dormant s'il n'est pas utilisé, avec une consommation d'UC proche de zéro (0) % d'UC et moins de 20 Mo de consommation de mémoire. Lorsque le Smart Agent est actif, il utilise de 2 à 4 % d'utilisation des ressources du processeur et moins de 150 Mo de mémoire, y compris lors du transfert des instantanés vers le Core.

Le Smart Agent reconnaît les applications car il détecte le type de l'application installée et l'emplacement des données. Il regroupe automatiquement les volumes de données avec dépendance, telles que les bases de données, puis les interconnecte pour assurer une protection efficace et une restauration rapide. Une fois configuré, l'agent utilise une technologie intelligente pour faire le suivi des blocs modifiés sur les volumes de disque protégés. Lorsque l'instantané est prêt, il est rapidement transféré au Core à l'aide de connexions socket multithreads intelligentes. Pour conserver la bande passante de l'UC et la mémoire sur les machines protégées, le smart agent ne crypte pas et ne déduplique pas les données à la source et les machines protégées sont associées à un Core à des fins de protection.

DL4300

Le Core est le composant central de l'architecture de déploiement. Le Core stocke et gère toutes les sauvegardes de la machine, et fournit des services de base de sauvegarde, restauration et rétention, réplication, archivage et gestion. Le Core est un ordinateur autonome adressable sur le réseau exécutant une version 64 bits du système d'exploitation Microsoft Windows. Votre matériel réalise en ligne sur la base de la cible à la compression, le cryptage et la déduplication des données reçues depuis la machine protégée. Le Core stocke alors les sauvegardes des instantanés dans les référentiels, tels que SAN (Storage Area Network) ou 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://CORENAME:8006/apprecovery/admin**. En interne, tous les services de core sont accessibles par l'intermédiaire des APIREST. Vous pouvez accéder aux services du core depuis le core ou directement sur Internet à partir de toute application qui peut envoyer une demande HTTP/HTTPS et recevoir une réponse HTTP/HTTPS. Toutes les opérations API s'effectuent sur 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 depuis une machine protégée vers le Core. Ceci est le seul moment où une copie complète de la machine est transportée sur le réseau dans des conditions normales de fonctionnement, suivie d'instantanés incrémentiels. Le logiciel AppAssure Agent pour Windows utilise Microsoft VSS (Volume Shadow copy Service) pour figer et suspendre les données d'application sur le disque, afin de capturer un système de fichiers cohérent et une sauvegarde cohérente avec l'application. Lors de la création d'un instantané, l'enregistreur VSS, et le rédacteur sur le serveur cible empêchent l'écriture du contenu sur le disque. Lorsque l'écriture du contenu sur le disque est arrêtée, toutes les opérations d'E/S sur disque sont mises en file d'attente et reprennent uniquement lorsque l'instantané est terminé, tandis que les opérations déjà en cours sont terminées et que tous les fichiers ouverts sont fermés. Le processus de création du cliché instantané n'a aucun impact significatif sur les performances du système de production.

AppAssure utilise Microsoft VSS car il inclut une prise en charge intégrée de toutes les technologies internes à Windows, notamment le NTFS, le registre, Active Directory, etc., pour vider les données sur disque avant de créer l'instantané. De plus, d'autres applications d'entreprise, comme Microsoft Exchange et SQL, utilisent des plug-ins de processus d'écriture VSS pour recevoir une notification lorsqu'un instantané est préparé et lorsqu'il faut vider ses pages de base de données utilisées sur disque pour placer la base de données dans un état de transaction cohérent. Il est important de bien noter que VSS sert à figer les données du système et des applications sur le disque, mais pas à créer l'instantané. Les données capturées sont rapidement transférées vers le Core, où elles sont stockées. L'utilisation de VSS pour la sauvegarde ne met pas le serveur d'applications en mode Sauvegarde très longtemps, car la durée nécessaire pour exécuter l'instantané se mesure en secondes, pas en heures. Autre avantage de l'utilisation de VSS pour la sauvegarde : cela permet de prendre un instantané de grandes quantités de données en une seule opération, car l'instantané fonctionne au niveau du volume.

Réplication de site de récupération après sinistre ou fournisseur de services

Le processus de réplication exige une relation source-cible associés 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
- True Global Deduplication (Fonctions)
- Cryptage
- Réplication
- RaaS (Restauration en tant que service)
- Rétention et archivage
- Virtualisation et cloud
- Alertes et gestion des événements
- Portail de licences
- Console Web
- API de gestion des services

Référentiel

Le référentiel utilise le DVM (Deduplication Volume Manager ou Gestionnaire de volumes de déduplication) pour implémenter un gestionnaire de volumes qui fournit une prise en charge de plusieurs volumes qui pourraient résider individuellement sur différentes technologies de stockage telles que Storage Area Network (SAN), Direct Attached Storage (DAS), Network Attached Storage (NAS) ou le stockage cloud. Chaque volume est composé d'un stockage d'objet évolutif avec une déduplication. Le stockage d'objet évolutif se comporte comme un système de fichiers basé sur des enregistrements, où l'unité d'allocation de stockage est un bloc de données à taille fixe appelé un enregistrement. Cette architecture vous permet de configurer un support en bloc pour la compression et la déduplication. Les opérations cumulatives sont réduites d'opérations intensives de disque à des opérations de métadonnées car le cumul ne déplace plus les données mais déplace uniquement les enregistrements.

Le DVM peut combiner un ensemble de stockage d'objets dans un volume et vous pouvez développer ceux-ci en créant des systèmes de fichiers supplémentaires. Les fichiers de stockage d'objets sont préalloués et peuvent être ajoutés sur demande à mesure que les exigences de stockage changent. Il est possible de créer jusqu'à 255 référentiels indépendants sur un Core unique et d'augmenter davantage la taille du référentiel en ajoutant de nouvelles extensions de fichier. Un référentiel étendu peut contenir un maximum de 4 096 extensions s'étendant sur différentes technologies de stockage. La taille maximale d'un référentiel est de 32 Exaoctects. Plusieurs référentiels peuvent exister sur un core unique.

Déduplication globale réelle

La déduplication globale réelle est une méthode permettant de réduire efficacement les besoins de stockage des sauvegardes, en éliminant les données redondantes ou en double. La déduplication est

efficace car le programme stocke dans le référentiel une instance unique des données pour plusieurs sauvegardes. Les données redondantes sont stockées, mais pas physiquement ; elles sont remplacées par un pointeur vers l'instance unique stockée dans le référentiel.

Les applications de sauvegarde conventionnelles effectuent des sauvegardes complètes répétitives chaque semaine, mais votre appliance exécute des sauvegardes incrémentielles des machines, au niveau du bloc. Cette approche « incrémentielle à jamais », associée à la déduplication des données, vous aide à réduire de façon significative la quantité totale de données validée sur le disque.

La disposition de disque typique d'un serveur comporte le système d'exploitation, l'application et les données. Dans la plupart des environnements, les administrateurs utilisent souvent une installation commune du système d'exploitation serveur et poste de travail sur plusieurs systèmes, pour un déploiement et une gestion plus efficaces. Lorsque la sauvegarde est réalisée au niveau du bloc sur plusieurs machines au même moment, vous obtenez une vue plus détaillée des éléments figurant dans la sauvegarde et de ceux qui n'y sont pas, quelle que soit la source. Ces données incluent le système d'exploitation, les applications et les données d'application pour l'ensemble de l'environnement.

Figure 4. Diagramme de déduplication

Votre appliance exécute une déduplication des données incorporée (inline) basée sur la cible : les données d'instantané sont transmises au Core avant leur déduplication. La déduplication des données incorporée signifie que les données sont dédupliquées avant leur validation sur disque. C'est très différent de la déduplication à la source (les données sont dédupliquées à la source avant leur transmission à la cible pour stockage) ou de la déduplication après traitement (les données sont envoyées brutes à la cible, où elles sont analysées et dédupliquées après leur validation sur disque). La déduplication à la source consomme de précieuses ressources système sur la machine, alors que la déduplication après traitement exige que toutes les données nécessaires se trouvent sur le disque (surcharge initiale de capacité plus importante) avant le lancement du processus de déduplication. D'autre part, la déduplication de données incorporée n'exige aucune capacité de disque ni aucun cycle d'UC supplémentaire sur la source ou sur le Core. Enfin, les applications de sauvegarde traditionnelles effectuent des sauvegardes complètes répétitives, toutes les semaines, alors que votre appliance exécute des sauvegardes incrémentielles des machines au niveau du bloc, à perpétuité. Cette approche incrémentielle en continu, alliée à la déduplication des données vous aide à réduire de façon significative la quantité totale de données validée sur le disque ; le taux de réduction peut atteindre 50:1.

Cryptage

Votre appliance fournit un cryptage intégré qui protège les sauvegardes et les données au repos de tout accès ou utilisation non autorisé, ce qui garantit la confidentialité des données. Seul un utilisateur qui dispose de la clé de cryptage peut accéder aux données et les décrypter. Il n'existe aucune limite au nombre de clés de cryptage qu'il est possible de créer et de stocker sur un système. DVM utilise le cryptage AES 256 bits en mode CBC (Cipher Block Chaining, chaînage des blocs de cryptage) avec des clés de 256 bits. Le cryptage est incorporé (inline) sur les données d'instantané, à haut débit, sans aucun impact sur les performances. En effet, l'implémentation de DVM est multithread et utilise l'accélération matérielle propre au processeur où il est déployé.

Le cryptage est prêt pour plusieurs locataires. La déduplication a été spécifiquement limitée aux enregistrements cryptés avec la même clé. Ainsi, deux enregistrements identiques cryptés avec des clés différentes ne sont pas dédupliqués l'un par rapport à l'autre. Cette optique de conception garantit que la déduplication ne peut pas servir à la fuite de données d'un domaine de cryptage à un autre. C'est un avantage pour les fournisseurs de services gérés (MSP), car il est possible de stocker les sauvegardes répliquées pour plusieurs locataires (clients) sur un seul core sans qu'un locataire puisse afficher les données d'un autre, ni y accéder. Chaque clé de cryptage de locataire active crée un domaine de cryptage dans l'espace de stockage, où seul le propriétaire des clés peut afficher les données, y accéder ou les utiliser. Dans un scénario multilocataire, les données sont partitionnées et dédupliquées dans les domaines de cryptage.

Dans les scénarios de réplication, votre appliance utilise SSL 3.0 pour sécuriser les connexions entre les deux cores d'une topologie de réplication afin de prévenir les indiscrétions et les modifications non autorisées.

Réplication

La réplication est le processus qui consiste à copier des points de restauration depuis un core AppAssure et à les transmettre à un autre core AppAssure dans un emplacement séparé en vue de récupération après sinistre. Ce processus requiert une relation source-cible en couple entre deux cores ou plus.

Le core source copie les points de restauration des machines protégées sélectionnées, puis transmet de manière asynchrone et continue les données d'instantané incrémentielles au core cible sur un site distant de reprise après sinistre. Vous pouvez configurer la réplication sortante vers un centre de données appartenant à la société ou dans un site de récupération après sinistre distant (à savoir, un core cible autogéré). Ou bien, vous pouvez configurer la réplication sortante vers un fournisseur tiers de services gérés (MSP) ou encore le Cloud qui héberge la sauvegarde hors site et les services de reprise après sinistre. Lors de la réplication d'un core cible tiers, vous pouvez utiliser les workflows intégrés, qui vous permettent de demander des connexions et de recevoir des notifications automatiques de rétroinformation.

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 se répliquer vers un core cible.

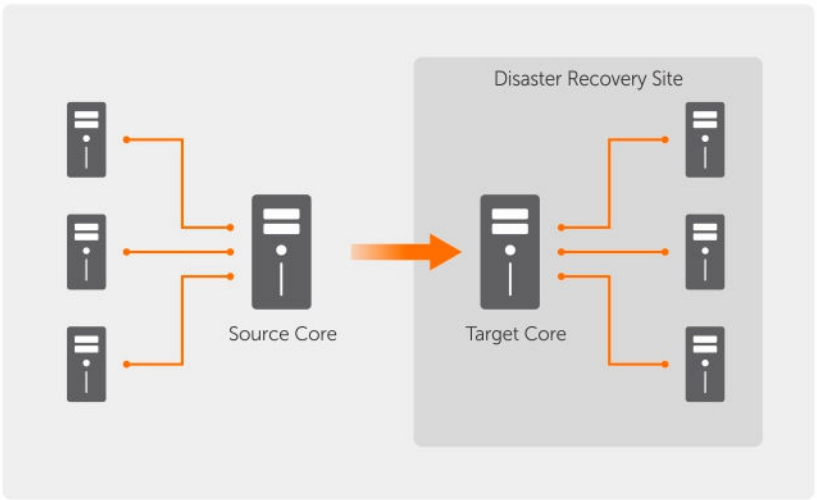


Figure 5. Architecture de réplication de base

La réplication s'optimise automatiquement grâce à un algorithme unique (RMW -Read-Match-Write) Lecture-Correspondance-Écriture étroitement associé à la déplication. Au moyen de la réplication RMW, le service de réplication source et cible établit la correspondance des clés avant le transfert de données, puis ne fait la réplique que des données compressées, chiffrées et dédupliquées sur le réseau étendu WAN, ce qui réduit de 10 x les besoins en bande passante.

La réplication commence par l'implantation (seeding), c'est-à-dire le transfert initial des images de base dédupliquées et les instantanés incrémentiels des machines protégées. Les données peuvent représenter des centaines ou des milliers de gigaoctets. La réplication initiale peut être implantée dans le core cible à l'aide de supports externes. Ceci est utile pour les ensembles de données volumineux ou les sites avec des liaisons lentes. Les données de l'archive d'amorçage sont compressées, cryptées et dédupliquées. Si la taille totale de l'archive est supérieure à l'espace disponible sur le support externe, l'archive peut être répartie sur plusieurs périphériques. Au cours du processus de départ, les points de restauration incrémentielle sont répliqués sur le site cible. Une fois que les données ont été transférées vers le core cible, les points de restauration incrémentiels récemment répliqués se synchronisent automatiquement.

RaaS (Restauration en tant que service)

Les MSP (Managed Service Providers - Fournisseurs de services gérés) peuvent tirer profit de l'appliance en tant que plateforme de RaaS (Fourniture de restauration en tant que service). RaaS facilite les restaurations complètes dans le cloud en répliquant les serveurs physiques et virtuels des clients, ainsi que leurs données, sur le cloud du fournisseur de service en tant que machines virtuelles pour prendre en charge les tests de restauration ou les opérations de restauration. Les clients qui souhaitent effectuer une restauration dans le cloud peuvent configurer la réplication sur leurs machines protégées sur les cores locaux sur un fournisseur de services AppAssure. En cas de sinistre, les MSP peuvent immédiatement accélérer les machines virtuelles du client.

Les MSP peuvent déployer l'infrastructure RaaS AppAssure multi-locataires, qui peut héberger plusieurs organisations ou unités d'entreprise (les locataires) discrètes qui ne partagent pas normalement la sécurité ou les données sur un serveur unique ou un groupe de serveurs. Les données de chaque locataire sont isolées et sécurisées de la vue des autres locataires et du fournisseur de services.

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.

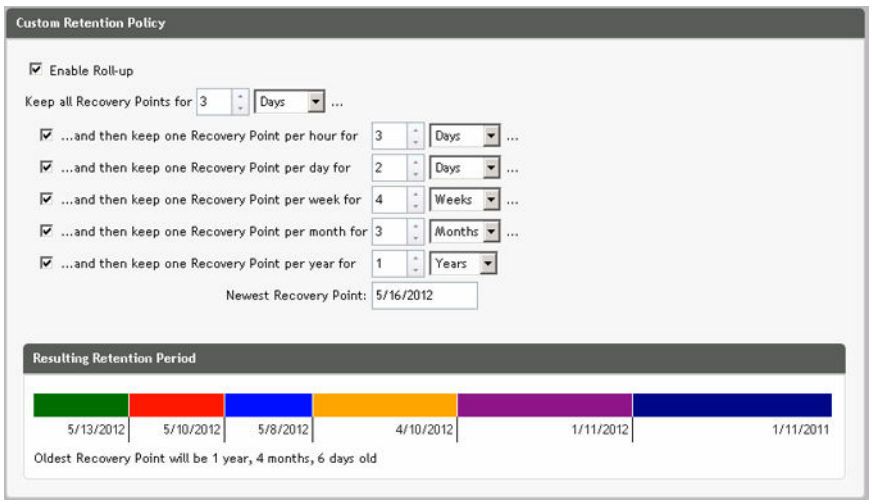


Figure 6. Stratégie de rétention personnalisée

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 Enterprise 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.

2

Travailler avec le Core DL4300

Accès à la Core Console DL4300

Pour accéder à la Core Console :

1. Mettez à jour les sites de confiance dans votre navigateur. Reportez-vous à la rubrique Mise à jour des sites de confiance dans Internet Explorer.
2. Configurez le navigateur pour accéder à distance à la Core Console. Voir Configuration des navigateurs pour accéder à distance à la Core Console .
3. Effectuez l'une des tâches suivantes pour accéder à la Core Console :
   - Connectez-vous localement au serveur DL4300, puis double-cliquez sur l'icône **Core Console**.
   - Saisissez une des URL suivantes dans votre navigateur Web :
     - **https://<NomDeVotreServeurCore>:8006/apprecovery/admin/core ou**
     - **https://<AdresseIPDeVotreServeurCore>:8006/apprecovery/admin/core**

Mise à jour des sites de confiance dans Internet Explorer

Pour mettre à jour les sites de confiance dans Microsoft Internet Explorer :

1. Ouvrez Internet Explorer.
2. Si les menus **Fichier**, **Modifier la vue** et autres ne sont pas affichés, appuyez sur <F10>.
3. Cliquez sur le menu **Outils** et sélectionnez **Options Internet**.
4. Dans la fenêtre **Options Internet**, cliquez sur l'onglet **Sécurité**.
5. Cliquez sur **Sites de confiance** et cliquez sur **Sites**.
6. Dans **Ajouter ce site Web à la zone**, saisissez **https://[Nom d'affichage]** et utilisez le nouveau nom que vous avez fourni pour le nom d'affichage.
7. Cliquez sur **Add** (Ajouter).
8. Sous **Ajouter ce site Web à la zone**, entrez **about:blank**.
9. Cliquez sur **Add** (Ajouter).
10. Cliquez sur **Fermer**, puis sur **OK**.

Configuration des navigateurs pour accéder à distance à Core Console

Pour accéder à Core Console depuis une machine distante, vous devez modifier les paramètres de votre navigateur.

REMARQUE : Pour ce faire, connectez-vous au système en tant qu'administrateur.

REMARQUE : Google Chrome utilise les paramètres Microsoft Internet Explorer. Modifiez les paramètres du navigateur Chrome à l'aide d'Internet Explorer.

REMARQUE : Veillez à activer la **configuration de sécurité renforcée d'Internet Explorer** lorsque vous accédez à Core web Console localement ou à distance. Pour activer la **configuration de sécurité renforcée d'Internet Explorer** :

1. Ouvrez le **Gestionnaire de serveur**.
2. Sélectionnez **Configuration de sécurité renforcée d'Internet Explorer du serveur local** sur la droite. Vérifiez que la fonction est **activée**.

Modification des paramètres de navigateur dans Internet Explorer et Chrome

Pour modifier les paramètres de navigateur dans Internet Explorer et Chrome :

1. Ouvrez Internet Explorer.
2. Dans le menu **Outils** , sélectionnez **Options Internet**, onglet **Sécurité**.
3. Cliquez sur **Sites de confiance** et cliquez sur **Sites**.
4. Désélectionnez l'option **Exiger la vérification du serveur (https) pour tous les sites de cette zone**, puis ajoutez http://<*nom d'hôte ou adresse IP du serveur de l'Appliance hébergeant AppAssure Core*> à la zone **Sites de confiance**.
5. Cliquez sur **Fermer**, sélectionnez **Sites de confiance**, puis cliquez sur **Personnaliser le niveau**.
6. Faites défiler l'affichage jusqu'à **Divers → Affiche un contenu mixte** et sélectionnez **Activer**.
7. Faite défiler l'affichage jusqu'au bas de l'écran vers l'entrée **Authentification utilisateur → Ouverture de session**, puis sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuel**.
8. Cliquez sur **OK**, puis sélectionnez l'onglet **Avancé**.
9. Faites défiler la liste jusqu'à **Multimédia**, puis sélectionnez **Lire les animations dans les pages Web**.
10. Faites défiler l'écran jusqu'à **Sécurité**, sélectionnez **Activer l'authentification Windows intégrée**, puis cliquez sur **OK**.

Configuration des paramètres du navigateur Mozilla Firefox

REMARQUE : Pour modifier les paramètres du navigateur Mozilla Firefox dans les dernières versions de Firefox, désactivez la protection. Cliquez avec le bouton droit sur le bouton Identifier un site (situé à gauche de l'URL), accédez à **Options**, puis cliquez sur **Désactiver la protection pour l'instant**.

Pour modifier les paramètres du navigateur Mozilla Firefox :

1. Dans la barre d'adresse de Firefox, entrez **about:config**, puis, à l'invite, cliquez sur **Je ferai attention, promis**.
2. Recherchez le terme **ntlm**.

   La recherche doit renvoyer au moins trois résultats.
3. Double-cliquez sur **network.automatic-ntlm-auth.trusted-uris** et entrez les paramètres suivants, en fonction de votre machine :
   - Pour les machines locales, entrez le nom d'hôte.
   - Pour les machines distantes, entrez le nom d'hôte et l'adresse IP, séparés par une virgule du système d'appliance qui héberge AppAssure Core ; par exemple, *AdresseIP,nom d'hôte*.
4. Redémarrez Firefox.

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 rétention
- Configurer la capacité d'attachement SQL

REMARQUE : Si vous utilisez cette appliance, Dell vous recommande d'utiliser l'onglet **Appliance** pour configurer le Core. Pour plus d'informations sur la configuration du Core après l'installation initiale, voir le *Guide de déploiement de l'appliance Dell DL4300* sur **dell.com/support/home**.

Gestion des licences

Vous pouvez gérer les licences directement dans Core Console. Depuis la console, vous pouvez modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au portail des licences depuis la page Licences dans Core Console.

La page de gestion des licences inclut les informations suivantes :

- Type de licence
- État de licence
- Contraintes de licence
- Nombre de machines protégées
- État de la dernière réponse reçue du serveur de gestion des licences
- Heure du dernier contact avec le serveur de gestion des licences
- Prochaine tentative de contact programmée avec le serveur de gestion des licences

Modifier une clé de licence

Pour modifier une clé de licence :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Licences**.
   La page **Gestion des licences** s'affiche.
3. Dans la section **Détails de la licence , cliquez sur Modifier la licence**.
   La boîte de dialogue **Modifier la licence** s'affiche.
4. Dans la boîte de dialogue **Modifier la licence**, entrez la nouvelle clé de licence, puis cliquez sur **Continuer**.

Contacter le serveur de Portail de licences

La console Core contacte fréquemment le serveur de portail pour rester à jour en appliquant toutes les modifications apportées au portail de licences. En général, la communication avec le serveur de portail se produit automatiquement selon l'intervalle défini ; cependant, vous pouvez lancer la communication à la demande.

Pour contacter le serveur de portail :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Licences**.
3. À partir de l'option **Licence Server**, cliquez sur **Contacter maintenant**.

Modification manuelle de la langue d'AppAssure

AppAssure vous permet de changer la langue sélectionnée lors de l'exécution de l'Assistant Configuration de l'appliance AppAssure par l'une des langues prises en charge.
Pour changer la langue d'AppAssure par la langue souhaitée :

1. Lancez l'Éditeur de registre à l'aide de la commande `regdit`.
2. Rendez-vous sur **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** → **Core** → **Localization**.
3. Ouvrez **Lcid**.
4. Sélectionnez **Valeur décimale**.
5. Entrez la valeur correspondant à la langue requise dans la case `Données de la valeur`. Les valeurs correspondant aux langues prises en charge sont les suivantes :
   a. Anglais : 1033
   b. Portugais brésilien : 1046
   c. Espagnol : 1034
   d. Français : 1036
   e. Allemand : 1031
   f. Chinois simplifié : 2052
   g. Japonais : 1041
   h. Coréen : 1042
6. Cliquez avec le bouton droit de la souris et redémarrez les services dans l'ordre indiqué :
   a. WMI (infrastructure de gestion Windows)
   b. Service Internet SRM
   c. AppAssure Core
7. Effacez le cache du navigateur.
8. Fermez le navigateur et redémarrez la Core Console depuis l'icône sur le bureau.

Modification de la langue du système d'exploitation au cours de l'installation

Sur une installation fonctionnant sous Windows, vous pouvez utiliser le Panneau de configuration pour sélectionner des packs de langue et configurer des paramètres internationaux supplémentaires.
Pour modifier la langue du SE :

REMARQUE : Il est recommandé que la langue du système d'exploitation et celle d'AppAssure soient identiques. Dans le cas contraire, certains messages peuvent être affichés dans plusieurs langues.

REMARQUE : Il est recommandé de modifier la langue du système d'exploitation avant de modifier celle d'AppAssure.

1. Sur la page **Démarrer**, entrez `Langue`, et assurez-vous que le domaine de recherche est défini sur Paramètres.
2. Dans le volet **Résultats**, sélectionnez **Langue**.
3. Dans le volet **Modifier vos préférences linguistiques** , sélectionnez **Ajouter une langue**.
4. Parcourir ou rechercher la langue que vous souhaitez installer.

   Par exemple, sélectionnez Catalan, puis sélectionnez Ajouter. Le catalan a été ajouté comme l'une des langues.
5. Dans le volet Modifier vos préférences de langue, sélectionnez **Options** en regard de la langue ajoutée.
6. Si un pack de langue est disponible pour votre langue, sélectionnez `Télécharger et installer le pack de langue`.
7. Lorsque le pack de langue est installé, la langue est affichée comme étant disponible en tant que langue d'affichage de Windows.
8. Pour faire de cette langue votre langue d'affichage, déplacez-la en haut de votre liste de langues.
9. Pour que le changement prenne effet, déconnectez-vous de Windows puis reconnectez-vous.

Gestion des paramètres Core

Les paramètres de Core s'utilisent pour définir divers paramètres de configuration et performance. La plupart des paramètres sont configurés pour un usage optimal mais il est possible de modifier les paramètres suivants selon les besoins :

- généralités
- tâches nocturnes
- file d'attente de transfert
- paramètres d'expiration du délai d'attente client
- configuration du cache de déduplication
- paramètres de connexion de base de données

Modification du nom d'affichage du Core

REMARQUE : Il est recommandé de sélectionner un nom d'affichage permanent au cours de la configuration initiale de l'appliance. Si vous le modifiez ultérieurement, vous devez effectuer plusieurs opérations manuelles pour garantir que le nouveau nom d'hôte prend bien effet et que l'appliance fonctionne correctement. Pour plus d'informations, voir Modification manuelle du nom d'hôte.

Pour modifier le nom d'affichage du core :

1. naviguez jusqu'à Core Console.
2. Cliquez sur **Configuration** → **Paramètres.**
3. Dans la section **Général**, cliquez sur **Modifier**.

   La boîte de dialogue **Paramètres généraux** s'affiche.
4. Dans la zone de texte **Nom d'affichage** entrez le nouveau nom d'affichage du core.

   Il s'agit du nom qui s'affichera dans la Core Console. Vous pouvez saisir un maximum de 64 caractères.

5. Dans la zone de texte **Port du serveur Web** , entrez un numéro de port pour le serveur Web. La valeur par défaut est 8006.
6. Dans le **port de service**, entrez le numéro de port de service. La valeur par défaut est 8006.
7. Cliquez sur **OK**.

Régler l'option Heure de tâche nocturne

Pour régler l'heure de tâche nocturne :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Paramètres**.
3. Dans la zone **Tâches nocturnes**, cliquez sur **Modifier**.

   La boîte de dialogue **Tâches nocturnes** s'affiche.
4. Dans la zone de texte **Heure de tâche nocturne**, entrez une nouvelle heure pour effectuer les tâches nocturnes.
5. Cliquez sur **OK**.

Modification des paramètres de 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.

Pour modifier les paramètres de file d'attente de transfert :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Paramètres**.
3. Dans la section **File d'attente de transfert**, cliquez sur **Modifier**.

   La boîte de dialogue **File d'attente de transfert** s'affiche.
4. Dans le champ **Nombre maximal de transferts simultanés**, entrez une valeur pour mettre à mettre à jour le nombre de transferts simultanés.

   Définissez une valeur comprise entre 1 et 60. Plus la valeur est faible, plus la charge du réseau et des autres ressources système est faible. Avec l'augmentation du nombre des agents traités, la charge système augmente également.
5. Dans le champ **Nombre maximal de nouvelles tentatives**, entrez une valeur pour mettre à jour le nombre de nouvelles tentatives.
6. Cliquez sur **OK**.

Réglage des paramètres de délai d'attente du client

Pour régler les paramètres de délai d'attente du client :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Paramètres**.
3. Dans la zone **Configuration des paramètres de délai d'attente client**, cliquez sur **Modifier**.

   La boîte de dialogue **Paramètres de délai d'attente du client** s'affiche.
4. Dans le champ **Délai d'attente de connexion**, entrez le délai imparti, en nombre de minutes et de secondes.
5. Dans le champ **Délai d'attente de connexion de l'utilisateur de l'interface**, entrez le nombre de minutes et de secondes devant précéder l'expiration du délai d'attente de connexion de l'utilisateur de l'interface.

6. Dans le champ **Délai d'attente de lecture/écriture**, entrez le délai imparti (en minutes et secondes) pour un événement de lecture/écriture.
7. Dans le champ **Délai d'attente de lecture/écriture de l'utilisateur de l'interface**, entrez le délai imparti (en minutes et secondes) à l'utilisateur de l'interface pour un événement de lecture/écriture.
8. Cliquez sur **OK**.

Configuration des paramètres de cache de déduplication

Pour configurer les paramètres de cache de déduplication :

1. naviguez jusqu'à Core Console.
2. Cliquez sur **Configuration → Paramètres.**
3. Dans la zone de **Configuration du cache de déduplication**, cliquez sur **Modifier**.
   La boîte de dialogue **Configuration du cache de déduplication** s'affiche.
4. Dans le champ **Emplacement du cache principal**, entrez une valeur mise à jour pour modifier l'emplacement du cache principal.
5. Dans le champ **Emplacement du cache secondaire**, entrez une valeur mise à jour pour modifier l'emplacement du cache principal.
6. Dans le champ **Emplacement du cache de métadonnées**, entrez une valeur mise à jour pour modifier l'emplacement du cache de métadonnées.
7. Dans la zone de texte **Taille du cache de déduplication** , entrez une valeur correspondant à la quantité d'espace à allouer au cache de déduplication.
   Dans la liste déroulante du champ Taille de l'unité, sélectionnez Go (gigaoctets) ou To (téraoctets), pour indiquer l'unité de mesure de la valeur dans la zone de texte « Taille de cache de déduplication ».
8. Cliquez sur **OK**.

   REMARQUE : Vous devez redémarrer le Service de core pour que les modifications prennent effet.

Modification des paramètres du moteur

Pour modifier les paramètres du moteur :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration → Paramètres.**
3. Dans la section **Configuration du moteur de relecture**, cliquez sur **Modifier**.
   La boîte de dialogue **Configuration du moteur de relecture** s'affiche.
4. Entrez les informations concernant la configuration comme suit :

Zone de texte	Description
adresse IP	• Pour utiliser l'adresse IP préférée depuis votre TCP/IP, cliquez sur **Déterminé automatiquement**. • Pour entrer manuellement une adresse IP, cliquez sur **Utiliser une adresse spécifique**.
Port préférable	Entrez un numéro de port ou acceptez le paramètre par défaut (le port par défaut est 8007). Le port est utilisé pour spécifier le canal de communication du moteur.

Zone de texte	Description
Port en cours d'utilisation	Représente le port qui est utilisé pour la configuration du moteur de relecture.
Autoriser l'affectation de port automatique	Cliquez sur ce bouton pour créer une affectation automatique de port TCP.
Groupe Admin	Entrez le nouveau nom du groupe d'administration. Le nom par défaut est BUILTIN\Administrators.
Longueur d'E/S asynchrones minimale	Entrez la valeur ou choisissez le paramètre par défaut. Elle décrit la longueur entrée/sortie minimale. Le paramètre par défaut est 65536.
Taille du tampon de réception	Entrez une taille du tampon entrant ou acceptez le paramètre par défaut. Le paramètre par défaut est 8192.
Taille du tampon d'envoi	Entrez une taille de tampon d'envoi sortant ou acceptez le paramètre par défaut. Le paramètre par défaut est 8192.
Expiration du délai d'attente de lecture	Entrez la valeur d'expiration du délai d'attente de lecture ou choisissez le paramètre par défaut. Le paramètre par défaut est 00:00:30.
Expiration du délai d'attente d'écriture	Entrez la valeur d'expiration du délai d'attente d'écriture ou choisissez le paramètre par défaut. Le paramètre par défaut est 00:00:30.
Pas de délai	Il est recommandé de laisser cette case à cocher désélectionnée pour éviter de réduire l'efficacité du réseau. Si vous estimez nécessaire de modifier ce paramètre, contactez le support Dell pour obtenir de l'aide.

5. Cliquez sur **OK**.

Modification des paramètres de connexion de base de données

Pour modifier les paramètres de connexion de base de données :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration → Paramètres.**
3. Dans la zone **Paramètres de connexion de base de données**, effectuez l'une des tâches suivantes :
   - Cliquez sur **Appliquer la valeur par défaut**.
   - Cliquez sur **Modifier**.

   La boîte de dialogue **Paramètres de connexion de base de données** s'affiche.
4. Entrez les paramètres nécessaires pour modifier la connexion de base de données, comme suit :

Zone de texte	Description
Nom d'hôte	Entrez un nom d'hôte pour la connexion de base de données.
Port	Entrez un numéro de port pour la connexion de base de données.

Zone de texte	Description
Nom d'utilisateur (facultatif)	Entrez un nom d'utilisateur d'accès et de gestion des paramètres de connexion de base de données. Ce nom est utilisé pour spécifier le journal dans les références d'accès à la connexion de base de données.
Mot de passe (facultatif)	Entrez un mot de passe d'accès et de gestion des paramètres de connexion de base de données.
Conserver l'historique des événements et des tâches pendant, jours	Entrez le nombre de jours de conservation de l'historique des événements et des tâches pour la connexion de base de données.
Taille du pool de connexion max.	Définit le nombre maximal de connexions de la base de données mises en cache permettant la réutilisation dynamique. La valeur par défaut est 100.
Taille du pool de connexion min.	Définit le nombre minimal de connexions de la base de données mise en cache permettant la réutilisation dynamique. Le paramètre par défaut est 0.

5. Cliquez sur **Tester la connexion** pour vérifier vos paramètres.
6. Cliquez sur **Enregistrer**.

À propos des référentiels

Un référentiel est utilisé pour stocker les instantanés capturés depuis vos stations de travail et serveurs protégés. Le référentiel peut résider sur différentes technologies de stockage telles que SAN (Storage Area Network), DAS (Direct Attached Storage) ou NAS (Network Attached Storage).

Lorsque vous créez un référentiel, le Core préalloue l'espace de stockage requis pour les données et métadonnées à l'emplacement spécifié. Vous pouvez créer un maximum de 255 référentiels indépendants sur un même core avec différentes technologies de stockage. De plus, vous pouvez augmenter la taille d'un référentiel en ajoutant de nouveaux ensembles de blocs contigus ou spécifications de fichier. Un référentiel étendu peut contenir un maximum de 4 096 ensembles de blocs contigus couvrant différentes technologies de stockage.

Parmi les concepts clés et les considérations :

- Le référentiel est basé sur l'AppAssure Scalable Object File System.
- Toutes les données stockées au sein d'un référentiel sont dédupliquées globalement.
- Le Scalable Object File System peut fournir des performances d'E/S évolutives en conjonction avec la déduplication globale des données, le chiffrement et la gestion de la rétention.

REMARQUE : Les référentiels DL4300 sont stockés sur des périphériques de stockage principaux. Les périphériques de stockage d'archive comme le domaine de données (Data Domain) ne sont pas pris en charge en raison des limites de performances. De même, les référentiels ne doivent pas être stockés sur des fichiers NAS dans le cloud, car ces périphériques sont limités en matière de performances lorsqu'ils sont utilisés en tant que stockage principal.

Schéma de gestion d'un référentiel

La feuille de route de gestion d'un référentiel couvre des tâches comme la création, la configuration et l'affichage d'un référentiel, et inclut les rubriques suivantes :

- Accès à la Core Console
- Création d'un référentiel
- Affichage des détails du référentiel
- Modification des paramètres de référentiel
- Ajout d'une spécification de fichier à un référentiel existant
- Vérification d'un référentiel
- Suppression d'un référentiel
- Restauration d'un référentiel

REMARQUE : Il est recommandé d'utiliser l'onglet **Appliance** pour configurer les référentiels.

Avant d'utiliser votre appliance, vous devez configurer un ou plusieurs référentiels sur le serveur core. Un référentiel stocke vos données protégées ; plus précisément, il stocke les instantanés capturés depuis les serveurs protégés de votre environnement.

Lorsque vous configurez un référentiel, vous pouvez effectuer diverses tâches, notamment spécifier l'emplacement de stockage des données sur le serveur core, le nombre d'emplacements qui doivent être ajoutés à chaque référentiel, le nom du référentiel, le nombre d'opérations actuelles prises en charge par les référentiels.

Lorsque vous créez un référentiel, le core préalloue l'espace requis pour le stockage des données et des métadonnées dans l'emplacement spécifié. Vous pouvez créer jusqu'à 255 référentiels indépendants sur un même core. Pour augmenter davantage la taille d'un seul référentiel, vous pouvez ajouter de nouveaux emplacements de stockage ou volumes.

Vous pouvez ajouter ou modifier des référentiels dans la Core Console.

Création d'un référentiel

REMARQUE : Si vous utilisez cette appliance en tant que réseau de stockage SAN, il est recommandé d'utiliser l'onglet **Appliance** pour créer des référentiels, reportez-vous à la section Provisionnement du stockage sélectionné.

Exécutez les étapes suivantes pour créer manuellement un référentiel :

1. Naviguez jusqu'à la Core Console.
2. Cliquez sur **Configuration** → **Référentiels**.
3. Cliquez sur **Ajouter un nouveau**.
   La boîte de dialogue **Ajouter un nouveau référentiel** s'affiche.
4. Entrez les informations de configuration telles que décrites dans le tableau suivant.

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 d'index, ajouté par ordre de séquence aux nouveaux référentiels à partir du numéro 1. Vous pouvez modifier ce nom si nécessaire. Vous pouvez entrer jusqu'à 150 caractères.
Opérations simultanées	Définissez le nombre de demandes simultanées que votre référentiel doit prendre en charge. La valeur par défaut est 64.
Commentaires	(Optionnel) Entrez une note descriptive concernant ce référentiel.

5. Pour définir l'emplacement de stockage ou le volume spécifique du référentiel, cliquez sur **Ajouter un emplacement de stockage**.

   PRÉCAUTION : Si le référentiel AppAssure que vous créez à cette étape est supprimé ultérieurement, tous les fichiers de l'emplacement de stockage de ce référentiel sont supprimés. Si vous ne définissez par de dossier dédié pour les fichiers du référentiel, ils sont stockés dans la racine, ce qui signifie que la suppression du référentiel supprimera également l'intégralité du contenu du lecteur racine, d'où une perte de données catastrophique.

   REMARQUE : Les référentiels sont stockés sur des périphériques de stockage principaux. Les périphériques de stockage d'archive comme le domaine de données (Data Domain) ne sont pas pris en charge en raison des limites de performances. De même, les référentiels ne doivent pas être stockés sur des fichiers NAS dans le cloud, car ces périphériques sont limités en matière de performances lorsqu'ils sont utilisés en tant que stockage principal.

   La boîte de dialogue **Ajouter un emplacement de stockage** s'affiche.

6. Spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez ajouter un fichier sur le disque local ou sur le partage CIFS.

   - Pour spécifier une machine locale, cliquez sur **Ajouter un fichier sur le disque local**, puis entrez les informations indiquées ci-dessous :

Zone de texte	Description
Chemin de données	Indiquez l'emplacement de stockage des données protégées ; par exemple, entrez X:\Repository\Data. 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 ne sont pas sensibles à la casse. N'utilisez aucun espace. Aucun autre symbole ou caractère de ponctuation n'est admis.
Chemin des métadonnées	Indiquez l'emplacement de stockage des métadonnées protégées ; par exemple, entrez X:\Repository\Metadata. 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 ne sont pas sensibles à la casse. N'utilisez aucun espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

   - Vous pouvez aussi spécifier un partage réseau : cliquez sur **Ajouter un fichier dans un partage CIFS**, puis entrez les informations indiquées ci-dessous :

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, Référentiel). Le chemin 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 ne sont pas sensibles à la casse. N'utilisez aucun espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

Zone de texte	Description
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.

7. Dans le panneau **Détails**, cliquez sur **Afficher/Masquer les détails**, puis entrez les détails de l'emplacement de stockage comme indiqué ci-dessous :

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille par défaut est de 250 Mo. Vous avez le choix entre : • Mo • Go • To **REMARQUE :** La taille spécifiée ne peut pas excéder la taille du volume. **REMARQUE :** 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 ou Windows Server 2012, la taille de fichier est limitée à 256 To. **REMARQUE :** Pour valider 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 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 • Désactivé • Synchroniser Si vous choisissez Activé (valeur par défaut), Windows contrôle la mise en cache. **REMARQUE :** La configuration de la stratégie de mise en cache d'écriture sur Activé peut améliorer la vitesse des performances. Si vous utilisez une version de Windows Server antérieure à Server 2012, la valeur recommandée est **Désactivé**. Si la fonction est définie sur **Off** (Désactivé), AppAssure contrôle la mise en cache. Si la fonction est définie sur **Synchroniser**, Windows contrôle la mise en cache et les entrées/sorties synchrones.

Zone de texte	Description
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.

8. Cliquez sur **Enregistrer**.
   L'écran **Référentiels** s'affiche pour inclure le nouvel emplacement de stockage qui vient d'être ajouté.
9. Répétez les Étapes 4 à 7 pour ajouter plus d'emplacements de stockage au référentiel.
10. Cliquez sur **Créer** pour créer le référentiel.
    Les informations du **Référentiel** s'affichent dans l'onglet **Configuration**.

Affichage des détails du référentiel

Pour afficher les détails du référentiel :

1. naviguez jusqu'à Core Console.
2. Cliquez sur **Configuration** → **Référentiels**.
3. Cliquez sur **>** en regard de la colonne **État** du référentiel dont vous voulez afficher les détails.
4. Dans la vue développée, vous pouvez effectuer les opérations suivantes :
   - Modifier les paramètres
   - Ajouter un emplacement de stockage
   - Vérifier un référentiel
   - Supprimer un référentiel

   L'écran affiche également des détails sur le référentiel, et inclut les emplacements de stockage et des statistiques. Les détails des emplacements de stockage incluent le chemin des métadonnées et celui des données, ainsi que la taille. Les informations statistiques affichées sont les suivantes :
   - Déduplication : affiché sous forme de nombre de réussites de déduplication des blocs, nombre d'échecs de déduplication des blocs et taux de compression des blocs.
   - E/S d'enregistrement : les chiffres affichés sont le débit (Mo/s), le débit de lecture (Mo/s) et le débit d'écriture (Mo/s).
   - Moteur de stockage : les chiffres affichés sont le débit (Mo/s), le débit de lecture (Mo/s) et le débit d'écriture (Mo/s).

Modification des paramètres de référentiel

Après avoir ajouté un référentiel, vous pouvez en modifier les paramètres, notamment la description ou le nombre maximal d'opérations simultanées. Vous pouvez également créer un nouvel emplacement de stockage pour le référentiel.

Pour modifier des paramètres de référentiel

1. naviguez jusqu'à Core Console.
2. Cliquez sur **Configuration** → **Référentiels**.
3. cliquez sur l'icône Paramètres en regard de la colonne Taux de compression sous le bouton **Actions**, puis sur **Paramètres** .
   La boîte de dialogue **Paramètres de référentiel** s'affiche.
4. Modifiez les informations concernant le référentiel comme suit :

Champ	Description
Nom de référentiel	Représente le nom d'affichage du référentiel. Par défaut, cette zone de texte comprend le Référentiel word et un numéro d'index, qui correspond au numéro du référentiel. REMARQUE : Il est impossible de modifier le nom du référentiel.
Description	(Optionnel) Entrez une note descriptive concernant ce référentiel.
Nombre maximal d'opérations simultanées	Définissez le nombre de demandes simultanées que le référentiel devrait prendre en charge.
Activer la déduplication	Pour désactiver la déduplication, décochez cette case. Pour activer la déduplication, cochez cette case. REMARQUE : Les modifications apportées à ce paramètre ne s'appliquent qu'aux sauvegardes effectuées après la création du paramètre. Les données existantes ou les données répliquées depuis un autre core ou importées d'une archive, conservent les valeurs de déduplication établies au moment où les données ont été capturées de la machine protégée.
Activation de la compression	Pour désactiver la compression, décochez cette case. Pour activer la compression, cochez cette case. REMARQUE : Ce paramètre ne s'applique qu'aux sauvegardes effectuées après la modification du paramètre. Les données existantes ou les données répliquées depuis un autre core ou importées d'une archive, conservent les valeurs de compression établies au moment où les données ont été capturées de la machine protégée.

5. Cliquez sur **Enregistrer**.

Extension d'un référentiel existant

Si vous ajoutez un autre DAS MD1400 à l'appliance, vous pouvez utiliser le stockage disponible pour étendre un référentiel existant.

Pour étendre un référentiel existant :

1. Après avoir installé le DAS MD1400, ouvrez la Core console et sélectionnez l'onglet **Appliance**, puis cliquez sur **Tâches**.
2. Dans l'écran **Tâches**, en regard du nouveau stockage, cliquez sur **Provisionner**.
3. Dans l'écran **Provisionnement du stockage**, sélectionnez **Étendre le référentiel existant**, puis cliquez sur le référentiel à étendre.
4. Cliquez sur **Provisionner**.

   L'écran **Tâches** affiche le champ **Description de l'état**, en regard du périphérique de stockage. Ce champ contient la mention **Provisionné**.

Ajout d'un emplacement de stockage à un référentiel existant

L'ajout d'un emplacement de stockage vous permet de définir l'endroit où stocker le référentiel ou le volume.

Pour ajouter une spécification de fichier à un référentiel existant :

1. Cliquez sur **>** en regard de la colonne **État** du référentiel pour lequel vous voulez ajouter un emplacement de stockage.
2. Cliquez sur **Ajouter un emplacement de stockage**.

   La boîte de dialogue **Ajouter un emplacement de stockage** apparaît.
3. Spécifiez comment ajouter un fichier pour l'emplacement de stockage. Vous pouvez ajouter un fichier sur le disque local ou dans un partage CIFS.
   - Pour spécifier une machine locale, cliquez sur **Ajouter un fichier sur le disque local**, puis entrez les informations indiquées ci-dessous :

Zone de texte	Description
Chemin des métadonnées	Entrez l'emplacement de stockage des métadonnées protégées.
Chemin de données	Entrez l'emplacement de stockage des données protégées.

   - Pour spécifier lémplacement d'un partage réseau : cliquez sur **Ajouter un fichier dans un partage CIFS**, puis entrez les informations indiquées ci-dessous :

Zone de texte	Description
Chemin UNC	Entrez le chemin de l'emplacement du partage réseau.
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.

4. Dans la section **Détails**, cliquez sur **Afficher/Masquer les détails**, puis entrez les détails de l'emplacement de stockage comme indiqué ci-dessous :

Zone de texte	Description
Taille	Définissez la taille ou la capacité de l'emplacement de stockage. La taille par défaut est de 250 Mo. Vous avez le choix entre : • Mo • Go • To **REMARQUE :** La taille spécifiée ne peut pas excéder la taille du volume. **REMARQUE :** Si l'emplacement de stockage est un volume NTFS 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 ou Windows Server 2012, la taille de fichier est limitée à 256 To. **REMARQUE :** Pour valider le système d'exploitation, vous devez installer WMI sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle la manière d'utiliser le Windows Cache Manager dans le référentiel et aide à régler le référentiel pour obtenir une performance optimale sur des configurations différentes. Définissez la valeur sur une des options suivantes : • Activé

Zone de texte	Description
	• Désactivé • Synchroniser Si la fonction est définie sur **Activé**, qui est la valeur par défaut, Windows contrôle la mise en cache. REMARQUE : La configuration de la stratégie de mise en cache d'écriture sur **Activé** peut accélérer les performances, mais le paramétrage recommandé est **Désactivé**. Si la fonction est définie sur **Off** (Désactivé), AppAssure 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.

5. Cliquez sur **Enregistrer**.
   L'écran **Référentiels** s'affiche pour inclure le nouvel emplacement de stockage qui vient d'être ajouté.
6. Répétez les Étapes 4 à 7 pour ajouter plus d'emplacements de stockage pour le référentiel.
7. Cliquez sur **OK**.

Vérification d'un référentiel

L'appliance peut effectuer une vérification diagnostique d'un volume de référentiel lorsqu'une erreur survient. Les erreurs de core peuvent résulter, entre autres, d'un arrêt incorrect ou d'un échec du matériel.

REMARQUE : Cette procédure doit être strictement réservée au diagnostic.

Pour vérifier un référentiel :

1. Dans l'onglet **Configuration**, cliquez sur **Référentiels**, puis sélectionnez **>** en regard du référentiel que vous souhaitez vérifier.
2. Dans le volet **Actions**, cliquez sur **Vérifier**.
   La boîte de dialogue **Vérifier le référentiel** s'affiche.
3. Dans la boîte de dialogue **Vérifier le référentiel**, cliquez sur **Vérifier**.

   REMARQUE : Si la vérification échoue, restaurez le référentiel à partir d'une archive.

Suppression d'un référentiel

Pour supprimer un référentiel :

1. Dans l'onglet **Configuration**, cliquez sur **Référentiels**, puis sélectionnez **>** en regard du référentiel que vous souhaitez supprimer.
2. Dans le volet **Actions**, cliquez sur **Supprimer**.

3. dans la boîte de dialogue **Supprimer un référentiel**, cliquez sur **Supprimer.**

   PRÉCAUTION : Lorsqu'un référentiel est supprimé, les données qu'il contient sont mises au rebut et ne peuvent pas être récupérées.

   Lorsque vous supprimez un référentiel, vous devez passer par l'OpenManage System Administrator et supprimer les disques virtuels qui hébergeaient le référentiel. Une fois que vous avez supprimé les disques virtuels, vous pouvez reprovisionner les disques et recréer le référentiel.

Remontage des volumes

Pour remonter les volumes :

1. naviguez jusqu'à Core Console.
2. **Tâches → de l'appliance**.
3. Cliquez sur **Remonter les volumes**.
   Les volumes sont remontés.

Résolution de volumes étrangers

Si vous avez éteint ou déconnecté un MD1400 provisionné, puis que vous le rallumez ultérieurement, un événement s'affiche sur la Core Console et vous signale que le MD1400 est connecté. Toutefois, aucune tâche n'apparaît dans l'écran **Tâches** de l'onglet **Appliance** pour vous permettre d'effectuer la restauration. L'écran **Enceintes** indique le MD1400 comme « étranger » et signale les référentiels des disques virtuels étrangers comme étant hors ligne.

Pour résoudre les volumes étrangers :

1. Dans Core Console , cliquez sur l'onglet **Appliance**, puis sur **Remonter les volumes**.
   Les volumes sont remontés.
2. Sélectionnez l'onglet **Configuration** puis cliquez sur **Référentiels**.
3. Développez le répertoire portant un indicateur d'état rouge, en cliquant sur **>** en regard de l'option **État**.
4. Pour vérifier l'intégrité du référentiel, ouvrez la liste **Actions** et cliquez sur **Vérifier**.

Restauration d'un référentiel

Si l'appliance ne parvient pas à importer un référentiel, elle signale cet échec dans l'écran **Tâches** en affichant comme indicateur d'état de tâche un cercle rouge, avec la description d'état **Erreur, Terminé — Exception**. Pour afficher les détails de l'erreur depuis l'écran **Tâches**, développez la tâche en cliquant sur **>** en regard de la colonne **État**. La zone **Détails de l'état** indique que la tâche de restauration est à l'état d'exception et la colonne **Message d'erreur** fournit des détails supplémentaires sur la condition d'erreur.

Pour restaurer un référentiel avec le statut Échec de l'importation :

1. naviguez jusqu'à la Core Console.
   L'écran **Référentiels** affiche le référentiel en échec avec un indicateur d'état rouge.
2. Cliquez sur **Configuration → Référentiels**.
3. Développez le référentiel en échec en cliquant sur **>** en regard de l'option **État**.
4. Dans la section **Actions**, cliquez sur **Vérifier**, puis sur **Oui** pour confirmer que vous souhaitez exécuter la vérification.
   L'appliance restaure le référentiel.

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 dédupliquées 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.

Ajout d'une clé de chiffrement

Pour ajouter une clé de chiffrement :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité**.
   La page**clés de cryptage** s'affiche.
3. Cliquez sur **Actions**, puis sélectionnez **Ajouter une clé de chiffrement**.
   La boîte de dialogue **Créer une clé de cryptage** apparaît.
4. Dans la boîte de dialogue **Créer une clé de cryptage**, entrez les détails de la clé comme indiqué ci-dessous.

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement.
Description	Entrez la description de la clé de cryptage. Elle sert à fournir des détails supplémentaires sur la clé.
Phrase de passe	Entrez une phrase de passe. Elle sert à contrôler l'accès.
Confirmer la phrase de passe	Entrez la phrase de passe de nouveau. Elle sert à confirmer la saisie de la phrase de passe.

5. Cliquez sur **OK**.

   PRÉCAUTION : Il vous est recommandé de protéger la phrase de passe. Si vous la perdez, vous ne pourrez pas accéder aux données.

Modification d'une clé de chiffrement

Pour modifier une clé de chiffrement :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité.**
   L'écran **Clés de chiffrement** s'affiche.
3. Sélectionnez la clé de chiffrement à modifier et cliquez sur **Modifier**.
   La boîte de dialogue **Modifier la clé de cryptage** apparaît.
4. Dans la boîte de dialogue **Modifier la clé de cryptage**, modifiez le nom ou la description de la clé.
5. Cliquez sur **OK**.

Modification d'une phrase d'authentification de clé de chiffrement

Pour modifier une phrase d'authentification de clé de chiffrement :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité**.
   La page clés de chiffrement s'affiche.
3. Sélectionnez la clé de chiffrement à modifier et cliquez sur **Modifier**.
   La boîte de dialogue **Modifier la phrase d'authentification** apparaît.
4. Dans la boîte de dialogue **Modifier la phrase d'authentification**, entrez la nouvelle phrase d'authentification pour le cryptage, puis entrez-la de nouveau pour confirmer votre saisie.
5. Cliquez sur **OK**.

   PRÉCAUTION : Il vous est recommandé de protéger la phrase d'authentification. Si vous la perdez, vous ne pourrez pas accéder aux données sur le système.

Importation d'une clé de cryptage

Pour importer une clé de cryptage :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité**.
3. Cliquez sur le menu déroulant **Actions**, puis cliquez sur **Importer**.
   La boîte de dialogue **Importer une clé** apparaît.
4. Dans la boîte de dialogue **Importer une clé**, cliquez sur **Parcourir** pour repérer la clé de cryptage à importer, puis sélectionnez **Ouvrir**.
5. Cliquez sur **OK**.

Exportation d'une clé de chiffrement

Pour exporter une clé de chiffrement :

1. naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité**.
3. Cliquez sur le symbole de chevron droit **>** en regard du nom de la clé de cryptage à exporter, puis cliquez sur **Exporter**.
   La boîte de dialogue **Exporter la clé** apparaît.

4. Dans la boîte de dialogue **Exporter une clé**, cliquez sur **Télécharger la clé** pour enregistrer et stocker les clés de chiffrement à un emplacement sécurisé.
5. Cliquez sur **OK**.

Suppression d'une clé de chiffrement

Pour supprimer une clé de chiffrement

1. Naviguez jusqu'à Core Console.
2. cliquez sur **Configuration** → **Sécurité**.
3. Cliquez sur le symbole de chevron droit **>** en regard du nom de la clé de chiffrement à supprimer, puis cliquez sur **Supprimer**.

   La boîte de dialogue **Supprimer la clé** apparaît.
4. Dans la boîte de dialogue **Supprimer la clé**, cliquez sur **OK** pour supprimer la clé de chiffrement.

   REMARQUE : La suppression d'une clé de chiffrement entraîne le déchiffrement des données.

Gestion des comptes Cloud

Le système DL permet de sauvegarder les données en créant une archive de sauvegarde des points de restauration vers un Cloud. Avec le système DL, vous pouvez créer, modifier et gérer le compte Cloud par le biais d'un fournisseur de stockage Cloud. Vous pouvez archiver les données dans le Cloud à l'aide de Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage ou d'autres services Cloud OpenStack. Reportez-vous aux rubriques suivantes pour gérer les Clouds :

- Ajout d'un compte Cloud
- Modification d'un compte Cloud
- Définition des paramètres d'un compte Cloud
- Suppression d'un compte Cloud

Ajout d'un compte Cloud

Pour pouvoir exporter les données archivées vers un Cloud, vous devez ajouter le compte de votre fournisseur Cloud dans la Core Console.

Pour ajouter un compte Cloud :

1. Dans la Core Console, cliquez sur l'onglet **Outils**.
2. Dans le menu de gauche, cliquez sur **Clouds**.
3. Sur la page **Clouds**, cliquez sur **Ajouter un nouveau compte**.

   La boîte de dialogue **Ajouter un nouveau compte** s'ouvre.
4. Sélectionnez un fournisseur Cloud compatible dans la liste déroulante **Type de Cloud**.
5. Entrez les informations décrites dans le tableau suivant en fonction du type de Cloud sélectionné à l'étape 4.

Tableau 1. Ajout d'un compte Cloud

Type de Cloud	Zone de texte	Description
Microsoft Azure	Nom de compte de stockage	Entrez le nom du compte de stockage Windows Azure.
	Clé d'accès	Entrez la clé d'accès du compte.
	Nom d'affichage	Créez le nom d'affichage du compte dans AppAssure ; par exemple, Windows Azure 1.
Amazon S3	Clé d'accès	Entrez la clé d'accès du compte Cloud Amazon.
	Clé secrète	Saisissez la clé secrète du compte.
	Nom d'affichage	Créez le nom d'affichage du compte dans AppAssure ; par exemple, Amazon 1.
Optimisé par OpenStack	Nom d'utilisateur	Entrez le nom d'utilisateur du compte Cloud OpenStack.
	Clé API	Entrez la clé de l'API du compte.
	Nom d'affichage	Créez le nom d'affichage du compte dans AppAssure ; par exemple, OpenStack 1.
	ID du client	Entrez l'ID de client du compte.
	URL d'authentification	Entrez l'URL d'authentification du compte.
Rackspace Cloud Block Storage	Nom d'utilisateur	Entrez le nom d'utilisateur du compte Cloud Rackspace.
	Clé API	Entrez la clé de l'API du compte.
	Nom d'affichage	Créez le nom d'affichage du compte dans AppAssure ; par exemple, Rackspace 1.

6. Cliquez sur **Ajouter**.
   La boîte de dialogue se ferme et le compte s'affiche dans la page **Clouds** de Core Console.

Modification d'un compte Cloud

Procédez comme suit pour modifier un compte Cloud :

1. dans Core Console, cliquez sur l'onglet **Outils**.
2. Dans le menu de gauche, cliquez sur **Clouds**.
3. En regard du compte Cloud à modifier, cliquez sur le menu déroulant, puis sur **Modifier**.

La fenêtre **Éditer un compte** s'ouvre.

4. Modifiez les informations de manière appropriée, puis cliquez sur **Enregistrer**.

   REMARQUE : Vous ne pouvez pas modifier le type de Cloud.

Définition des paramètres d'un compte Cloud

Les paramètres de compte Cloud permettent de déterminer le nombre de fois où la solution AppAssure doit tenter de se connecter à votre compte Cloud et le temps passé à essayer avant l'expiration du délai. Pour définir les paramètres de connexion du compte Cloud :

1. Dans la console Core, cliquez sur l'onglet **Configuration**.
2. Dans le menu de gauche, cliquez sur **Paramètres**.
3. Dans la page **Paramètres**, faites défiler la page jusqu'à **Configuration Cloud**.
4. Cliquez sur le menu déroulant en regard du compte Cloud à configurer, puis effectuez l'une des opérations suivantes :
   - Cliquez sur **Modifier**.
     La boîte de dialogue **Configuration Cloud** apparaît .

     1. Utilisez les flèches Haut et Bas pour modifier l'une ou l'autre des options suivantes :
        - **Délai d'attente de la demande** : indiquée en minutes et secondes, l'option définit le temps qu'AppAssure doit consacrer à une seule tentative de connexion au compte Cloud quand il existe un retard. Les tentatives de connexion sont interrompues après l'expiration du délai.
        - **Nombre de tentatives :** détermine le nombre de tentatives que doit exécuter AppAssure avant de déterminer que le compte Cloud est inaccessible.
        - **Taille du tampon d'écriture :** détermine la taille de la mémoire tampon réservée à l'écriture des données archivées dans le Cloud.
        - **Taille du tampon de lecture :** détermine la taille du bloc réservé à la lecture des données archivées à partir du Cloud.
     2. Cliquez sur **Suivant**.
   - Cliquez sur **Réinitialiser**. Restaure les paramètres par défaut suivants de la configuration :
     - **Délai d'expiration de la demande :** 01:30 (minutes et secondes)
     - **Nombre de tentatives :** 3 (tentatives)

Suppression d'un compte Cloud

Vous pouvez supprimer un compte Cloud, arrêtez le service Cloud ou arrêter de l'utiliser pour un Core. Pour supprimer un compte Cloud :

1. dans la Core Console, cliquez sur l'onglet **Outils** .
2. Dans le menu de gauche, cliquez sur **Clouds**.
3. En regard du compte Cloud à modifier, cliquez sur le menu déroulant, puis sur **Supprimer**.
4. Dans la fenêtre **Supprimer le compte**, cliquez sur **Oui** pour confirmer que vous souhaitez supprimer le compte.
5. Si le compte Cloud est en cours d'utilisation, une deuxième fenêtre demande si vous souhaitez le supprimer. Cliquez sur **Oui** pour confirmer.

   REMARQUE : La suppression d'un compte en cours d'utilisation provoque l'échec de toutes les tâches planifiées du compte.

Comprendre la réplication

À propos de la protection des stations de travail et des serveurs

Pour protéger les données, ajoutez les postes de travail et les serveurs à protéger dans Core Console ; par exemple, le serveur Exchange, SQL Server ou le serveur Linux.

REMARQUE : Dans ce chapitre, en général, le terme *machine* désigne également le logiciel d'agent AppAssure installé sur cette machine.

Dans la Core Console, vous pouvez identifier la machine où un AppAssure Agent est installé et spécifier les volumes à protéger, définir des planifications de protection, ajouter des mesures de sécurité supplémentaires, telles que le cryptage, etc. Pour plus d'informations sur l'accès à la Core Console pour protéger les stations de travail et serveurs, voir Protection d'une machine.

À propos de la réplication

La réplication consiste à copier des points de restauration et à les transmettre vers un emplacement secondaire en vue de la récupération après sinistre. Ce processus nécessite une relation entre une paire de cores (source et cible). Le core source copie les points de restauration des agents protégés, puis les transmet en continu de façon asynchrone à un core cible sur un site distant de récupération après sinistre. L'emplacement hors site peut être un centre de données appartenant à l'entreprise (core autogéré), un site appartenant à un fournisseur tiers de services gérés (MSP) ou un environnement de cloud. Lors de la réplication vers un MSP, vous pouvez utiliser des flux de travail intégrés, qui vous permettent de demander des connexions et de recevoir des notifications de retour d'informations automatiques. Les scénarios de réplication possibles sont les suivants :

- **Réplication vers un emplacement local**. Le core cible réside dans un centre de données local ou un emplacement sur site, et la réplication est maintenue à tout moment. Dans cette configuration, la perte du core n'empêche pas la restauration.
- **Réplication vers un emplacement hors site**. Le core cible réside sur une installation hors site de récupération après sinistre, qui permet la restauration en cas de perte.
- **Réplication mutuelle**. Deux centres de données, à deux emplacements différents, contiennent chacun un core et protègent les agents ; ils servent de sauvegarde pour la récupération après sinistre hors site l'un pour l'autre. Dans ce scénario, chaque core réplique les agents vers le core situé dans l'autre centre de données.
- **Réplication hébergée et dans le cloud**. Les partenaires MSP d'AppAssure maintiennent plusieurs cores cible dans un centre de données ou un cloud public. Sur chacun de ces cores, le partenaire MSP permet à un ou plusieurs de ses clients de répliquer des points de restauration depuis un core source sur le site du client vers le core cible du MSP moyennant paiement.

  REMARQUE : Dans ce scénario, les clients ont uniquement accès à leurs propres données.

Les configurations de réplication possibles incluent :

- **Point à point**. Réplique un agent unique d'un seul core source vers un seul core cible.

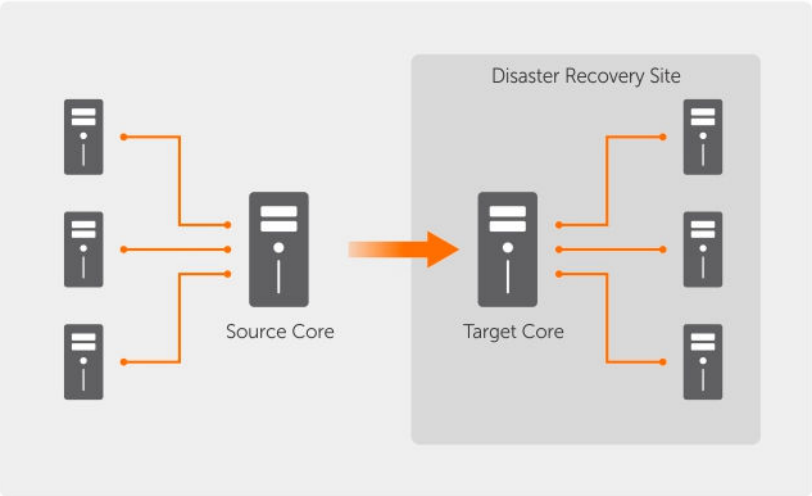


Figure 7. Diagramme de l'architecture de réplication de base

- **Multipoint à point**. Réplique plusieurs cores source vers un seul core cible.

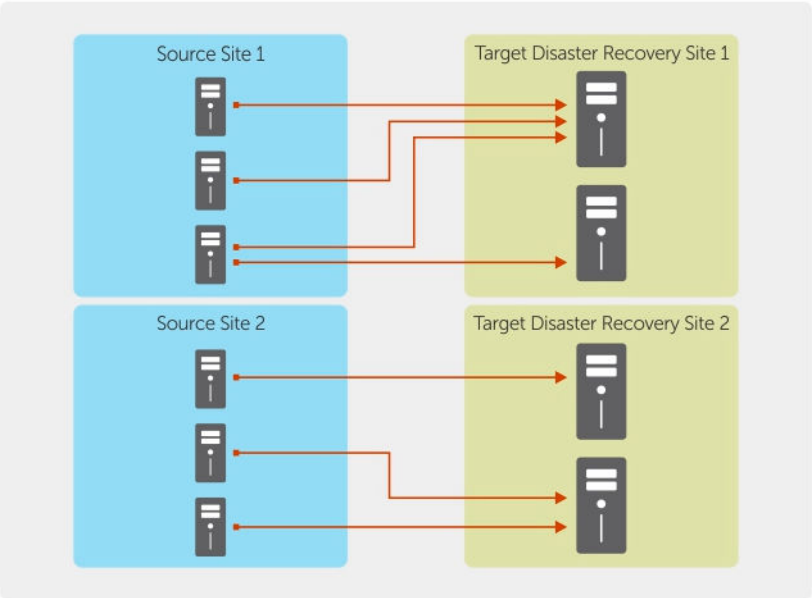


Figure 8. Diagramme de l'architecture de réplication multipoint

À propos de l'amorçage

La réplication commence par l'amorçage de données : le transfert initial d'images de base dédupliquées et d'instantanés incrémentiels de machines protégées, ce qui peut ajouter jusqu'à des centaines voire des milliers de gigaoctets de données. La réplication initiale peut être amorcée sur le core cible à l'aide de supports externes pour transférer les données initiales au core cible. En général, cela est utile pour les gros ensembles de données ou les sites dont les liens sont lents.

REMARQUE : Bien qu'il soit possible d'amorcer les données de base sur une connexion réseau, cette action n'est pas recommandée. L'amorçage initial exige de très gros volumes de données, ce qui peut submerger une connexion WAN typique. Par exemple, si les données d'amorçage mesurent 10 Go et que le lien WAN transfert 24 Mbits/s, le transfert peut prendre plus de 40 jours.

Les données de l'archive d'amorçage sont compressées, chiffrées et dédupliquées. Si la totalité de l'archive est supérieure à l'espace disponible dans le support amovible, l'archive peut s'étendre sur plusieurs périphériques en fonction de l'espace disponible dans le support. Au cours du processus d'amorçage, les points de restauration incrémentiels sont répliqués au site cible. Suite à la consommation de l'archive d'amorçage par le core cible, les points de restauration incrémentiels récemment répliqués se synchronisent automatiquement.

L'amorçage est un processus en deux parties (également appelé copy-consume (copier/consommer) :

- La première partie comprend la copie, c'est-à-dire l'écriture des données répliquées initialement sur une source de support amovible. La copie duplique tous les points de restauration existants du core source à un périphérique de stockage tel qu'un lecteur USB. Après la fin de la copie, vous devez transporter le lecteur de l'emplacement du core source à l'emplacement du core cible à distance.
- La deuxième partie est la consommation, qui se produit lorsqu'un core cible reçoit le lecteur transporté et copie les données répliquées sur le référentiel. Le core cible consomme ensuite les points de restauration et les utilise pour former des machines protégées.

REMARQUE : Tandis que la réplication d'instantanés incrémentiels peut se produire entre le core source et le core cible avant la fin de l'amorçage, les instantanés répliqués transmis de la source au core resteront « orphelins » jusqu'à la consommation des données initiales et sont associés aux images de base répliquées.

En raison d'importantes quantités de données devant être copiées dans le périphérique de stockage mobile, une connexion eSATA, USB 3.0 ou une autre connexion haut débit à ce périphérique de stockage mobile est recommandée.

À propos du basculement sur incident et de la restauration

En cas de panne de courant entraînant des pannes du core source et de l'agent, l'appliance DL prend en charge le basculement et la restauration dans des environnements répliqués. Le terme basculement désigne le passage à un Core cible redondant ou de secours après une panne du système ou un arrêt anormal d'un core source et de ses machines protégées associées. L'objectif principal du basculement est de lancer un nouvel agent identique à celui qui est tombé en panne et qui était protégé par le core source tombé en panne. L'objectif secondaire est de faire passer le core cible dans un nouveau mode de sorte à ce que le core cible protège l'agent de basculement de la façon dont le core source protégeait l'agent initial avant la panne. Le core cible peut restaurer des instances à partir d'agents répliqués et commencer immédiatement la protection sur les ordinateurs en panne.

Le terme restauration désigne le processus de restauration d'un agent et d'un core à leurs états d'origine (avant la panne). L'objectif principal de la restauration est de restaurer la machine protégée (dans la plupart des cas, il s'agit d'une nouvelle machine remplaçant un agent en panne) à un état identique au dernier état du nouvel agent temporaire. Une fois restauré, il est protégé par un core source restauré. La réplication est également restaurée, et le core cible agit de nouveau en tant que cible de réplication.

À propos de la réplication et des points de restauration chiffrés

Alors que le lecteur d'amorçage ne contient aucune sauvegarde du registre core source et des certificats, le lecteur d'amorçage ne contient aucune clé de chiffrement du core source si les points de restauration en cours de réplication de la source à la cible sont chiffrés. Les points de restauration répliqués restent

chiffrés après avoir été transmis au core cible. Les propriétaires ou administrateurs du core cible ont besoin de la phrase de passe pour restaurer les données chiffrées.

À propos de la stratégie de rétention de la réplication

La stratégie de rétention sur le core source détermine celle des données répliquées sur le core cible, car la tâche de réplication transmet les points de restauration fusionnés résultant d'un processus de cumul ou d'une suppression ad-hoc.

REMARQUE : Le core cible ne peut pas effectuer des suppressions de cumul ou ad-hoc de points de restauration. Ces actions peuvent être effectuées uniquement par le core source.

Considérations sur les performances de transfert de données répliquées

Si la bande passante entre le core source et le core cible ne peut pas assurer le transfert de points de restauration stockés, la réplication commence par l'amorçage du core cible avec des images de base et des points de restauration depuis les serveurs sélectionnés qui sont protégés sur le core source. Le processus d'amorçage ne doit être effectué qu'une seule fois car il sert de fondation requise pour la réplication planifiée régulièrement.

Lors de la préparation de la réplication, vous devez prendre en compte les facteurs suivants :

Taux de modification.	La vitesse de modification est la vitesse à laquelle la quantité de données protégées s'accumule. La vitesse dépend de la quantité de données qui change sur les volumes protégés et de l'intervalle de protection des volumes. Si un ensemble de blocs change sur le volume, la réduction de l'intervalle de protection réduit la vitesse de modification.
Bande passante	La bande passante est la vitesse de transfert disponible entre le core source et le core cible. Il est crucial que la bande passante soit supérieure à la vitesse de modification pour que la réplication suffise aux points de restauration créés par les instantanés. Étant donné la quantité de données transmise de core à core, plusieurs flux parallèles peuvent être exigés pour réaliser ces transferts à des vitesses filaires allant jusqu'à une vitesse de connexion Ethernet de 1 Go. REMARQUE : La bande passante spécifiée par l'ISP est la bande passante totale disponible. La bande passante sortante est partagée par tous les périphériques sur le réseau. Assurez-vous qu'il y ait suffisamment de bande passante libre pour que la réplication corresponde à la vitesse de modification.
Nombre de machines protégées	Il est important de prendre en compte le nombre de machines protégées par core source et le nombre que vous planifiez de répliquer vers la cible. AppAssure vous permet d'effectuer la réplication sur base d'un serveur protégé à la fois, pour que vous puissiez choisir de répliquer certains serveurs. Si tous les serveurs protégés doivent être répliqués, ceci affecte considérablement la vitesse de modification, en particulier 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.

En fonction de la configuration de votre réseau, la réplication peut prendre quelque temps.

Le tableau suivant montre des exemples de bande passante nécessaire par Gigaoctet pour une vitesse de modification raisonnable

REMARQUE : Pour des résultats optimaux, suivez les recommandations indiquées dans le tableau suivant.

Taux de modification maximum pour des types de connexion WAN.

Tableau 2. Taux de modification maximum pour des types de connexion WAN.

Large bande	Bande passante	Vitesse de modification maximale
DSL	768 Kbits/s et plus	330 Mo par heure
Câble	1 Mbit/s et plus	429 Mo par heure
T1	1,5 Mbits/s et plus	644 Mo par heure
Fibre	20 Mbit/s et plus	838 Go par heure

Si une liaison échoue pendant le transfert des données, la réplication est reprise à partir du point d'échec précédent du transfert, une fois la fonctionnalité de la liaison restaurée.

Schéma d'exécution d'une réplication

Pour répliquer des données à l'aide d'AppAssure, vous devez configurer les cores source et cible pour la réplication. Après avoir configuré la réplication, vous pouvez répliquer les données de la machine protégée, surveiller et gérer la réplication et effectuer des restaurations.

L'exécution d'une réplication dans AppAssure implique d'exécuter les tâches suivantes :

- Configuration de la réplication autogérée. Pour plus d'informations sur la réplication d'un core cible autogéré, reportez-vous à la section Réplication vers un core autogéré.
- Configuration de la réplication tierce. Pour plus d'informations sur la réplication d'un core cible tiers, reportez-vous à la section Réplication vers un core géré par un tiers
- Réplication d'une nouvelle machine protégée rattachée au core source. Pour plus d'informations sur la réplication d'une machine protégée, voir Réplication d'une nouvelle machine protégée.
- Répliquer une machine protégée existante. Pour plus d'informations sur la configuration d'un agent pour la réplication, voir Réplication des données d'agent sur une machine.
- Définir la priorité de réplication d'un agent. Pour plus d'informations sur la définition des priorités de réplication des agents, reportez-vous à Définition de la priorité de réplication d'un agent .
- Surveiller la réplication si nécessaire. Pour en savoir plus sur la surveillance de la réplication, voir Surveillance de la réplication.
- Gérer des paramètres de réplication si nécessaire. Pour plus d'informations sur la gestion des paramètres de réplication, voir Gestion des paramètres de réplication.
- Restaurer des données répliquées en cas de sinistre ou de perte de données. Pour plus d'informations sur la restauration des données répliquées, voir Restauration des données répliquées .

Réplication vers un core autogéré

Un core autogéré est un core auquel vous avez accès, généralement parce qu'il est géré par votre entreprise dans un emplacement hors site. La réplication peut être réalisée entièrement sur le core source, sauf si vous choisissez de créer des données de départ à diffuser. Les données de départ exigent que vous consommiez le lecteur de départ sur le core cible après avoir configuré la réplication sur le core source.

REMARQUE : Cette configuration s'applique à la réplication vers un emplacement hors site et à la réplication mutuelle. Vous devez installer AppAssure Core sur toutes les machines source et cible. Si vous configurez AppAssure pour une réplication multipoint à point, vous devez réaliser cette tâche sur tous les cores source et sur le core cible.

Configuration du core source pour la réplication vers un core cible autogéré

Pour configurer le core source afin qu'il réplique les données vers un core cible autogéré :

1. Dans Core Console, cliquez sur l'onglet **Réplication**.
2. Cliquez sur **Ajouter un core cible**.

   L'Assistant **Réplication** apparaît.
3. Sélectionnez **Je possède mon propre core cible**, puis entrez les informations décrites dans le tableau suivant.

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	Entrez le numéro de port sur lequel AppAssure Core communique avec la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Entrez le nom d'utilisateur pour accéder à la machine ; par exemple, **Administrateur.**
Mot de passe	Entrez le mot de passe d'accès à la machine.

   Si le Core à ajouter est associé à ce core source, effectuez les opérations suivantes :

   a. sélectionnez **Utiliser un core cible existant**.
   b. Sélectionnez le core cible dans la liste déroulante.
   c. Cliquez sur **Suivant**.
   d. Passez à l'étape 7.
4. Cliquez sur **Suivant**.
5. Sur la page **Détails**, entrez le nom de la configuration de réplication ; par exemple, SourceCore1. Si vous réinitialisez ou réparez une configuration précédente de réplication, sélectionnez **Mon Core a été migré et je souhaite réparer la réplication**
6. Cliquez sur **Suivant**.
7. Sur la page **Agents** , sélectionnez les agents à répliquer, puis utilisez les listes déroulantes dans la colonne **Référentiel** pour sélectionner un référentiel pour chaque agent.
8. Si vous prévoyez d'effectuer le processus d'amorçage pour le transfert de la base de données, procédez comme suit :

   REMARQUE : En raison d'importantes quantités de données devant être copiées dans le périphérique de stockage mobile, une connexion eSATA, USB 3.0 ou une autre connexion haut débit à ce périphérique de stockage mobile est recommandée.

   a. Sur la page **Agents**, sélectionnez **Utiliser un lecteur de départ pour effectuer un transfert initial**. Si un ou plusieurs agents répliquent vers un core cible , vous pouvez inclure ces machines protégées dans le lecteur source, en sélectionnant **Avec déjà répliqué**.
   b. Cliquez sur **Suivant**.
   c. Sur la page **Emplacement du lecteur de départ**, utilisez la liste déroulante **Type d'emplacement** pour sélectionner l'une des options suivantes :

- Local : dans la zone de texte **Emplacement**, entrez l'emplacement dans lequel AppAssure doit enregistrer le lecteur source ; par exemple, D :\work\archive.
- Réseau : dans la zone de texte **Emplacement**, entrez l'emplacement dans lequel AppAssure doit enregistrer le lecteur de source, puis entrez vos informations d'identification pour le partage réseau dans les zones de texte **Nom d'utilisateur** et **Mot de passe**.
- Cloud : Dans la zone de texte **du compte** , sélectionnez le compte. Pour sélectionner un compte Cloud, vous devez, en premier lieu, avoir ajouté dans la Core Console. Pour en savoir plus, reportez-vous à la section Ajout d'un Compte Cloud. Sélectionnez le **conteneur** associé à votre compte. Sélectionnez le **Nom du dossier** vers lequel les données d'archives doit être enregistré.

d. Cliquez sur **Suivant**. ntainer

9. Dans la boîte de dialogue **Options de lecteur de départ**, saisissez les informations décrites ci-dessous :

Zone de texte	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 : • sélectionner **Toute la cible** pour réserver l'intégralité de l'espace disponible dans le chemin fourni sur la page Emplacement des unités source pour une utilisation ultérieure (par exemple, si l'emplacement est D:\work\archive, tout l'espace disponible sur le disque D: est réservé si nécessaire pour la copie du lecteur source, mais il n'est pas réservé immédiatement après le démarrage de la copie). • Sélectionnez la zone de texte vide, tapez une valeur, puis sélectionnez une unité de mesure dans la liste déroulante pour personnaliser la quantité maximale d'espace à réserver.
ID de client (facultatif)	Le cas échéant, entrez l'ID client qui vous a été affecté par le fournisseur de service.
Action de recyclage	Si le chemin contient déjà un lecteur de départ, sélectionnez l'une des options suivantes : • **Ne pas réutiliser** : n'écrase ou n'efface aucune donnée existante de l'emplacement. Si celui-ci n'est pas vide, l'écriture de lecteur d'amorçage échoue. • **Remplacer ce core** : écrase toute donnée pré-existante appartenant à ce core mais laisse intactes les données des autres cores. • **Tout effacer** : efface toutes les données du répertoire avant d'écrire le lecteur d'amorçage.
Commentaire	Entrez un commentaire ou une description de l'archive.
Ajouter tous les agents au lecteur source	Sélectionnez les agents que vous souhaitez répliquer à l'aide du lecteur d'amorçage.
Créer des chaînes points de restauration	Sélectionnez cette option pour répliquer l'intégralité de la chaîne de points de restauration vers le lecteur source. Cette option est sélectionnée par défaut. L'amorçage typique dans AppAssure ne réplique que le dernier point le restauration vers lecteur source, ce qui réduit le délai et l'espace de création

Zone de texte	Description
	du lecteur de source. La création de chaînes de points de restauration vers le lecteur source nécessite un espace suffisant sur le lecteur source afin de stocker les derniers points de restauration de l'agent ou des agents spécifiés, et peut prendre plus de temps pour terminer la tâche.
Utiliser un format compatible	Sélectionnez cette option pour créer le lecteur source dans un format compatible avec les nouvelles et les anciennes versions d'AppAssure Core.

10. Sur la page **Agents**, sélectionnez les agents à répliquer vers le core cible en utilisant le lecteur source.
11. Cliquez sur **Terminer**.
12. Si vous avez créé un lecteur source, envoyez-le au core cible.

    L'association d'un core source au core cible est terminée. La réplication commence, mais produit des points de restauration orphelins sur le core cible jusqu'à ce que le lecteur source soit consommé et fournisse les images de base.

Consommation du lecteur de départ sur un core cible

Cette procédure est nécessaire uniquement si vous avez créé un lecteur de départ au cours de la configuration de la réplication d'un core auto-géré.
Pour consommer le lecteur de départ sur un core cible :

1. Si le lecteur de départ a été enregistré sur un périphérique de stockage portable comme une clé USB, connectez ce lecteur au core cible.
2. Dans Core console sur le core source, cliquez sur l'onglet **Réplication**.
3. Sous **Réplication entrante**, sélectionnez le core source correct à l'aide du menu déroulant, puis cliquez sur **Consommer**.

   La fenêtre Consommer s'affiche.
4. Pour **Type d'emplacement**, sélectionnez l'une des options suivantes dans la liste déroulante :
   - Local
   - Réseau
   - Cloud
5. Saisissez les informations suivantes si nécessaire :

Zone de texte	Description
Emplacement	Entrez le chemin de l'emplacement du lecteur de départ, par exemple un lecteur USB ou un partage réseau (comme D:\).
Nom d'utilisateur	Entrez le nom d'utilisateur du lecteur ou dossier partagé. Le nom d'utilisateur est nécessaire uniquement pour un chemin réseau.
Mot de passe	Entrez le mot de passe du lecteur ou dossier partagé. Le mot de passe est nécessaire uniquement pour un chemin réseau.
Compte	Sélectionnez un compte dans la liste déroulante. Pour sélectionner un compte Cloud, vous devez, en premier lieu, avoir ajouté dans la Core Console.
Conteneur	Sélectionnez un conteneur associé à votre compte dans le menu déroulant.

Zone de texte	Description
Nom de dossier	Entrez le nom du dossier dans lequel les données archivées sont sauvegardées, par exemple : l'archivage - [DATE DE CRÉATION DE CRÉATION DE TEMPS] - []

6. Cliquez sur **Vérifier le fichier**.

   Une fois que le core a vérifié le fichier, il remplit automatiquement le champ **Plage de dates** avec les dates du point de restauration le plus ancien et du point de restauration le plus récent figurant dans le lecteur de départ. Il importe également les commentaires entrés dans Configuration de la réplication d'un core autogéré .

7. Sous **Noms d'agent** dans la fenêtre **Consommer**, sélectionnez les machines pour lesquelles vous voulez consommer les données, puis cliquez sur **Consommer**.

   REMARQUE : Pour surveiller l'avancement de la consommation des données, sélectionnez l'onglet **Événements**.

Abandon d'un lecteur de départ en attente

Si vous créez un lecteur de départ dans l'intention de le consommer sur le core cible, mais que vous choisissez de ne pas l'envoyer à l'emplacement distant, un lien correspondant à ce lecteur de départ en attente demeure dans l'onglet **Réplication** du core source. Vous pouvez abandonner ce lecteur en attente pour un préférer un autre ou des données de départ plus récentes.

REMARQUE : Cette procédure supprime le lien vers le lecteur source permanent de la Core Console sur le core source. Elle ne supprime pas le lecteur de l'emplacement de stockage où il est enregistré.

Pour abandonner un lecteur de départ en attente :

1. Dans Core console sur le core source, cliquez sur l'onglet **Réplication**.
2. Cliquez sur **Lecteur de départ en attente (No.)**.

   La section **Lecteurs de départ en attente** s'affiche. Elle inclut le nom du noyau cible distant, la date et l'heure de création du lecteur de départ, et la plage de données des points de restauration inclus dans le lecteur de départ.

3. Cliquez sur le menu déroulant correspondant au lecteur à abandonner, puis sélectionnez **Abandon**.

   La fenêtre **Lecteur de départ en attente** s'ouvre.

4. Cliquez sur **Oui** pour confirmer l'opération.

   Le lecteur de départ est supprimé. S'il n'en existe aucun autre sur le core source, la prochaine fois que vous ouvrirez l'onglet **Réplication**, vous ne verrez pas apparaître le lien **Lecteur de départ en attente (No.)** ni la section **Lecteurs de départ en attente**.

Réplication vers un core géré par un tiers

Un core tiers est un core cible géré et entretenu par un MSP. La réplication vers un core géré par un tiers ne nécessite pas que vous ayez accès à ce core cible. Une fois que le client a configuré la réplication sur le ou les cores source, le MSP effectue la configuration sur le core cible.

REMARQUE : Cette configuration s'applique à la réplication hébergée et dans le cloud. AppAssure Core doit être installé sur toutes les machines core source.

Configuration de la réplication vers un core cible géré par un tiers

REMARQUE : Cette configuration s'applique à la réplication hébergée et dans le cloud. Si vous configurez AppAssure pour une réplication multipoint à point, vous devez réaliser cette tâche sur tous les cores source.

Pour configurer la réplication d'un core géré par un tiers :

1. Naviguez jusqu'à la console Core, puis sélectionnez l'onglet **Réplication**.
2. Dans le menu déroulant **Actions**, sélectionnez **Ajouter un core distant**.
3. Dans la boîte de dialogue **Sélectionner un type de réplication**, sélectionnez l'option **Je possède un abonnement auprès d'un fournisseur tiers de services hors site de sauvegarde et de récupération après sinistre, et je souhaite répliquer mes sauvegardes vers ce service**, puis entrez les informations comme indiqué ci-dessous :

Zone de texte	Description
Nom d'hôte	Entrez le nom d'hôte, l'adresse IP ou le nom de domaine (FQDN) entièrement qualifié de la machine core distant.
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.

4. Cliquez sur **Continuer**.
5. Dans la boîte de dialogue **Ajouter un core distant**, effectuez les tâches suivantes :
   a. Sélectionnez les machines protégées à répliquer.
   b. Sélectionnez un référentiel pour chaque machine protégée.
   c. Entrez l'adresse e-mail de votre abonnement et l'ID client qui vous a été fourni par le fournisseur de service.
6. Si vous prévoyez d'effectuer le processus d'amorçage pour le transfert de données de la base, sélectionnez **Utiliser un lecteur de départ pour effectuer un transfert initial.**
7. Cliquez sur **Soumettre une demande**.

   REMARQUE : Si vous avez sélectionné l'option **Utiliser un lecteur de départ pour effectuer le transfert initial**, la boîte de dialogue **Copier vers le lecteur de départ** apparaît.
8. Dans la boîte de dialogue **Copier vers le lecteur d'amorçage**, entrez les informations du lecteur d'amorçage comme indiqué dans le tableau suivant.

Zone de texte	Description
Emplacement	Entrez le chemin du lecteur sur lequel vous souhaitez enregistrer les données initiales, tel qu'un lecteur USB local.
Nom d'utilisateur	Entrez le nom d'utilisateur en vue de la connexion au lecteur. REMARQUE : Ceci est obligatoire si le lecteur d'amorçage est situé sur un partage réseau.
Mot de passe	Entrez le mot de passe en vue de la connexion au lecteur. REMARQUE : Ceci est obligatoire si le lecteur d'amorçage est situé sur un partage réseau.

Zone de texte	Description
Taille maximale	Sélectionnez l'une des options suivantes : • La cible entière. • une partie de l'espace disponible sur le lecteur. Ensuite, pour désigner une partie du lecteur : a. Entrez le montant d'espace désiré dans la zone de texte. b. Sélectionnez la dimension.
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 ou n'efface aucune donnée existante de l'emplacement. Si celui-ci n'est pas vide, l'écriture de lecteur d'amorçage échoue. • **Remplacer ce core** : écrase toute donnée pré-existante appartenant à ce core mais laisse intactes les données des autres cores. • **Tout effacer** : efface toutes les données du répertoire avant d'écrire le lecteur d'amorçage.
Commentaire	Entrez un commentaire ou une description de l'archive.
Agents	Sélectionnez les agents que vous souhaitez répliquer à l'aide du lecteur d'amorçage.

REMARQUE : En raison d'importantes quantités de données devant être copiées dans le périphérique de stockage mobile, une connexion eSATA, USB 3.0 ou une autre connexion haut débit à ce périphérique de stockage mobile est recommandée.

9. Cliquez sur **Démarrer** pour écrire le lecteur de départ dans le chemin sélectionné.
10. Envoyez le lecteur de départ comme indiqué par le fournisseur de services tiers.

Passage en revue d'une demande de réplication

Une demande de réplication est envoyée depuis le core source au core cible tiers. En tant que tiers, vous pouvez passer la demande en revue, puis l'approuver pour lancer la réplication pour votre client ou la refuser pour empêcher la réplication.

Pour passer en revue une demande de réplication sur un core cible tiers :

1. Ouvrez Core Console sur le core cible, puis cliquez sur l'onglet **Réplication**.
2. Cliquez sur **Demandes en attente (Nbre)**.
   La section **Demandes de réplication en attente** s'affiche.
3. En regard de la demande à passer en revue, sélectionnez **Vérifier** dans le menu déroulant.
   La fenêtre **Vérifier la demande de réplication** s'affiche.

   REMARQUE : La demande remplie par le client détermine les informations affichées dans la section **Identité du core source**.
4. Dans la fenêtre Vérifier la demande de réplication, effectuez l'une des opérations suivantes :
   - Pour rejeter la demande, cliquez sur **Refuser**.
   - Pour approuver la demande :

1. – Sélectionnez **Remplacer un core répliqué existant**, puis sélectionnez un core à partir de la liste déroulante.
   – Sélectionnez **Créer une nouvelle source Core**. Vérifiez le **nom du core**, l' **adresse e-mail**du client et l'**ID du client**, et modifiez les informations si nécessaire.
2. Sous **Agents** sélectionnez les machines auxquelles l'approbation s'applique, puis sélectionnez le référentiel approprié pour chaque machine à l'aide de la liste déroulante.
3. (Facultatif) Entrez les remarques à afficher dans le champ **Commentaire**.
4. Cliquez sur **Envoyer la réponse**.

   La réplication est acceptée.

Non-prise en compte d'une demande de réplication

En tant que fournisseur de services tiers pour un core cible, vous pouvez choisir d'ignorer une demande de réplication émise par un client. Cette option peut être utile si un client envoie la demande par erreur ou si vous souhaitez rejeter une demande sans l'examiner au préalable.

Pour ignorer une demande de réplication :

1. Dans Core console sur le core source, cliquez sur l'onglet **Réplication**.
2. Dans l'onglet Réplication, cliquez sur **Demandes en attente (Nbre)**.
   La section **Demandes de réplication en attente** s'affiche.
3. En regard de la demande à ignorer, sélectionnez **Ignorer** dans le menu déroulant.
   Le core cible envoie une notification au core source pour luis indiquer que la demande a été ignorée.

Surveillance de la réplication

Lorsque la réplication est configurée, vous pouvez surveiller l'état des tâches de réplication des cores source et cible. Vous pouvez actualiser les informations d'état, afficher les détails concernant la réplication, et bien plus.

Pour surveiller la réplication :

1. Dans la Core Console, cliquez sur l'onglet **Réplication**.
2. Dans cet onglet, vous pouvez afficher les informations sur les tâches de réplication et surveiller leur état comme indiqué ci-dessous :

Tableau 3. Surveillance de la réplication

Section	Description	Actions disponibles
Demandes de réplication en attente	Affiche votre ID de client, l'adresse e-mail et le nom d'hôte lors de la soumission d'une demande à un fournisseur de services tiers (MSP). Ces informations sont affichées ici jusqu'à ce que le MSP accepte la demande.	Dans le menu déroulant, cliquez sur **Ignorer** pour ignorer ou rejeter la demande.
Lecteurs d'amorçage en attente	Affiche les lecteurs d'amorçage écrits mais pas encore consommés par le core cible. Il inclut le nom de core cible, la	Dans le menu déroulant, cliquez sur **Abandonner** pour abandonner ou annuler le processus de création des données de départ.

Section	Description	Actions disponibles
	date de création et la plage de dates.	
Réplication sortante	Affiche tous les cores cible sur lesquels le core source effectue une réplication. Cela inclut le nom de core distant, l'état d'existence, le nombre de machines protégées en cours de réplication et l'avancement d'une transmission de réplication.	Sur le core source, sélectionnez les options suivantes dans le menu déroulant : • **Détails** : répertorie l'ID, l'URI, le nom d'affichage, l'état, l'ID de client, l'adresse e-mail et les commentaires définis pour le core répliqué. • **Paramètres de modification** : répertorie le nom d'affichage et vous permet de modifier l'hôte et le port du core cible. • **Ajouter des agents** : vous permet de sélectionner un hôte dans une liste déroulante, sélectionner des machines protégées pour la réplication et créer un lecteur d'amorçage pour le transfert initial de la nouvelle machine protégée.
Réplication entrante	Affiche toutes les machines source depuis lesquelles la cible reçoit des données répliquées. Cela inclut le nom, l'état, les machines et l'avancement du core distant.	Sur le core cible, sélectionnez les options suivantes dans le menu déroulant : • **Détails** : répertorie l'ID, le nom d'hôte, l'ID de client, l'adresse e-mail et les commentaires définis pour le core répliqué. • **Consommer** : consomme les données initiales depuis le lecteur source, puis les enregistre dans le référentiel local.

3. Cliquez sur le bouton **Actualiser** pour mettre à jour les sections de cet onglet avec les dernières informations.

Paramètres de gestion de réplication

Vous pouvez régler un certain nombre de paramètres d'exécution de la réplication sur le core source et le core cible.

Pour gérer les paramètres de réplication :

1. Dans la Core Console, cliquez sur l'onglet **Réplication**.
2. Dans le menu déroulant **Actions**, cliquez sur **Paramètres**.
3. Dans la fenêtre **Paramètres de réplication**, modifiez les paramètres de réplication comme suit :

Option	Description
Durée de vie du cache	Indiquez une durée entre chaque demande d'état du core cible effectuée par le core source.
Délai d'attente de la session d'image de volume	Indiquez la période de temps pendant laquelle le core source tentera de transférer une image de volume vers le core cible.
Nombre maximal de tâches de réplication simultanées	Indiquez le nombre de machines protégées autorisées à répliquer vers le core cible à la fois.
Nombre maximal d'émissions parallèles	Indiquez le nombre de connexions réseau autorisées pour une utilisation par une seule machine protégée afin de répliquer les données de cette machine en une seule fois.

4. Cliquez sur **Enregistrer**.

Suppression d'une réplication

Vous pouvez supprimer une réplication et retirer des machines protégées d'une réplication de plusieurs façons. Les options disponibles sont les suivantes :

- Retrait d'un agent de la réplication sur le core source
- Suppression d'un agent du core cible
- Suppression d'un core cible de la réplication
- Suppression d'un core source de la réplication

REMARQUE : La suppression d'un core source entraîne la suppression de toutes les machines répliquées qui sont protégées par ce core.

Suppression d'une machine protégée de la réplication sur le Core source

Pour supprimer une machine protégée de la réplication sur le Core source :

1. Depuis le Core source, ouvrez la Core Console, puis cliquez sur l'onglet **Réplication**.
2. Développez la section **Réplication sortante**.
3. Dans le menu déroulant de la machine protégée que vous souhaitez supprimer de la réplication, cliquez sur **Supprimer.**
4. Dans la boîte de dialogue **Réplication sortante**, cliquez sur **Oui** pour confirmer la suppression.

Suppression d'une machine protégée sur le Core cible

Pour supprimer une machine protégée sur le Core cible :

1. Depuis le Core cible, ouvrez la Core Console, puis cliquez sur l'onglet **Réplication**.
2. Développez la section **Réplication entrante**.
3. Dans le menu déroulant de la machine protégée que vous souhaitez supprimer de la réplication, cliquez sur **Supprimer**, puis sélectionnez une des options suivantes.

Option	Description
Relation seulement	Supprime la machine protégée de la réplication mais conserve les points de restauration répliqués.
Avec point de restauration	Supprime la machine protégée de la réplication et supprime tous les points de restauration reçus de cette machine.

Supprimer un core cible de la réplication

Pour supprimer un core cible de la réplication :

1. Sur le core source, ouvrez Core Console, puis cliquez sur l'onglet **Réplication**.
2. Sous **Réplication sortante**, cliquez sur le menu déroulant en regard du noyau distant que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Dans la boîte de dialogue **Réplication sortante**, cliquez sur **Oui** pour confirmer la suppression.

Supprimer un core source de la réplication

REMARQUE : La suppression d'un core source entraîne la suppression de tous les agents répliqués protégés par ce core.

Pour supprimer un core source de la réplication

1. Depuis le core cible, ouvrez Core Console, puis cliquez sur l'onglet **Réplication**.
2. Sous **Réplication entrante** dans le menu déroulant, cliquez sur **Supprimer**, puis sélectionnez une des options suivantes.

Option	Description
Relation seulement	Retire le core source de la réplication mais conserve les points de restauration répliqués.
Avec les points de restauration	Retire le core source de la réplication et supprime tous les points de restauration reçus depuis cet ordinateur.

3. Dans la boîte de dialogue **Réplication entrante**, cliquez sur **Oui** pour confirmer la suppression.

Restauration de données répliquées

La fonctionnalité de réplication « au quotidien » est maintenue sur le core source, tandis que le core cible peut accomplir les fonctions nécessaires en cas de récupération après sinistre.

En cas de récupération après sinistre, le core cible peut utiliser les points de restauration répliqués pour restaurer les agents et le core protégés.

Réalisez les options de restauration suivantes depuis le core cible :

- Monter des points de restauration.
- Restaurer selon des points de restauration.
- Effectuer l'exportation d'une machine virtuelle (VM).
- Effectuer une restauration sans système d'exploitation (BMR).
- Effectuer la restauration (si vous avez configuré un environnement de réplication basculement/ restauration).

Schéma de basculement et restauration

Lorsqu'il se produit une panne de votre core source et de l'agent associé (une situation de sinistre), vous pouvez activer le basculement dans AppAssure pour transférer la protection à votre core (cible) de basculement identique et lancer un nouvel agent (répliqué) identique à l'agent en panne. Une fois vos core et agents source réparés, vous pouvez effectuer un basculement pour restaurer les données situées sur le core et l'agent de basculement vers le core et l'agent source. Dans AppAssure, le basculement et la restauration incluent les procédures suivantes.

- Configurer votre environnement pour le basculement.
- Effectuer le basculement du core cible et de son agent associé.
- Restaurer un core source grâce à une restauration.

Configuration d'un environnement pour le basculement

La configuration de votre environnement pour un basculement exige qu'une source et un Core cible soient configurés pour une réplication. Effectuez les étapes de cette procédure pour configurer la réplication pour le basculement

Pour configurer un environnement pour le basculement :

1. Installez un Core pour la source, puis installez un Core pour la cible.
2. Installez un AppAssure Agent devant être protégé par le core source.
3. Créez un référentiel sur le core source et une logithèque sur le core cible.

   Pour plus d'informations, voir Créer un référentiel.
4. Ajoutez l'agent à protéger sous le core source.

   Pour plus d'informations, voir Protéger un ordinateur.
5. Configurez la réplication du core source vers le core cible, puis répliquez l'agent protégé avec tous les points de restauration.

   Suivez les étapes dans la section Réplication vers un core autogéré pour ajouter le core cible vers lequel vous allez effectuer la réplication.

Exécution d'un basculement sur le Core cible

Lorsqu'il se produit un sinistre au cours duquel le core source et les machines protégées associées sont défaillants, vous pouvez activer le basculement pour transférer la protection vers le core (cible) de basculement identique. Le core cible devient le seul core protégeant les données dans votre environnement. Vous pouvez ensuite lancer un nouvel agent pour remplacer temporairement l'agent en panne.

Pour effectuer un basculement sur le core cible

1. Accédez à Core Console sur le core cible, puis cliquez l'onglet **Réplication**.
2. Sous **Réplication entrante**, sélectionnez le core source, puis développez les détails de l'agent voulu.
3. Dans le menu **Actions** de ce core, cliquez sur **Basculement**.

   L'état présenté pour cette machine dans ce tableau devient **Basculement**.
4. Cliquez sur l'onglet **Machines** (Ordinateurs), puis sélectionnez la machine ayant l'agent AppAssure associé avec les points de restauration.
5. Exportez les informations sur les points de restauration de sauvegarde sur cet agent vers une machine virtuelle.

6. Arrêtez la machine qui possède l'AppAssure agent.
7. Démarrez la machine virtuelle qui contient maintenant les informations sur les sauvegardes exportées.

   Vous devez attendre que le logiciel du pilote de périphérique soit installé.
8. Redémarrez la machine virtuelle, puis attendez que le service de l'agent démarre.
9. Retournez vers la Core Console du core cible, puis vérifiez que le nouvel agent apparait bien sur l'onglet **Machines** (Ordinateurs) sous **Machines protégées** et à l'onglet **Réplication** sous **Réplication entrante**.
10. Forcez plusieurs instantanés, puis vérifiez qu'ils s'exécutent correctement.

    Pour plus d'informations, voir Forcer un instantané.
11. Vous pouvez à présent procéder à un basculement.

    Pour plus d'informations, voir Exécution d'une restauration.

Effectuer une restauration

Après avoir réparé ou remplacé le core source d'origine et les machines protégées en échec, vous devez déplacer les données à partir des machines de basculement en échec pour restaurer les machines source.

Pour effectuer la restauration automatique :

1. Accédez à Core Console sur le core cible, puis cliquez l'onglet **Réplication**.
2. Sous **Réplication entrante**, sélectionnez l'agent de basculement, puis développez les détails.
3. Dans le menu **Actions**, cliquez sur **Restauration automatique**.

   La boîte de dialogue **Avertissements de restauration automatique** s'ouvre pour décrire les étapes que vous devez suivre avant de cliquer sur le bouton **Démarrer la restauration automatique**.
4. Cliquez sur **Annuler**.
5. Si la machine de basculement exécute Microsoft SQL Server ou Microsoft Exchange Server, arrêtez ces services.
6. Dans la console Core du core cible, cliquez sur l'onglet **Outils**.
7. Créez une archive de l'agent en basculement, puis exportez-la vers un disque ou un partage réseau.
8. Une fois l'archive créée, naviguez jusqu'à la console Core dans le core source récemment réparé, puis cliquez sur l'onglet **Outils**.
9. Importez l'archive que vous venez de créer au cours de l'étape 7.
10. Naviguez de nouveau jusqu'à la console Core sur le core cible, puis cliquez sur l'onglet **Réplication**.
11. Sous **Réplication entrante**, sélectionnez l'agent de basculement, puis développez les détails.
12. Dans le menu **Actions**, cliquez sur **Restauration automatique**.
13. Dans la boîte de dialogue **Avertissements de restauration automatique**, cliquez sur **Démarrer la restauration automatique**.
14. Arrêtez la machine qui contient l'agent exporté créé au cours du basculement.
15. Effectuez une restauration sans système d'exploitation (BMR) du core source et de l'agent.

    REMARQUE : Lorsque vous lancez la restauration, vous devez utiliser les points de restauration importés à partir du core cible vers l'agent sur la machine virtuelle.
16. Patientez jusqu'à ce que le BMR redémarre et le service d'agent démarre, puis affichez et enregistrez les détails de connexion réseau de la machine.
17. Naviguez jusqu'à la console Core sur le core cible source, puis sur l'onglet **Machines**, modifiez les paramètres de protection de la machine pour ajouter les détails de la nouvelle connexion réseau.
18. Naviguez jusqu'à la console Core sur le core cible, puis supprimez l'agent de l'onglet **Réplication**.

19. Dans la console Core sur le core source, redéfinissez la réplication entre la source et la cible en cliquant sur l'onglet **Réplication**, puis en ajoutant le core cible à la réplication.

Gestion des événements

La gestion des événements du core facilite la surveillance de l'intégrité et de l'utilisation du Core. Le core inclut des ensembles prédéfinis d'événements, qui peuvent être utilisés pour notifier les administrateurs de problèmes critiques sur le Core ou au cours de tâches de sauvegarde.

À partir de l'onglet **Événements**, vous pouvez gérer les groupes de notification, les paramètre SMTP d'e-mails, la réduction des répétitions et la rétention des événements. L'option Notification des groupes vous permet de gérer la notification des groupes, à partir desquels vous pouvez :

- Spécifier un événement pour lequel vous voulez générer une alerte pour l'un des éléments suivants :
  - Clusters
  - Capacité d'attachement
  - Tâches
  - Licences
  - Troncature du journal
  - Archivage
  - Service de core
  - Exportation
  - Protection
  - Réplication
  - Restauration
  - Paramètres du serveur SMTP
  - Activation des journaux de suivi
  - Configuration du Cloud
- Spécifiez le type d'alerte (erreur, avertissement et informationnel).
- Spécifiez à qui et où les alertes seront envoyées.
  - Adresse e-mail
  - Journaux d'événements Windows
  - Syslog Server
- Spécifiez un seuil horaire pour la répétition.
- Spécifiez la période de rétention pour tous les événements.

Configuration des groupes de notification

Pour configurer les groupes de notification :

1. Depuis le Core, sélectionnez l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Événements**.
3. Cliquez sur **Ajouter un groupe**.
   La boîte de dialogue **Ajouter un groupe de notification** s'affiche et présente trois volets :
   - **Généralités**
   - **Activez les événements**

- **Options de notification**

4. Dans le panneau **Généralités**, entrez les informations de base du groupe de notification, comme indiqué ci-dessous.

Zone de texte	Description
Nom	Entrez le nom d'un groupe de notification d'événement. Il est utilisé pour identifier le groupe de notification d'événement.
Description	Entrez la description du groupe de notification d'événement. Il est utilisé pour décrire le but du groupe de notification d'événement.

5. Dans le volet **Activer les événements**, sélectionnez les conditions dans lesquelles les journaux d'événements (alertes) seront créés et rapportés.

   Vous pouvez choisir de créer des alertes pour les éléments suivants :

   - **Tous les événements**
   - **Événements d'appliance**
   - **CD d'amorçage**
   - **Sécurité**
   - **Conservation de la base de données**
   - **LocalMount (Montage local)**
   - **Clusters**
   - **Notification**
   - **Scripts PowerShell**
   - **Installation en mode Push**
   - **Tâches nocturnes**
   - **Capacité d'attachement**
   - **Tâches**
   - **Licences**
   - **Troncature du journal**
   - **Archivage**
   - **Service de core**
   - **Exportation**
   - **Protection**
   - **Réplication**
   - **Référentiel**
   - **Restauration**
   - **Rollup (Cumul)**

6. Dans le volet **Options de notification**, spécifiez la méthode de prise en charge du processus de notification.

   Les options de notification sont les suivantes :

Zone de texte	Description
Notifier par courrier électronique	Désignez les destinataires de l'e-mail de notification. Vous pouvez choisir de spécifier plusieurs adresses e-mail ainsi que des adresses CC ou CCI. Vous disposez des options suivantes : • **À :**

Zone de texte	Description
	• **Cc** • **Cci :**
Notifier par journal d'événements Windows	Sélectionnez cette option si vous souhaitez que les alertes soient rapportées via le journal d'événements Windows. Cette option est utilisée pour spécifier si la notification d'alertes doit être rapportée via le journal d'événements Windows.
Notifier par syslogd	Sélectionnez cette option si vous souhaitez que les alertes soient signalées via syslogd. Spécifiez les détails de syslogd dans les zones de texte suivantes : • **Nom d'hôte :** • **Port : 1**

7. Cliquez sur **OK**.

Configuration d'un serveur de courrier électronique et d'un modèle de notification par courrier électronique

Pour recevoir des notifications par e-mail concernant les événements, configurez un serveur de messagerie et un modèle de notification par e-mail.

REMARQUE : Vous devez également configurer les paramètres de groupe de notifications, notamment activer l'option **Notifier par e-mail** préalablement à l'envoi de messages d'alerte par e-mail. Pour en savoir plus sur la façon d'indiquer les événements pour lesquels vous devez recevoir des alertes par e-mail, voir « Configuration des groupes de notification pour les événements système » dans le *Guide d'utilisation de l'appliance Dell DL4300*.

Pour configurer un serveur de messagerie et un modèle de notification par e-mail

1. Depuis le Core, sélectionnez l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Événements**.
3. Dans le volet **Paramètres SMTP d'e-mail**, cliquez sur **Modifier**.
   La boîte de dialogue Modifier la **configuration des notifications par e-mail** apparaît.
4. Sélectionnez **Activer les notifications par e-mail**, puis entrez des informations détaillées pour le serveur de messagerie de la façon décrite ci-dessous :

Zone de texte	Description
Serveur SMTP	Entrez le nom du serveur de messagerie que le modèle de notification par e-mail doit utiliser. Selon la convention de nommage, le nom inclut le nom d'hôte, le domaine et le suffixe, par exemple, **smtp.gmail.com**.
Port	Entrez un numéro de port qui identifiera le port d'un serveur de messagerie, par exemple, le port 587 pour Gmail. La valeur par défaut est 25.
Délai (secondes)	Entrez une valeur pour spécifier la durée de la tentative de connexion avant l'expiration du délai. Cette valeur s'utilise pour établir le temps en secondes avant la survenue de l'expiration d'un délai lors de tentatives de connexion au serveur d'e-mail.

Zone de texte	Description
	La valeur par défaut est de 30 secondes.
TLS	Sélectionnez cette option si le serveur de messagerie utilise une connexion sécurisée telle que TLS(Transport Layer Security) ou SSL (Secure Sockets Layer).
Nom d'utilisateur	Entrez un nom d'utilisateur pour le serveur de messagerie.
Mot de passe	Entrez un mot de passe pour le serveur de messagerie.
De	Entrez une adresse d'expéditeur qui servira à préciser l'adresse à laquelle le modèle de notification par e-mail sera retourné, par exemple, **noreply@localhost.com**.
Objet de l'e-mail	Entrez l'objet du modèle d'e-mail qui servira à définir l'objet d'un modèle de notification par e-mail, par exemple, `<hostname> – <level> <name>`.
E-mail	Entrez les informations de corps du modèle qui décrivent l'événement, le moment où il s'est produit et sa gravité.

5. Cliquez sur **Envoyer un e-mail test**, puis examinez les résultats.
6. Lorsque vous êtes satisfait des résultats des tests, cliquez sur **OK**.

Configuration de la réduction des répétitions

Pour configurer la réduction des répétitions :

1. Depuis le Core, sélectionnez l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Événements**.
3. Dans la zone **Réduction des répétitions**, cliquez sur **Modifier**.
   La boîte de dialogue Réduction des répétitions apparaît.
4. Sélectionnez **Activer la réduction des répétitions**.
5. Dans le champ **Stocker les événements pendant X minutes**, entrez le nombre de minutes pendant lesquelles les événements de réduction des répétitions doivent être stockés.
6. Cliquez sur **OK**.

Configuration de la rétention des événements

Pour configurer la rétention des événements :

1. Depuis le Core, sélectionnez l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Événements**.
3. Sous **Paramètres de connexion de base de données**, cliquez sur **Modifier**.
   La boîte de dialogue **Paramètres de connexion de base de données** s'affiche.
4. Dans le champ **Conserver l'historique des événements et des tâches pendant**, entrez le nombre de jours de conservation des informations concernant les événements.
   Par exemple, vous pouvez sélectionner 30 jours (valeur par défaut).
5. Cliquez sur **Enregistrer**.

Gestion de la restauration

Le Core peut immédiatement restaurer des données ou restaurer des ordinateurs à des machines physiques ou virtuelles à partir de points de restauration. Les points de restauration contiennent des instantanés de volumes d'agents capturés au niveau bloc. Ces instantanés prennent en compte les applications ; ainsi, toutes les transactions ouvertes et tous les journaux de transactions restaurées sont accomplis et les caches sont vidés sur le disque avant de créer l'instantané. L'utilisation d'instantanés prenant en compte l'application en conjonction avec Verified Recovery permet au Core d'effectuer plusieurs types de restauration, y compris :

- 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 ad-hoc et exportation continue sur des machines virtuelles

À propos des informations système

AppAssure vous permet d'afficher les informations concernant le Core qui incluent des informations sur le système, les volumes locaux et montés et les connexions du moteur AppAssure.

Si vous souhaitez démonter, individuellement ou dans leur ensemble, des points de restauration montés localement sur un core, vous pouvez le faire depuis l'option **Monter** de l'onglet **Outils**.

Affichage des informations système

Pour afficher les informations système :

1. Naviguez jusqu'au Core, puis sélectionnez l'onglet **Outils**.
2. Depuis l'option **Outils**, sélectionnez **Infos système**.

Téléchargement des programmes d'installation

Vous pouvez télécharger des programmes d'installation depuis le Core. Vous pouvez choisir de télécharger le programme d'installation de l'agent ou le Local Mount Utility depuis l'onglet **Outils**.

REMARQUE : Pour accéder au programme d'installation de l'agent, voir la section Téléchargement et installation du programme d'installation de l'agent. Pour plus d'informations sur le déploiement du programme d'installation de l'agent, voir le *Guide de déploiement de l'appliance Dell DL4300* disponible à l'adresse **Dell.com/support/home**. Pour accéder au programme d'installation de l'utilitaire Local Mount Utility, voir la section À propos de Local Mount Utility et pour en savoir plus sur l'utilitaire Local Mount Utility, voir la section Téléchargement et installation de l'utilitaire Local Mount Utility.

À propos du programme d'installation de l'agent

Le programme d'installation de l'agent sert à installer l'application AppAssure Agent sur les ordinateurs destinés à être protégés par le Core. Si vous estimez que votre ordinateur exige le programme d'installation de l'agent, vous pouvez télécharger ce programme depuis l'onglet **Outils** dans le Core.

REMARQUE : Le téléchargement du Core est effectué depuis le portail de licences. Pour télécharger le programme d'installation du Core, rendez-vous sur le site **https://licenseportal.com**.

Téléchargement et installation du programme d'installation de l'agent

Vous pouvez télécharger et déployer le programme d'installation de l'Agent sur n'importe quelle machine protégée par le Core.

Pour télécharger et installer le programme d'installation de l'agent :

1. Téléchargez le fichier de programme d'installation de l'agent depuis le portail de licences, ou depuis le Core.

   Par exemple : Agent-X64-5.3.x.xxxxx.exe
2. Cliquez **Enregistrer le fichier**.

   Pour en savoir plus sur l'installation des agents, voir le *Guide de déploiement de l'appliance DellDL4300* disponible à l'adresse **Dell.com/support/home**.

À propos de Local Mount Utility

L'utilitaire LMU (Local Mount Utility) est une application téléchargeable qui vous permet de monter un point de restauration sur un Core distant depuis n'importe quel ordinateur. L'utilitaire léger inclut les pilotes `aavdisk` et `aavstor`, mais il ne s'exécute pas en tant que service. Lors de l'installation de l'utilitaire, par défaut, il est installé dans le répertoire C:\Program Files\AppRecovery\Local Mount Utility et un raccourci s'affiche sur le bureau de l'ordinateur.

Bien que l'utilitaire ait été conçu pour l'accès à distance des cores, vous pouvez également installer le LMU sur le Core. Lorsqu'il s'exécute sur un Core, l'application reconnaît et affiche tous les montages depuis ce core, y compris les montages exécutés depuis Core Console. De même, les montages exécutés sur un LMU s'affichent également dans la console.

Téléchargement et installation de l'utilitaire Local Mount Utility

Pour télécharger et installer l'utilitaire Local Mount Utility :

1. Depuis l'ordinateur sur lequel vous souhaitez installer le LMU, accédez à Core Console en entrant l'URL de la console dans le navigateur puis en vous connectant à l'aide de votre nom d'utilisateur et votre mot de passe.
2. Dans la Core Console, cliquez sur l'onglet **Outils** .
3. Depuis l'onglet **Outils**, cliquez sur **Télécharger**.
4. Sous l'utilitaire **Local Mount Utility**, cliquez sur le lien **Télécharger le programme d'installation Web**.
5. Depuis la fenêtre **Ouvrir LocalMountUtility-Web.exe**, cliquez sur **Enregistrer le fichier**.

   Le fichier est enregistré dans le dossier Téléchargements locaux. Dans certains navigateurs, le dossier s'ouvre automatiquement.
6. Depuis le dossier **Téléchargements**, effectuez un clic droit sur le fichier exécutable Web **LocalMountUtility-Web**, puis sélectionnez **Ouvrir**.

En fonction de la configuration de votre ordinateur, la fenêtre **Contrôle du compte utilisateur** peut s'afficher.

7. Si la fenêtre **Contrôle du compte utilisateur** apparaît, cliquez sur **Oui** pour permettre au programme d'effectuer des modifications à l'ordinateur.

   L'Assistant **Installation de l'utilitaire Local Mount Utility** se lance.

8. Sur l'écran de **bienvenue** de l'Assistant **Installation de l'utilitaire Local Mount Utility**, cliquez sur **Suivant** pour passer à la page **Contrat de licence**.
9. Sur l'écran **Contrat de licence**, sélectionnez **J'accepte les termes du contrat de licence**, cliquez sur **Suivant** pour passer à l'écran **Conditions requises**.
10. Sur l'écran **Conditions requises**, installez les conditions requises nécessaires puis cliquez sur **Suivant** pour passer à l'écran **Options d'installation**.
11. Sur l'écran **Options d'installation**, effectuez les tâches suivantes :
    a. Sélectionnez un dossier de destination pour votre utilitaire LMU en cliquant sur le bouton **Modifier**.

       REMARQUE : Le dossier de destination par défaut est C:\Program Files\AppRecovery \LocalMountUtility.

    b. Choisissez si vous souhaitez ou pas **Autoriser l'utilitaire Local Mount Utility** à envoyer automatiquement des informations de diagnostic et d'utilisation à AppAssure Software, Inc.
    c. Cliquez sur **Suivant** pour avancer à la page **Avancement** et télécharger l'application. L'application est téléchargée dans le dossier de destination et l'avancement est affiché dans la barre d'avancement. Ensuite, l'Assistant avance directement à la page **Terminé**.
12. Cliquez sur **Terminer** pour fermer l'Assistant.

Ajout d'un core à l'utilitaire Local Mount Utility

Pour monter un point de restauration, vous pouvez ajouter le noyau au LMU. Il n'existe pas de limite au nombre de noyaux que vous pouvez ajouter.

Pour ajouter un core à l'utilitaire Local Mount Utility

1. Depuis la machine sur laquelle l'utilitaire LMU est installé, lancez l'utilitaire LMU en double cliquant sur l'icône bureau.
2. Si la fenêtre **Contrôle de compte d'utilisateur** apparaît, cliquez sur **Oui** pour permettre au programme d'apporter des modifications à la machine.
3. Dans le coin supérieur gauche de la fenêtre Local Mount Utility AppAssure, cliquez sur **Ajouter un core**.
4. Dans la fenêtre **Ajouter un core**, entrez les références demandées comme indiqué ci-dessous :

Zone de texte	Description
Nom de l'hôte	Le nom du core à partir duquel vous souhaitez monter les points de restauration. REMARQUE : Lors de l'installation de l'utilitaire LMU sur un core, l'utilitaire LMU ajoute automatiquement la machine hôte local.
Port	Le numéro de port utilisé pour la connexion au core. Le numéro de port par défaut est 8006.

Zone de texte	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 vos références Windows.
Nom d'utilisateur	Le nom d'utilisateur servant à accéder à la machine core. REMARQUE : Cette option est disponible uniquement si vous choisissez d'utiliser des références spécifiques.
Mot de passe	Le mot de passe utilisé pour accéder à la machine core. REMARQUE : Cette option est disponible uniquement si vous choisissez d'utiliser des références spécifiques.

5. Cliquez sur **Connexion** .
6. Lors de l'ajout de plusieurs cores, répétez les étapes 3 à 5, si nécessaire.

Exploration d'un point de restauration monté à l'aide de l'utilitaire LMU (Local Mount Utility)

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.

Pour explorer un point de restauration monté à l'aide de l'utilitaire Local Mount Utility :

1. Depuis la machine sur laquelle l'utilitaire LMU est installé, lancez l'utilitaire LMU en double cliquant sur l'icône bureau.
2. Depuis l'écran principal **Restauration du montage local**, cliquez sur **Montages actifs**.

   La fenêtre **Montages actifs** s'ouvre et affiche tous les points de restauration montés.
3. Cliquez sur **Explorer** en regard du point de restauration à partir duquel vous souhaitez effectuer la restauration pour ouvrir le dossier de volumes dédupliqués.

Montage d'un point de restauration à l'aide de Local Mount Utility (LMU)

Avant le montage d'un point de restauration, l'utilitaire LMU doit se connecter au Core sur lequel le point de restauration est stocké. Comme le décrit la section Ajouter un Core à Local Mount Utility, le nombre de cores pouvant être ajoutés à LMU est illimité ; toutefois, l'application ne peut se connecter qu'à un seul core à la fois. Par exemple, si vous montez le point de restauration d'un agent protégé par un core, puis celui d'un agent protégé par un autre core, LMU se déconnecte automatiquement du premier core pour établir la connexion avec le deuxième.

Pour démonter un point de restauration à l'aide de l'utilitaire Local Mount Utility :

1. Depuis la machine sur laquelle l'utilitaire LMU est installé, lancez l'utilitaire LMU en double cliquant sur l'icône bureau.
2. Depuis la fenêtre principale **AppAssure Local Mount Utility**, développez le core souhaité dans l'arborescence de navigation pour révéler les agents protégés.
3. Dans l'arborescence de navigation, sélectionnez l'agent désiré.

   Les points de restauration s'affichent dans le cadre principal.

4. Développez le point de restauration à monter pour révéler chaque volume de disque ou base de données.
5. Effectuez un clic droit sur le point de restauration à monter et sélectionnez l'une des options suivantes :
   - Monter
   - Monter en lecture-écriture
   - Monter avec les écritures précédentes
   - Montage avancé
6. Dans la fenêtre **Montage avancé**, complétez les options comme suit :

Zone de texte	Description
Chemin d'accès du point de montage	Pour sélectionner un chemin de point de restauration autre que le chemin de point de montage par défaut, cliquez sur le bouton **Parcourir**.
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

7. Cliquez sur **Monter.**

L'utilitaire LMU ouvre automatiquement le dossier qui contient le point de restauration monté.

REMARQUE : La sélection d'un point de restauration déjà monté entraîne l'affichage, dans la boîte de dialogue **Montage**, d'une invite de démontage du point de restauration.

Démontage d'un point de restauration à l'aide de Local Mount Utility

Pour démonter un point de restauration à l'aide de l'utilitaire Local Mount Utility :

1. Depuis la machine sur laquelle l'utilitaire LMU est installé, lancez l'utilitaire LMU en double cliquant sur l'icône bureau.
2. Depuis l'écran principal **Restauration du montage local**, cliquez sur **Montages actifs**.
   La fenêtre **Montages actifs** s'ouvre et affiche tous les points de restauration montés.
3. Sélectionnez l'une des options décrites dans le tableau ci-dessous pour démonter des points de restauration.

Option	Description
Démonter	Démonte uniquement le point de restauration adjoint. a. Cliquez sur **Démonter** à côté du point de restauration choisi. b. Fermez la fenêtre.
Démonter tout	Démonte tous les points de restauration montés. a. Cliquez sur **Démonter tout**. b. Dans la fenêtre **Démonter tout**, cliquez sur **Oui** pour confirmer. c. Fermez la fenêtre.

À propos de la barre de menus de l'utilitaire Local Mount Utility

La barre de menu du LMU se trouve dans la barre des tâches de votre bureau. Cliquez droit sur l'icône pour afficher les options suivantes :

Navigateur de points de restauration	Ouvre l'écran principal du LMU.
Montages actifs	Ouvre l'écran Montages actifs.
Options	Ouvre l'écran Options, dans lequel vous pouvez modifier le **Répertoire de point de montage par défaut**, les **références de core par défaut**, ainsi que la **langue** de l'interface utilisateur du LMU.
À propos de	Ouvre l'écran d'accueil des informations de licence.
Quitter	Ferme l'application.

REMARQUE : Le X dans le coin supérieur de l'écran principal réduit l'application dans la barre.

Utiliser Core et les options d'agent

En effectuant un clic droit sur le Core ou l'agent dans l'écran LMU principal, vous pouvez utiliser certaines options, notamment :

- Options Hôtelocal
- Options de core distant
- Options d'agent

Accès aux options de Localhost

Pour accéder aux options d'hôte local (Localhost), effectuez un clic droit sur le Core ou l'agent, puis cliquez sur **Reconnecter au core**. Les informations émises par le Core sont mises à jour et actualisées, notamment le nom des agents récemment ajoutés.

Accès aux options du core distant

Pour accéder aux options du core distant, effectuez un clic droit sur le Core ou l'agent, puis sélectionnez l'une des options de core distant décrites ci-dessous :

Option	Description
Se reconnecter au core	Actualise et met à jour les informations du core, tels que des agents ajoutés récemment.
Supprimer le core	Supprime le core de l'utilitaire **Local Mount Utility** (LMU).
Modifier le core	Ouvre la fenêtre **Modifier le core**, dans laquelle vous pouvez modifier le nom d'hôte, le port et les références.

Accès aux options d'agent

Pour accéder aux options d'agent, effectuez un clic droit sur le Core ou l'agent , puis cliquez sur **Actualiser les points de restauration**. La liste des points de restauration de l'agent sélectionné est mise à jour.

Gestion des stratégies de rétention

Les instantanés de sauvegarde périodique de tous les serveurs protégés s'accumulent sur le Core au fil du temps. Les stratégies de rétention servent à conserver plus longtemps les instantanés de sauvegarde et elles facilitent leur gestion. Un processus de cumul (rollup) applique la stratégie de rétention, et gère l'âge et la suppression des anciennes sauvegardes. Pour plus informations sur la configuration des stratégies de rétention, voir Personnalisation des paramètres des stratégies de rétention.

Archivage dans un Cloud

Vous pouvez archiver vos données vers un Cloud en les téléchargeant vers un large éventail de fournisseurs de Cloud, directement à partir de la console Core. Les Clouds compatibles sont notamment Windows Azure, Amazon, Rackspace et tous les fournisseurs OpenStack.

Pour exporter une archive vers un Cloud :

- ajoutez votre compte Cloud à Core Console. Pour en savoir plus, reportez-vous à Ajout d'un compte Cloud.
- Archive vos données et les exporter vers votre compte Cloud.
- Récupérer des données archivées en l'important à partir du Cloud.

À propos de l'archivage

Les stratégies de conservation définissent les périodes de stockage des sauvegardes sur support à court terme (rapide et cher). Parfois, certaines contraintes techniques et professionnelles imposent de conserver les sauvegardes plus longtemps, mais l'utilisation du stockage rapide est particulièrement onéreuse. Par conséquent, il devient nécessaire d'utiliser un stockage à long terme (lent et économique). Les entreprises utilisent souvent le stockage à long terme pour l'archivage des données de conformité et de non-conformité. La fonction d'archivage d'AppAssure permet de prendre en charge la conservation étendue des données de conformité et de non-conformité ; elle permet également de créer des données de réplication source sur un core de réplique distant.

Création d'une archive

Pour créer une archive

1. Dans la console Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Archive**.
   La boîte de dialogue **Créer une archive** apparaît.
3. Dans la boîte de dialogue **Créer une archive**, entrez les détails de l'archive comme indiqué ci-après :

Zone de texte	Description
Plage de dates	Pour spécifier la plage de dates, entrez les dates de début et de fin.
Mot de passe de l'archive	Entrez un mot de passe pour l'archive. Il est utilisé pour établir les coordonnées de connexion pour sécuriser l'archive.

Zone de texte	Description
Confirmer	Ressaisissez le mot de passe pour sécuriser l'archive. Il est utilisé pour valider les informations que vous avez saisies dans la zone de texte **Mot de passe d'archive**.
Emplacement de sortie	Saisissez l'emplacement de la sortie. Il est utilisé pour définir le chemin de l'emplacement où vous souhaitez que l'archive réside. Il peut s'agir d'un disque local ou d'un partage réseau. Par exemple, **d:\work\archive** ou **\\servername \sharename** pour les chemins réseau. **REMARQUE :** Si l'emplacement de sortie est un partage réseau, vous devrez entrer un nom d'utilisateur et un mot de passe pour vous connecter au partage.
Nom d'utilisateur	Entrez un nom d'utilisateur. Il est utilisé pour établir les coordonnées de connexion du partage réseau.
Mot de passe	Entrez un mot de passe pour le partage réseau. Il est utilisé pour établir les coordonnées de connexion du partage réseau.
Taille maximale	Entrez la quantité d'espace à utiliser pour l'archive. Vous avez le choix entre : • Cible entière • Quantité spécifique en Mo ou Go
Action de recyclage	Sélectionnez l'action de recyclage appropriée.
Commentaire	Entrez toute information supplémentaire nécessaire pour l'archive.

4. Cliquez sur **Archive**.

Définition d'un archivage planifié

La fonction d'archivage planifié permet de définir une durée pendant laquelle un ordinateur sélectionné sera créé automatiquement et enregistré à l'emplacement indiqué. Ceci est pratique dans les cas où vous pouvez souhaiter les archivages et les sauvegardes fréquentes d'un ordinateur, sans avoir besoin de devoir créer les archives manuellement. Suivez les étapes de la procédure suivante pour planifier l'archivage automatique.
Pour définir une archive planifiée :

1. Dans Core Console, cliquez sur l'onglet **Outils**.
2. Depuis l'option **Archive**, sélectionnez **Planifié**.
3. sur la page Archive Planifiée, cliquez sur **Ajouter**.
   La boîte de dialogue **Assistant Ajouter une archive** apparaît.
4. Sur la page **Emplacement** de l'**Assistant Ajout d'une archive**, sélectionnez l'une des options suivantes dans la liste déroulante **Type d'emplacement** :
   - local : emplacement de sortie : permet d'entrer l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.
   - Réseau
     - Emplacement de sortie : indiquez l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.

- Nom d'utilisateur : entrez un nom d'utilisateur. Il est utilisé pour établir les références pour le partage du réseau.
- Mot d passe : entrez un mot de passe pour le chemin d'accès au réseau. Il est utilisé pour établir les références pour le partage du réseau.

• Cloud

- Compte : sélectionnez un compte dans la liste déroulante. Pour sélectionner un compte Cloud, vous devez, en premier lieu, l'avoir ajouté dans la Core Console.
- Conteneur : sélectionnez un conteneur associé à votre compte dans le menu déroulant.
- Nom de dossier : entrez un nom pour le dossier où les données d'archive doivent être enregistrées. Le nom par défaut est AppAssure 5-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION].

5. Cliquez sur **Suivant**.
6. Dans la page **Machines** de l'assistant, sélectionnez les machines protégées contenant les points de restauration à archiver.
7. Cliquez sur **Suivant**.
8. Sur la page**Options**, sélectionnez dans la liste déroulante, l'une des options Recycle Actions (Actions de recyclage) suivantes :
   - **Remplacer ce Core** : écrase toutes les données archivées pré-existantes appartenant à ce Core mais laisse intactes les données des autres Cores.
   - **Effacer complètement** : efface toutes les données archivées du répertoire avant d'écrire la nouvelle archive.
   - **Incrémentielle** : permet d'ajouter des points de restauration à une archive existante. Cette option compare les points de restauration pour éviter la duplication des données qui existent déjà dans l'archive.
9. Sur la page **Programmation**, sélectionnez l'une des options de fréquence d'envoi de données suivantes :
   - Tous les jours : au moment : sélectionnez l'heure de la journée où vous voulez créer une archive.
   - Toutes les semaines
     - Au jour de la semaine : sélectionnez le jour de la semaine pour créer automatiquement l'archive.
     - À l'heure : sélectionnez l'heure du jour à laquelle vous souhaitez créer une archive.
   - Tous les mois
     - Au jour du mois : sélectionnez le jour du mois où pour créer automatiquement l'archive.
     - À l'heure : sélectionnez l'heure du jour à laquelle vous souhaitez créer une archive.
10. Pour suspendre l'archivage à des fins de reprise ultérieurement, sélectionnez **Initial suspendre l'archivage**.

    Il se peut que vous souhaitiez interrompre l'opération d'archivage planifiée si vous donne davantage de temps pour préparer l'emplacement cible avant d'archiver les reprend. Si vous ne sélectionnez pas cette option, l'archivage commence à l'heure planifiée.
11. Cliquez sur **Terminer**.

Interruption ou reprise du traitement d'archivage planifié

Si vous avez intialement opté pour la suspension de l'archivage lorsque vous avez effectué cette procédure de définition d'archivage planifié, vous pouvez souhaiter reprendre l'opération d'archivage planifiée à une date ultérieure.

Pour interrompre ou reprendre le traitement d'archivage planifié :

1. Accédez à **Core Console**, puis sélectionnez l'onglet **Outils**.
2. Depuis l'option **Archive**, sélectionnez **Planifié**.
3. Dans la page **Archive Planifiée**, effectuez l'une des actions suivantes :
   - sélectionnez l'archive préférée, puis cliquez sur l'une des actions suivantes selon le cas :
     - pause
     - reprise
   - En regard de l'archive préférée, cliquez sur le menu déroulant, puis cliquez sur l'une des actions suivantes selon le cas :
     - pause
     - reprise

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

Modification d'un archivage planifié

1. Dans Core Console, cliquez sur l'onglet **Outils**.
2. Depuis l'option **Archive**, sélectionnez **Planifié**.
3. Sur la page Archive planifiée, cliquez sur le menu déroulant en regard de l'archive que vous souhaitez modifier, puis cliquez sur **Modifier**.

   La boîte de dialogue **Assistant Ajouter une archive** apparaît.
4. Sur la page **Emplacement** de l'**Assistant Ajout d'une archive**, sélectionnez l'une des options suivantes dans la liste déroulante**Type d'emplacement** :
   - local : emplacement de sortie : permet d'entrer l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.
   - Réseau
     - Emplacement de sortie : indiquez l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.
     - Nom d'utilisateur : entrez un nom d'utilisateur. Il est utilisé pour établir les références pour le partage du réseau.
     - Mot d passe : entrez un mot de passe pour le chemin d'accès au réseau. Il est utilisé pour établir les références pour le partage du réseau.
   - Cloud
     - Compte : sélectionnez un compte dans la liste déroulante. Pour sélectionner un compte Cloud, vous devez, en premier lieu, l'avoir ajouté dans la Core Console.
     - Conteneur : sélectionnez un conteneur associé à votre compte dans le menu déroulant.
     - Nom de dossier : entrez un nom pour le dossier où les données d'archive doivent être enregistrées. Le nom par défaut est AppAssure 5-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION].
5. Cliquez sur **Suivant**.
6. Dans la page **Machines** de l'assistant, sélectionnez les machines protégées contenant les points de restauration à archiver.
7. Cliquez sur **Suivant**.
8. Sur la page **Programmation**, sélectionnez l'une des options de fréquence d'envoi de données suivantes :

- Tous les jours : au moment : sélectionnez l'heure de la journée où vous voulez créer une archive.
- Toutes les semaines
  - Au jour de la semaine : sélectionnez le jour de la semaine pour créer automatiquement l'archive.
  - À l'heure : sélectionnez l'heure du jour à laquelle vous souhaitez créer une archive.
- Tous les mois
  - Au jour du mois : sélectionnez le jour du mois où pour créer automatiquement l'archive.
  - À l'heure : sélectionnez l'heure du jour à laquelle vous souhaitez créer une archive.

9. Pour suspendre l'archivage à des fins de reprise ultérieurement, sélectionnez **Initial suspendre l'archivage**.

   Il se peut que vous souhaitiez interrompre l'opération d'archivage planifiée si vous donne davantage de temps pour préparer l'emplacement cible avant d'archiver les reprend. Si vous ne sélectionnez pas cette option, l'archivage commence à l'heure planifiée.
10. Cliquez sur **Terminer**.

Vérification d'une archive

Vous pouvez effectuer le balayage d'une archive en vue de l'intégrité de la structure en exécutant une vérification de l'archive. Ce contrôle vérifie la présence de tous les fichiers nécessaires au sein de l'archive. Pour effectuer une vérification de l'archive, suivez les étapes de la procédure suivante :

1. dans Core Console, cliquez sur l'onglet **Outils**.
2. depuis l'option **Archive**, sélectionnez **Vérifier Archive**.

   La boîte de dialogue **Vérifier une archive** apparaît.
3. Sélectionnez l'une des options suivantes dans la liste :
   - local : emplacement de sortie : permet d'entrer l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.
   - Réseau
     - Emplacement de sortie : indiquez l'emplacement de la sortie. Il définit le chemin de l'emplacement où vous souhaitez que l'archive réside.
     - Nom d'utilisateur : entrez un nom d'utilisateur. Il est utilisé pour établir les références pour le partage du réseau.
     - Mot d passe : entrez un mot de passe pour le chemin d'accès au réseau. Il est utilisé pour établir les références pour le partage du réseau.
   - Cloud
     - Compte : sélectionnez un compte dans la liste déroulante. Pour sélectionner un compte cloud, vous devez, en premier lieu, l'avoir ajouté dans la Core Console.
     - Conteneur : sélectionnez un conteneur associé à votre compte dans le menu déroulant.
     - Nom de dossier : entrez un nom pour le dossier où les données d'archive doivent être enregistrées. Le nom par défaut est AppAssure-5-Archive-[DATE DE CRÉATION]-[HEURE DE CRÉATION].
4. Pour vérifier l'intégrité de la structure, sélectionnez **Structure d'intégrité**.
5. Cliquez sur **Vérifier le fichier**.

Importation d'une archive

Pour importer une archive :

1. Dans la console Core, sélectionnez l'onglet **Configuration**.
2. Sous l'option **Gérer**, sélectionnez **Archive** puis **Importer**.
   La boîte de dialogue **Importer une archive** apparaît.
3. Dans la boîte de dialogue **Importer une archive**, entrez les détails nécessaires pour importer une archive, comme indiqué ci-dessous :

Zone de texte	Description
Emplacement d'entrée	Sélectionnez l'emplacement d'importation de l'archive.
Nom d'utilisateur	Pour établir l'accès de sécurisation de l'archive, entrez les références de connexion.
Mot de passe	Entrez un mot de passe pour accéder à l'archive.

4. Cliquez sur **Vérifier le fichier** pour valider l'existence de l'archive à importer.
   La boîte de dialogue **Restaurer** apparaît.
5. Dans la boîte de dialogue **Restaurer**, vérifiez le nom du core source.
6. Sélectionnez les agents à importer depuis l'archive.
7. Sélectionnez le référentiel.
8. Cliquez sur **Restaurer** pour importer l'archive.

Gestion de la capacité d'attachement SQL

La configuration de la capacité d'attachement SQL permet à Core d'attacher une base de données SQL et des fichiers journaux dans un instantané d'un serveur SQL, à l'aide d'une instance locale de Microsoft SQL Server. Le test de capacité d'attachement permet au Core de vérifier la cohérence des bases de données SQL et garantit que tous les fichiers de données (MDF et LDF) sont disponibles dans l'instantané de sauvegarde. Les contrôles de capacité d'attachement peuvent être exécutés à la demande pour des points de restauration spécifiques ou dans le cadre d'une tâche exécutée pendant la nuit.

La capacité d'attachement nécessite une instance locale de Microsoft SQL Server sur la machine AppAssure Core. Cette instance doit être une version sous licence complète de SQL Server fournie par Microsoft ou l'un de ses revendeurs agréés. Microsoft interdit l'utilisation de licences SQL passives.

La fonction de capacité d'attachement prend en charge SQL Server 2005, 2008, 2008 R2, 2012 et 2014. Le compte utilisé pour exécuter le test doit disposer du rôle sysadmin sur l'instance SQL Server.

Le format de stockage sur disque SQL Server est identique dans les environnements 64 bits et 32 bits ; la capacité d'attachement fonctionne donc dans les deux versions. Une base de données détachée d'une instance de serveur qui fonctionne dans un environnement peut être attachée à une instance de serveur exécutée dans un autre environnement.

△ **PRÉCAUTION : La version de SQL Server installée sur le core doit être identique (ou supérieure) à la version de SQL Server présente sur tous les agents où SQL Server est installé.**

Configuration des paramètres de la capacité d'attachement SQL

Avant d'exécuter les vérification de capacité d'attachement sur les bases de données SQL protégées, sélectionnez une instance locale de SQL Server sur la machine de core qui servira à exécuter les vérifications sur la machine d'agent.

REMARQUE : La capacité d'attachement nécessite une instance locale de Microsoft SQL Server sur la machine AppAssure Core. Cette instance doit être une version sous licence complète de SQL Server fournie par Microsoft ou l'un de ses revendeurs agréés. Microsoft interdit l'utilisation de licences SQL passives.

Pour configurer les paramètres de la capacité d'attachement SQL :

1. Accédez à Core Console, puis sélectionnez l'onglet.
2. Cliquez sur **Configuration** → **Paramètres**.
3. Dans le volet Tâches nocturnes, cliquez sur **Modifier**.

   La boîte de dialogue **Tâches nocturnes** s'affiche.
4. Sélectionnez **la vérification de capacité d'attachement**, puis cliquez sur **Paramètres**.
5. Utilisez les menus déroulants pour sélectionner l'instance de SQL Server installée sur le Core parmi les options suivantes :

   Choisissez parmi les options suivantes :

   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. Sélectionnez le type de référence.

   Choisissez parmi les options suivantes :

   - **Windows**
   - **SQL**
7. Spécifiez les références avec privilèges d'administrateur des instances Windows ou SQL Server, comme indiqué ci-dessous :

Zone de texte	Description
Nom d'utilisateur	Entrez un nom d'utilisateur pour les permissions de connexion à SQL Server.
Mot de passe	Entrez un mot de passe pour la capacité d'attachement SQL. Il est utilisé pour contrôler les activités de connexion.

8. Cliquez sur **Test de connexion**.

   REMARQUE : Si vous avez entré les références incorrectement, un message s'affiche pour vous signaler que le test des références a échoué. Corrigez les informations de références et exécutez à nouveau le test de connexion.
9. Cliquez sur **Enregistrer**.

   Les vérifications de capacité d'attachement sont à présent disponibles pour l'exécution sur les bases de données SQL Server protégées.
10. Dans la fenêtre Tâches nocturnes, cliquez sur **OK**.

    Les vérifications de capacité d'attachement sont à présent programmées pour se produire avec les tâches nocturnes.

Configuration des vérifications de capacité d'attachement et de troncature des journaux SQL nocturnes

Pour configurer des vérifications de capacité d'attachement SQL et de troncature de journaux nocturnes

1. Dans la zone de navigation de gauche de Core, sélectionnez la machine pour laquelle vous souhaitez effectuer la vérification nocturne de capacité d'attachement et la troncature des journaux, puis cliquez sur **Paramètres SQL Server**.
2. naviguez jusqu'à Core Console.
3. cliquez sur **Configuration** → **Paramètres**.
4. Dans la section **Tâches nocturnes**, cliquez sur **Modifier**.
5. Sélectionnez ou supprimez les paramètres SQL Server suivants en fonction des besoins de votre organisation :
   - **Tâche de vérification de la capacité d'attachement**
   - **Tâche de troncature du journal (modèle à récupération simple uniquement)**
6. Cliquez sur **OK**.

   Les paramètres de capacité d'attachement et de troncature des journaux prennent effet pour le SQL Server protégé.

Gestion des vérifications de montabilité de base de données Exchange et de la troncature des journaux

Lorsque vous utilisez AppAssure pour sauvegarder des serveurs Microsoft Exchange, vous pouvez effectuer des vérifications de montabilité sur toutes les bases de données après chaque instantané. Cette fonction de détection de corruption signale des échecs éventuels aux administrateurs et assure que toutes les données des serveurs Exchange sont bien restaurées en cas de panne.

REMARQUE : Les fonctions de vérifications de montabilité et de troncature des journaux s'appliquent uniquement à Microsoft Exchange 2007, 2010 et 2013. De plus, le rôle d'Administrateur organisationnel doit être attribué au compte de service de l'agent AppAssure dans Exchange.

Configuration de la montabilité de base de données Exchange et de la troncature des journaux

Vous pouvez afficher, activer ou désactiver les paramètres de serveur de base de données Exchange, y compris la vérification de montabilité automatique, la vérification de somme contrôle nocturne ou la troncature nocturne des journaux.

Pour configurer la montabilité de la base de données et de la troncature des journaux :

1. Dans le volet de navigation de Core Console, sélectionnez l'ordinateur dont vous souhaitez configurer les vérifications de montabilité et/ou la troncature des journaux.

   L'onglet **Récapitulatif** de l'ordinateur sélectionné apparaît.
2. Cliquez sur **Paramètres Exchange Server**.

   La boîte de dialogue **Paramètres Exchange Server** s'affiche.
3. Sélectionnez ou supprimez les paramètres Exchange Server suivants en fonction des besoins de votre organisation :
   - **Activer la vérification de montabilité automatique**
   - **Activer la vérification de somme de contrôle nocturne**

- **Activer la troncature nocturne des journaux**

4. Cliquez sur **OK**.

   Les paramètres de montabilité et de troncature des journaux prennent effet pour le serveur Exchange protégé.

   REMARQUE : Pour en savoir plus sur le forçage de la troncature des journaux, voir Forcer la troncature des journaux .

Forçage d'une vérification de montabilité

Pour forcer une vérification de montabilité :

1. Dans la zone de navigation de gauche de Core Console, sélectionnez la machine pour laquelle vous souhaitez forcer la vérification de montabilité, puis cliquez sur l'onglet **Points de restauration**.
2. Cliquez sur **>** en regard d'un point de restauration dans la liste pour développer la vue.
3. Cliquez sur Forcer la **Vérification de montabilité**.

   Un message vous invite à forcer une vérification de montabilité.
4. Cliquez sur **Oui**.

   REMARQUE : Pour obtenir des instructions sur la façon d'afficher l'état des vérifications de capacité d'attachement, voir Affichage des événements et des alertes.

   Le système effectue une vérification de montabilité.

Forçage des vérifications de somme de contrôle

Pour forcer une vérification de somme de contrôle :

1. Dans la zone de navigation gauche de la console AppAssure Core, sélectionnez l'ordinateur pour lequel vous souhaitez forcer la vérification de somme de contrôle, puis cliquez sur l'onglet **Points de restauration**.
2. Cliquez sur **>** en regard d'un point de restauration dans la liste pour développer la vue.
3. Cliquez sur **Forcer la vérification de somme de contrôle**.

   La fenêtre **Forcer la vérification de capacité d'attachement** apparaît. Indiquez si vous souhaitez forcer une vérification de capacité d'attachement.
4. Cliquez sur **Oui**.

   Le système effectue une vérification de somme de contrôle.

   REMARQUE : Pour en savoir plus sur l'affichage de l'état des vérifications de capacité d'attachement, voir Affichage des événements et des alertes .

Forcer la troncature des journaux

REMARQUE : Cette option est uniquement disponible pour les ordinateurs Exchange ou SQL.

Pour forcer la troncature des journaux :

1. Accédez à Core Console, puis sélectionnez l'onglet **Machines**.
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de l'ordinateur dont vous souhaitez tronquer le journal.
   - Ou bien, dans le volet de navigation, sélectionnez l'ordinateur dont vous souhaitez tronquer le journal.

3. Dans le menu déroulant **Actions** de cet ordinateur, cliquez sur **Forcer la troncature des journaux**.
4. Confirmez si le forçage de la troncature du journal doit continuer.

Indicateurs d'état des points de restauration

Suite à la création d'un point de restauration sur un serveur SQL ou Exchange protégé, l'application affiche un indicateur d'état de couleur correspondante dans le tableau **Points de restauration**. La couleur affichée est basée sur les paramètres de vérification de l'ordinateur protégé et sur la réussite ou l'échec de ces vérifications, tel que décrit dans les tableaux suivants.

REMARQUE : Pour plus d'informations sur l'affichage des points de restauration, reportez-vous à la section Affichage de points de restauration.

Le tableau suivant affiche les indicateurs d'état qui s'affichent pour les bases de données SQL.

Couleurs d'état des points de restauration des bases de données SQL

Couleur d'état	Description
Blanc	Indique que l'une des conditions suivantes existe : • Il n'existe pas de base de données SQL • Les vérifications de capacité d'attachement sont désactivées • Les vérifications de capacité d'attachement n'ont pas encore été exécutées
Jaune	Indique que la base de données SQL est hors ligne et une vérification est impossible.
Rouge	Indique que la vérification de capacité d'attachement a échoué.
Vert	Indique que la vérification de capacité d'attachement a été réussi.

Le tableau suivant affiche les indicateurs d'état qui s'affichent pour les bases de données Exchange.

Couleurs d'état des points de restauration des bases de données Exchange

Terme	Description
Blanc	Indique que l'une des conditions suivantes existe : • Il n'existe pas de base de données Exchange • Les vérifications de montabilité n'ont pas été activées. **REMARQUE :** Ceci peut s'appliquer à certains volumes dans un point de restauration.
Jaune	Indique que les vérifications de montabilité de la base de données Exchange sont activées, mais les vérifications n'ont pas encore été exécutées.
Rouge	Indique que les vérifications de montabilité ou les vérifications de somme de contrôle ont échoué au moins sur une base de données.
Vert	Indique que la vérification de montabilité ou la que la vérification de somme de contrôle a réussi.

REMARQUE : Les points de restauration sans base de données Exchange ou SQL sont affichés avec un indicateur d'état blanc. Dans les cas où le point de restauration possède une base de données Exchange ou SQL, l'indicateur d'état le plus grave s'affiche pour ce point de restauration.

3

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.

Surveillance de l'état de l'appliance

Vous pouvez surveiller le statut des sous-systèmes de l'appliance en utilisant l'onglet **Appliance** de la page **Statut général**. La page **Statut général** affiche un voyant de statut en regard de chaque sous-système, ainsi que la description du statut qui indique l'état d'intégrité du sous-système.

La page État global fournit également des liens vers des outils permettant d'effectuer une analyse en cascade (drill down) des détails de chaque sous-système. Cela peut s'avérer utile pour le dépannage en cas d'avertissement ou d'erreur. Le lien **System Administrator**, disponible pour les sous-systèmes Matériel de l'appliance et Matériel de stockage, vous invite à vous connecter à l'application System Administrator, qui sert à gérer le matériel. Pour plus d'informations sur l'application System Administrator, consultez le manuel *OpenManage Server Administrator User's Guide* (Guide de l'utilisateur OpenManage Server Administrator), à l'adresse **dell.com/support/home**. Le lient **État de provisionnement**, disponible pour le sous-système Provisionnement du stockage, ouvre l'écran **Tâches**, qui affiche l'état de provisionnement de ce sous-système. Si le stockage est disponible pour provisionnement, un lien vers l'option **Provisionner** de la liste **Actions** apparaît en regard de la tâche de provisionnement.

Provisionnement du stockage

L'appliance configure le stockage interne DL4300 disponible et tout boîtier de stockage externe attaché pour :

- Référentiels AppAssure

  REMARQUE : Si l'adaptateur de bus hôte Fibre Channel est configuré, le processus de création de référentiels est manuel. AppAssure ne permet pas de créer un référentiel automatiquement dans le répertoire racine. Pour plus d'informations, reportez-vous au *Guide de déploiement de l'appliance Dell DL4300*.
- Mode Veille virtuelle des machines protégées

REMARQUE : Des MD1400 dotés de lecteurs 1 To, 2 To, 4 To ou 6 To (capacité élevée) connectés au contrôleur H830 sont pris en charge. Jusqu'à quatre MD 1400 sont pris en charge.

REMARQUE : La configuration DL4300 High-Capacity prend en charge l'adaptateur SAS PERC H830 ou ou deux HBA Fibre Channel. Pour en savoir plus sur la configuration des HBA Fibre Channel, voir le livre blanc *DL4xxx : Implémentation de Fibre Channel* sur **dell.com/support/home**.

Avant de commencer à provisionner le stockage sur le disque, déterminez la quantité de stockage dont vous avez besoin pour les machines virtuelles de secours. Vous pouvez attribuer aux VM hôtes de secours le pourcentage de votre choix par rapport à la capacité disponible. Par exemple, si vous utilisez la gestion

des ressources de stockage (Storage Resource Management, SRM), vous pouvez allouer jusqu'à 100 % de la capacité sur tous les périphériques qui sont provisionnés sur des machines virtuelles hôtes. Avec la fonction Live Recovery d'AppAssure, vous pouvez utiliser ces machines virtuelles pour remplacer rapidement tous les serveurs en échec protégés par l'appliance.

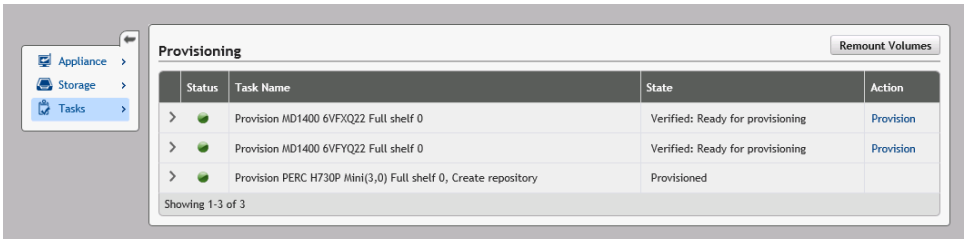
Sur la base d'un environnement de taille moyenne qui ne nécessite aucune machine virtuelle de secours, vous pouvez utiliser l'intégralité du stockage pour sauvegarder un nombre significatif d'agents. Toutefois, si vous avez besoin de davantage de ressources pour les VM de secours et que vous sauvegardez moins de machines d'agent, vous pouvez allouer plus de ressources aux VM de plus grande taille.

Lorsque vous cliquez sur l'onglet **Appliance**, le logiciel AppAssure Appliance repère l'espace de stockage disponible sur l'ensemble des contrôle pris en charge dans le système et vérifie que le matériel répond à la configuration requise.

Pour effectuer le provisionnement de disque pour tout le stockage disponible :

1. Dans l'onglet **Appliance** , cliquez sur **Tâches** → **Provisionnement**.
   L'écran **Provisionnement** affiche la capacité estimée pour le provisionnement. Cette capacité est utilisée pour créer un nouveau référentiel AppAssure.

   PRÉCAUTION : Avant de continuer, s'assurer que les étapes 2 à 4 sont suivies dans cette procédure.
2. Ouvrez la fenêtre **Storage (Stockage) de provisionnement** en cliquant sur **Provision** (Fournir des infos de paramétrage) dans la colonne Action, en regard du stockage auquel vous souhaitez fournir les infos de paramétrage.
3. Dans la section **Réserve de stockage facultative** , cochez la case en regard d' **allouer une portion du stockage aux machines virtuelles en mode Veille en cours de provisionnement ou à d'autres fins** et indiquer un pourcentage de stockage à allouer. Dans le cas contraire, le pourcentage de stockage indiqué dans la section **Réserve de stockage en option** seront pris sur tous les disques connectés.
4. Cliquez sur **Provisionner**.



Provisionnement du stockage sélectionné

Pour provisionner le stockage sélectionné :

1. Dans l'onglet **Appliance** , cliquez sur **Tâches** → **Provisionnement**.
   L'écran **Provisionnement** affiche la capacité estimée pour le provisionnement. Cette capacité est utilisée pour créer un nouveau référentiel AppAssure.
2. Pour provisionner uniquement une portion de l'espace disponible, cliquez sur **Provisionner** sous **Action**, en regard de l'espace de stockage à provisionner.
   - Pour créer un nouveau référentiel, sélectionnez **Créer un nouveau référentiel**, puis entrez un nom pour ce référentiel.
     Par défaut, le champ de nom du référentiel contient « Référentiel 1 ». Vous pouvez choisir d'écraser ce nom.

- Pour ajouter de la capacité à un référentiel existant, sélectionnez **Étendre le référentiel existant**, puis sélectionnez l'entrée voulue dans la liste **Référentiels existants**.

  REMARQUE : Pour ajouter de la capacité, il est recommandé d'étendre un référentiel existant au lieu d'en ajouter un. Des référentiels séparés n'utilisent pas la capacité aussi efficacement car la déduplication ne peut pas être effectuée sur plusieurs référentiels distincts.

3. Sous **Réserve de stockage facultative**, sélectionnez **Allouer une partie de l'espace de stockage en cours de provisionnement pour les machines virtuelles en mode de secours ou à d'autres fins**, puis spécifiez le pourcentage de stockage à allouer à ces VM.
4. Cliquez sur **Provisionner**.

   Le provisionnement de disque démarre et l'état de la création du référentiel AppAssure s'affiche dans la zone **État** de l'écran **Tâches**. L'**État** affiche **Provisionné**.
5. Pour afficher les détails une fois que le provsionnement de disque est terminé, cliquez sur **>** en regard du voyant d'état.

   La page **Tâches** se développe, et affiche les détails de l'état, du référentiel et des disques virtuels (s'ils ont été alloués).

Suppression de l'allocation d'espace pour un disque virtuel

Avant d'entamer cette procédure, déterminez les disques virtuels que vous pouvez supprimer. Dans Core Console, sélectionnez l'onglet **Appliance**, cliquez sur **Tâches**, puis développez le référentiel contenant les disques virtuels pour afficher les détails de ces disques.
Pour supprimer l'allocation d'espace d'un disque virtuel :

1. Dans l'application OpenManage Server Administrator, développez l'entrée **Stockage**.
2. Développez le contrôleur qui héberge le disque virtuel, puis sélectionnez **Disques virtuels**.
3. Sélectionnez le disque virtuel à supprimer, puis cliquez sur **Supprimer** dans le menu déroulant **Tâches**.
4. Après confirmation de la suppression, l'espace apparaît dans Core Console (onglet **Appliance**, écran **Tâches**) comme étant disponible pour provisionnement.

Résolution des tâches ayant échoué

AppAssure fait un rapport des tâches de vérification, de provisionnement et de restauration qui échouent, en créant un événement dans la page Accueil de Core Console, ainsi que dans l'onglet **Appliance** (écran **Tâches**).

Pour comprendre comment résoudre une tâche ayant échoué, sélectionnez l'onglet **Appliance**, puis cliquez sur **Tâches**. Développez la tâche en échec en cliquant sur **>** en regard de l'option **État**, puis passez en revue le message d'erreur et l'action recommandée.

Mise à niveau de votre appliance

Pour mettre à niveau votre appliance, procédez comme suit :

1. Téléchargez le **Recovery and Update Utility** (RUU, Utilitaire de restauration et de mise à jour) depuis le site **dell.com/support** sur l'applianceDL4300 Backup to Disk.
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, ASP .NET MVC3, du fournisseur LSI, des applications DL, et des logiciels OpenManage Server Administrator et AppAssure Core sont installés dans le cadre du Recovery and Update Utility. Outre ces options, l'utilitaire Recovery and Update Utility met également à jour le contenu RASR.

   REMARQUE : Dans le cadre du processus de mise à niveau du logiciel AppAssure Core, RUU (Recovery and Upgrade Utility, Utilitaire de restauration et de mise à niveau) vous avertit de la version d'AppAssure actuellement installée et vous demande de confirmer que vous voulez mettre le logiciel Core à niveau vers la version incluse dans l'utilitaire. Les rétrogradations du logiciel AppAssure Core ne sont pas prises en charge.
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. Téléchargez **Recovery and Update Utility** (RUU, Utilitaire de restauration et de mise à jour) depuis le site **dell.com/support** sur l'appliance.
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, ASP .NET MVC3, le fournisseur LSI, les applications DL, et les logiciels OpenManage Server Administrator et AppAssure Core sont installés 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 AppAssure 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 AppAssure Core.

   REMARQUE : Les rétrogradations du logiciel AppAssure 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 Configuration de l'appliance AppAssure est lancé si le système doit être configuré de nouveau après la réparation, sinon la console sera lancée.

4

Protection des stations de travail et des serveurs

À propos de la protection des stations de travail et des serveurs

Pour protéger les données, ajoutez les postes de travail et les serveurs à protéger dans Core Console ; par exemple, le serveur Exchange, SQL Server ou le serveur Linux.

REMARQUE : Dans ce chapitre, en général, le terme *machine* désigne également le logiciel d'agent AppAssure installé sur cette machine.

Dans la Core Console, vous pouvez identifier la machine où un AppAssure Agent est installé et spécifier les volumes à protéger, définir des planifications de protection, ajouter des mesures de sécurité supplémentaires, telles que le cryptage, etc. Pour plus d'informations sur l'accès à la Core Console pour protéger les stations de travail et serveurs, voir Protection d'une machine.

Configuration des paramètres de la machine

Une fois que vous avez ajouté une protection pour les machines dans AppAssure, vous pouvez modifier les paramètres de configuration de base des machines (nom, nom d'hôte, etc.), les paramètres de protection (en changeant la planification de protection des volumes de l'ordinateur, en ajoutant/supprimant des volumes ou en suspendant la protection), etc.

Affichage et modification des paramètres de configuration

Pour afficher et modifier les paramètres de configuration :

1. Après avoir ajouté une machine protégée, effectuez l'une des actions suivantes :
   - Dans Core Console, cliquez sur l'onglet **Machines**, puis cliquez sur le lien hypertexte de la machine à modifier.
   - Dans le panneau **Navigation**, sélectionnez la machine à modifier.
2. Cliquez sur l'onglet **Configuration**.

   La page **Paramètres** s'affiche.
3. Cliquez sur **Modifier** pour modifier les paramètres de la machine, tel que décrit dans le tableau suivant.

Zone de texte	Description
Nom d'affichage	Entrez un nom d'affichage pour la machine.

Zone de texte	Description
	Nom de cette machine à afficher dans Core Console. 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.
Nom d'hôte	Entrez un nom d'hôte pour la machine.
Port	Entrez un numéro de port pour la machine. Le core utilise ce port pour communiquer avec cette machine.
Référentiel	Sélectionnez le référentiel des points de restauration. Affiche sur le référentiel sur le core dans lequel les données de la machine doivent être stockées. REMARQUE : Ce paramétrage peut uniquement être modifié s'il n'existe pas de points de restauration ou si le référentiel précédent est manquant.
Clé de cryptage	Modifiez la clé de chiffrement si nécessaire. Spécifie si le chiffrement doit être appliqué aux données pour chaque volume de cette machine qui sera stocké dans le référentiel.

Affichage des informations système d'un ordinateur

La Core Console affiche toutes les machines protégées, en incluant une liste de toutes les machines et de leur état.

Pour afficher les informations système d'une machine :

1. Dans la Core Console, sous **Ordinateurs protégés**, sélectionnez l'ordinateur pour lequel vous souhaitez afficher des informations détaillées sur le système.
2. Cliquez sur l'onglet **Outils** de cet ordinateur.

   Les informations concernant la machine s'affichent dans la page **Informations système**. Les détails affichés sont les suivants :

   - Nom d'hôte
   - Version du SE
   - Architecture du SE
   - Mémoire (Physique)
   - Nom d'affichage
   - Nom de domaine complet
   - Type de machine virtuelle (le cas échéant)

   Les informations détaillées sur les volumes de cette machine comprennent :

   - Nom
   - ID de périphérique
   - Système de fichiers
   - Capacité (y compris brute, formatée et utilisée)
   - Processeurs
   - Type de processeurs
   - Cartes réseau

- Les adresses IP associées à cette machine

Configuration des groupes de notification pour les événements système

Dans AppAssure, vous pouvez configurer la façon dont le programme signale les événements système de votre machine, en créant des groupes de notification, qui peuvent inclure des alertes système, des erreurs, etc.

Pour configurer des groupes de notification pour les événements système :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à modifier.
   - Dans le panneau de navigation, sélectionnez la machine à modifier.

   L'onglet **Récapitulatif** s'affiche.
3. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Événements**.
   La page **Groupes de notification** s'affiche.
4. Cliquez sur **Utiliser les paramètres d'alertes personnalisés**, puis cliquez sur **Appliquer**.
   L'écran **Personnaliser des groupes de notification** s'affiche.
5. Cliquez sur **Ajouter un groupe** pour ajouter de nouveaux groupes de notifications pour l'envoi d'une liste d'événements système.
   La boîte de dialogue **Ajouter un groupe de notification** s'ouvre.

   REMARQUE : Pour utiliser les paramètres d'alerte par défaut, sélectionnez l'option **Utiliser les paramètres d'alerte du core**.
6. Ajoutez les options de notification tel que décrit dans le tableau suivant.

Zone de texte	Description
Nom	Entrez un nom pour le groupe de notification.
Description	Entrez une description du groupe de notification.
Activez les événements	Sélectionnez les événements à partager avec ce groupe de notification. Vous pouvez sélectionner **Tous** ou sélectionner un sous-ensemble d'événements à inclure : • **BootCd (CD d'amorçage)** • **LocalMount (Montage local)** • **Métadonnées** • **Clusters** • **Notification** • **PowerShellScripting (Scripts PowerShell)** • **PushInstall (InstallerPousser)** • **Capacité d'attachement** • **Tâches** • **Licences** • **LogTruncation (Troncature de journal)** • **Archivage** • **CoreService (Service de core)**

Zone de texte	Description
	• **Exportation** • **Protection** • **Réplication** • **Restauration** • **Rollup (Cumul)** Vous pouvez choisir d'effectuer une sélection par type : • **Informatif** • **Avertissement** • **Erreur** REMARQUE : Lorsque vous choisissez de sélectionner par type, par défaut, les événements appropriés sont automatiquement activés. Par exemple, si vous choisissez Avertissement, les événements de Capacité d'attachement, Tâches, Licences, Archive, CoreService, Exportation, Protection, Réplication et Restauration sont activés.
Options de notification	Sélectionnez la méthode de traitement des notifications. Vous pouvez choisir parmi les options suivantes : • **Notifier par e-mail** : spécifiez les adresses e-mail auxquelles envoyer les événements, dans les zones de texte À, Cc et Cci. REMARQUE : Pour recevoir un courrier, le SMTP doit avoir été configuré au préalable. • **Notifier via le journal d'événements Windows** : le journal d'événements Windows contrôle la notification. • **Notifier par syslogd** : spécifiez à quels nom d'hôte et port envoyer les événements. – **Hôte** : entrez le nom d'hôte du serveur. – **Port** : entrez le numéro de port qui permet de communiquer avec le serveur.

7. Cliquez sur **OK** pour enregistrer vos modifications.
8. Pour modifier un groupe de notification existant, cliquez sur **Modifier** en regard du groupe de notification à modifier.

   La boîte de dialogue **Modifier le groupe de notification** s'affiche et vous pouvez modifier les paramètres.

Modification des Groupes de notification pour les événements système

Pour modifier des groupes de notification pour les événements système :

1. Accédez à Core Console, puis sélectionnez l'onglet **Machines**.
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à modifier.
   - Ou bien, dans le panneau de navigation, sélectionnez la machine à retirer.

   L'onglet **Récapitulatif** s'affiche.

3. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Événements**.
4. Cliquez sur **Utiliser les paramètres d'alertes personnalisés**, puis cliquez sur **Appliquer**.
   L'écran **Personnaliser des groupes de notification** s'affiche.
5. Cliquez sur l'icône **Modifier** dans la colonne **Action**.
   La boîte de dialogue **Modifier le groupe de notifications** s'ouvre.
6. Modifiez les options de restauration telles que décrites dans le tableau suivant.

Zone de texte	Description
Nom	Entrez un nom pour le groupe de notification. REMARQUE : Vous ne pouvez pas modifier le nom du groupe de notification.
Description	Entrez une description du groupe de notification.
Activez les événements	Sélectionnez les événements à partager avec le groupe de notification. Vous pouvez sélectionner **Tous** ou sélectionner un sous-ensemble d'événement à inclure : • **BootCd (CD d'amorçage)** • **LocalMount (Montage local)** • **Métadonnées** • **Clusters** • **Notification** • **PowerShellScripting (Scripts PowerShell)** • **PushInstall (InstallerPousser)** • **Capacité d'attachement** • **Tâches** • **Licences** • **LogTruncation (Troncature de journal)** • **Archivage** • **CoreService (Service de core)** • **Exportation** • **Protection** • **Réplication** • **Restauration** • **Rollup (Cumul)** Vous pouvez choisir d'effectuer une sélection par type : • **Informatif** • **Avertissement** • **Erreur**

Zone de texte	Description
	REMARQUE : Lorsque vous choisissez de sélectionner par type, par défaut, les événements appropriés sont automatiquement activés. Par exemple, si vous choisissez Avertissement, les événements de Capacité d'attachement, Tâches, Licences, Archive, CoreService, Exportation, Protection, Réplication et Restauration sont activés.
Options de notification	Sélectionnez la méthode de traitement des notifications. Vous pouvez choisir parmi les options suivantes : • **Notifier par courrier électronique** : spécifiez à quelles adresses électroniques envoyer les événements dans les zones de texte À, Cc et, éventuellement, Cci. REMARQUE : Pour recevoir un courrier, le SMTP doit avoir été configuré au préalable. • **Notifier via le journal d'événements Windows** : le journal d'événements Windows contrôle la notification. • **Notifier par syslogd** : spécifiez à quel nom d'hôte et quel port envoyer les événements. – **Hôte** : entrez le nom d'hôte du serveur. – **Port** : entrez le numéro de port qui permet de communiquer avec le serveur.

7. Cliquez sur **OK**.

Personnalisation des paramètres de stratégie de rétention

La stratégie de rétention d'une machine spécifie la durée pendant laquelle les points de restauration d'une machine d'agent sont stockés dans le référentiel. Les stratégies de rétention servent à conserver plus longtemps les instantanés de sauvegarde et elles facilitent leur gestion. Un processus de cumul (rollup) applique la stratégie de rétention, et gère l'âge et la suppression des anciennes sauvegardes. Cette tâche est également une étape de la procédure dans Processus de modification des paramètres du nœud de cluster.

Pour personnaliser les paramètres de stratégie de rétention :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à modifier.
   - Dans le panneau de navigation, sélectionnez la machine à modifier.

   L'onglet **Récapitulatif** s'affiche.
3. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Stratégie de rétention**.

   REMARQUE : Pour utiliser la stratégie de rétention par défaut configurée pour le core, veillez à sélectionner l'option Utiliser la stratégie de rétention par défaut du core.

   L'écran **Stratégie de rétention** s'affiche.
4. Pour définir les stratégies personnalisées, cliquez sur **Utiliser une stratégie de rétention personnalisée**.

   L'écran **Stratégie de rétention personnalisée** s'affiche.
5. Sélectionnez **Activer le cumul (rollup)** et spécifiez les périodes de conservation des données de sauvegarde selon vos besoins. Les options de stratégie de rétention sont décrites ci-dessous :

Zone de texte	Description
Conserver tous les points de restauration pendant n [période de rétention]	Indique la période de rétention des points de restauration. Entrez un nombre représentant la période de rétention, puis sélectionnez une durée. La valeur par défaut est **3**. Choisissez parmi les options suivantes : • **Jours** • **Semaines** • **Mois** • **Années**
...puis gardez un point de restauration par heure pour n [période de rétention]	Fournit un niveau de rétention plus précis. Sert de bloc de construction, avec le paramétrage principal, pour affiner la définition de la durée de conservation des points de restauration. Entrez un nombre représentant la période de rétention, puis sélectionnez une durée. La valeur par défaut est 2. Choisissez parmi les options suivantes : • **Jours** • **Semaines** • **Mois** • **Années**
...puis gardez un point de restauration par jour pour n [période de rétention]	Fournit un niveau de rétention plus précis. Sert de bloc de construction pour affiner la définition de la durée de conservation des points de restauration. Entrez un nombre représentant la période de rétention, puis sélectionnez une durée. La valeur par défaut est 4. Choisissez parmi les options suivantes : • **Jours** • **Semaines** • **Mois** • **Années**
...puis gardez un point de restauration par semaine pour n [période de rétention]	Fournit un niveau de rétention plus précis. Sert de bloc de construction pour affiner la définition de la durée de conservation des points de restauration. Entrez un nombre représentant la période de rétention, puis sélectionnez une durée. La valeur par défaut est 3. Choisissez parmi les options suivantes : • **Semaines** • **Mois** • **Années**

Zone de texte	Description
...puis gardez un point de restauration par mois pour n [période de rétention]	Fournit un niveau de rétention plus précis. Sert de bloc de construction pour affiner la définition de la durée de conservation des points de restauration. Entrez un nombre représentant la période de rétention, puis sélectionnez une durée. La valeur par défaut est 2. Choisissez parmi les options suivantes : • **Mois** • **Années**
...puis gardez un point de restauration par an pour n [période de rétention]	Entrez un nombre représentant la période de rétention, puis sélectionnez une durée.

Le champ Point de restauration le plus récent indique le dernier point de restauration créé. Les paramètres de stratégie de rétention déterminent le point de restauration le plus ancien.

L'exemple suivant montre comment la période de rétention est calculée.

Conserver tous les points de restauration pendant 3 jours.

...puis conserver un point de restauration par heure pendant 3 jours

...et puis conserver un point de restauration par jour pendant 4 jours

...et puis conserver un point de restauration par semaine pendant 3 semaines

...et puis conserver un point de restauration par mois pendant 2 mois

...et puis conserver un point de restauration par mois pendant 1 an

Le Point de restauration le plus récent est défini sur le jour, le mois et l'année actuels.

Dans cet exemple, le point de restauration le plus ancien peut dater d'un an, 4 mois et 6 jours.

6. Cliquez sur **Appliquer** pour enregistrer vos modifications.
7. Pour effectuer le cumul (rollup) sur la base de la stratégie de rétention actuelle de la machine, sélectionnez **Forcer le cumul (rollup)** ; vous pouvez aussi laisser le programme appliquer la stratégie de rétention définie lors du cumul nocturne.

Affichage d'informations de licence

Vous pouvez afficher les informations de statut de licence actuelles du logiciel AppAssure Agent installé sur une machine.

Pour afficher les informations de licence

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à afficher.
   - Dans le panneau de navigation, sélectionnez la machine à afficher.

3. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Licences**.

   L'écran **État** affiche les détails de licences produit.

Modification des horaires de protection

Dans AppAssure vous pouvez modifier les horaires de protection des volumes spécifiques d'un ordinateur.

Pour modifier des horaires de protection :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à modifier.
   - Dans le panneau de navigation, sélectionnez la machine à modifier.
3. Effectuez l'une des opérations suivantes :
   - Dans le tableau **Volumes** de l'onglet **Récapitulatif** de la machine, cliquez sur le lien hypertexte correspondant à la planification de protection du volume à personnaliser.
   - Cliquez sur l'onglet **Configuration**, puis cliquez sur **Paramètres de protection**. Dans la liste de volumes, cliquez sur l'icône **Modifier** à côté du volume que vous souhaitez personnaliser.

   La boîte de dialogue **Planification de protection** s'affiche.
4. Dans la boîte de dialogue **Horaire de protection**, modifiez les options d'horaire suivantes au besoin pour protéger vos données. Le tableau suivant décrit les options.

Option	Description
Fréquence	**Jour de la semaine** : pour protéger les données à un intervalle de temps donné (par exemple, toutes les 15 minutes), sélectionnez l'**Intervalle**, puis : • Pour personnaliser l'horaire de protection des données pendant les heures de forte utilisation, indiquez une **heure de début**, une **heure de fin** et un **intervalle** depuis les menus déroulants. • Pour protéger les données pendant les heures de faible utilisation, cochez la case **Intervalle de protection pendant les heures de faible utilisation**, puis sélectionnez un intervalle de protection depuis le menu déroulant. **Week-ends** : pour protéger les données pendant le weekend, cochez la case **Intervalle de protection pendant le weekend**, puis sélectionnez un intervalle dans le menu déroulant. REMARQUE : Si les bases de données et journaux SQL ou Exchange se trouvent sur des volumes différents, ceux-ci doivent appartenir au même groupe de protection.
Tous les jours	Pour protéger les données quotidiennement, sélectionnez l'option **Quotidiennement**, puis, dans le menu déroulant **Heure de protection**, sélectionnez l'heure à laquelle la protection des données doit commencer.
Aucune protection	Pour ne plus protéger ce volume, sélectionnez l'option **Aucune protection**.

   Si vous souhaitez appliquer ces paramètres personnalisés à tous les volumes de cette machine, cochez la case **Appliquer à tous les volumes**.
5. Lorsque vous avez effectué toutes les modifications nécessaires, cliquez sur **OK.**

Modification des paramètres de transfert

Vous pouvez modifier les paramètres pour gérer les processus de transfert de données d'une machine protégée. Les paramètres de transfert décrits dans cette section sont des paramètres d'agent. Pour définir le transfert au niveau du core, voir Modification des paramètres de file d'attente de transfert.

PRÉCAUTION : La modification des paramètres de transfert peut avoir un effet dramatique sur votre environnement. Avant de modifier la valeur des paramètres de transfert, consultez le manuel « Transfer Performance Tuning Guide » (Guide de réglage des performances de transfert) dans la base de connaissances https://support.software.dell.com/appassure/kb.

Il existe trois types de transferts :

Instantanés	Le transfert qui sauvegarde les données de votre machine protégée.
Exportation VM	Un type de transfert qui crée une machine virtuelle avec toutes les informations de sauvegarde et les paramètres comme spécifié par la planification définie pour la protection de la machine.
Restauration	Un processus permettant de restaurer les informations de sauvegarde sur une machine protégée.

Le transfert de données implique la transmission d'un volume de données sur un réseau, depuis les machines Agent vers le Core. En cas de réplication, le transfert se produit également du core d'origine ou core source vers le core cible.

Vous pouvez optimiser le transfert de données pour votre système, à l'aide de certaines options de performances. Ces paramètres contrôlent l'utilisation de la bande passante de données lors du processus de sauvegarde des machines d'agent, l'exécution de l'exportation des VM ou l'exécution d'un cumul (rollback). Voici certains des facteurs qui influent sur les performances de transfert des 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 du référentiel
- Quantité de mémoire disponible pour la mise en tampon des données

Vous pouvez ajuster les options de performances pour qu'elles répondent aux mieux aux besoins de votre entreprise, et les ajuster en fonction de votre environnement.

Pour modifier les paramètres de transfert :

1. Dans la console Core, effectuez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Machines**, puis sur le lien hypertexte de la machine à modifier.
   - Dans le panneau de navigation, sélectionnez la machine à modifier.
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à modifier.
   - Dans le panneau de navigation, sélectionnez la machine à modifier.
3. Cliquez sur l'onglet **Configuration**, puis sur **Paramètres de transfert**.
   Les paramètres de transfert actuels s'affichent.

4. Dans la page **Paramètres de transfert**, cliquez sur **Modifier**.
   La boîte de dialogue **Paramètres de transfert** s'affiche.
5. Entrez les options **Paramètres de transfert** de la machine tel que décrit dans le tableau suivant.

Zone de texte	Description
Priorité	Définit la priorité de transfert entre les machines protégées. Vous pouvez attribuer à chaque machine une priorité par rapport aux autres machines protégées. Sélectionnez un numéro de 1 à 10, 1 représentant la priorité la plus élevée. Le paramètre par défaut est 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 liaisons TCP envoyées au core pour traitement en parallèle par l'agent. **REMARQUE :** Dell vous recommande de définir cette valeur sur 8. Si vous constatez une perte de paquets, augmentez cette valeur.
Nombre maximal d'écritures simultanées	Définit le nombre maximal d'actions d'écriture sur disque simultanées pour chaque connexion d'agent. **REMARQUE :** Dell vous recommande d'utiliser ici la même valeur que pour Nombre maximal de flux simultanés. En cas de perte de paquets, choisissez une valeur légèrement plus faible. Par exemple, si Nombre maximal de flux simultanés est défini sur 8, définissez cette option sur 7.
Nombre maximal de tentatives	Définit le nombre maximal de tentatives pour chaque machine protégée, en cas d'échec de certaines opérations.
Taille maximale de segment	Spécifie la quantité maximale de données, en octets, qu'une machine peut recevoir sur un seul segment TCP. La valeur par défaut est 4194304. **PRÉCAUTION : Ne modifiez pas cette option, conservez la valeur par défaut.**
Profondeur maximale de file d'attente de transfert	Spécifie le nombre de commandes simultanées que vous pouvez envoyer. Vous pouvez définir cette option sur une valeur plus élevée si votre système effectue un grand nombre d'opérations d'entrée/sortie simultanées.
Lectures en attente par flux	Spécifie le nombre d'opérations de lecture en file d'attente qui sont stockées dans le back-end. Ce paramètre permet de contrôler la mise en file d'attente des agents. **REMARQUE :** Dell vous recommande de définir cette valeur sur 24.
Programmes d'écriture exclus	Sélectionnez un service d'écriture si vous souhaitez l'exclure. Comme les processus d'écriture affichés dans la liste sont propres à la machine que vous configurez, vous ne verrez pas tous les services d'écriture de la liste. Ceux qui s'affichent peuvent être les suivants : • Rédacteur ASR • Rédacteur BITS

Zone de texte	Description
	• Rédacteur COM+ REGDB • Rédacteur de compteurs de performance • Rédacteur de registre • Rédacteur d'optimisation de copie en double • SQLServerWriter • Rédacteur système • Rédacteur de planificateur de tâche • Rédacteur de magasin de métadonnées VSS • Rédacteur WMI
Transfer Data Server Port (Port de serveur de transfert de données)	Définit le port utilisé pour les transferts. La valeur par défaut est 8009.
Délai d'attente de transfert	Spécifie (en minutes et secondes) la durée pendant laquelle un paquet est autorisé à rester statique sans transfert.
Délai d'attente d'instantané	Spécifie (en minutes et secondes) la durée maximale pendant laquelle le programme attend avant de capturer un instantané.
Expiration du délai d'attente de lecture réseau	Spécifie (en minutes et secondes) la durée maximale d'attente d'établissement d'une connexion de lecture. Si la lecture réseau n'est pas réalisée dans ce délai, l'opération est répétée.
Expiration du délai d'attente d'écriture réseau	Indique en secondes le temps d'attente maximal d'une connexion d'écriture. Si l'écriture réseau n'est pas réalisée dans ce délai, l'opération est répétée.

6. Cliquez sur **OK**.

Redémarrage d'un service

Pour redémarrer un service :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte correspondant à la machine à redémarrer.
   - Dans le panneau **Navigation**, sélectionnez la machine à redémarrer.
3. Sélectionnez l'onglet **Outils**, puis cliquez sur **Diagnostics**.
4. Sélectionnez l'option **Redémarrer le service**, puis cliquez sur le bouton **Redémarrer le service**.

Affichage des journaux de machine

Si vous rencontrez des erreurs ou problèmes de machine, consulter les journaux pour effectuer le dépannage.

Pour afficher les journaux de machine

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte correspondant à la machine qui contient les journaux à afficher.
   - Dans le panneau **Navigation**, sélectionnez la machine qui contient les journaux à afficher.
3. Sélectionnez l'onglet **Outils**, puis cliquez sur **Diagnostics**.
4. Cliquez sur le lien **Afficher le journal**.

Protection d'une machine

Cette rubrique explique comment démarrer la protection des données sur la machine spécifiée.

REMARQUE : Vous devez avoir installé le logiciel de l'agent sur la machine pour pouvoir la protéger. Vous pouvez choisir d'installer l'agent avant cette procédure ou vous pouvez déployer le logiciel vers l'agent lorsque vous définissez la protection dans la boîte de dialogue **Connexion**. Pour connaître les étapes spécifiques d'installation du logiciel agent pendant le processus de protection d'une machine, voir Déploiement du logiciel agent lors de la protection d'un agent.

Lorsque vous ajoutez une protection, vous devez spécifier le nom ou l'adresse IP de la machine à protéger, préciser les volumes de cette machine à protéger et définir la planification de protection de chaque volume.

Pour protéger plusieurs machines simultanément, voir Protection de plusieurs machines.

Pour protéger un ordinateur

1. Si vous ne l'avez pas fait après l'installation du logiciel de l'agent, redémarrez la machine sur laquelle vous avez installé le logiciel de l'agent.
2. Dans la console Core de la machine de core, effectuez l'une des opérations suivantes :
   - Dans l'onglet **Accueil**, sous **Machines protégées**, cliquez sur **Protéger une machine**.
   - Sélectionnez l'onglet **Machines**, puis ouvrez le menu déroulant **Actions** et cliquez sur **Protéger une machine**.

   La boîte de dialogue **Connexion** apparaît.
3. Dans la boîte de dialogue **Connecter**, entrez les informations de l'ordinateur sur lequel vous souhaitez vous connecter comme décrit dans le tableau suivant.

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
Port	Numéro de port sur lequel Core communique avec l'agent sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à cet ordinateur ; par exemple, administrateur.
Mot de passe	Le mot de passe utilisé pour vous connecter à cet ordinateur

4. Cliquez sur **Connecter** pour établir une connexion à cette machine.

REMARQUE : Si le logiciel de l'agent n'est pas encore installé sur la machine choisie, suivez la procédure décrite dans la rubrique Déploiement du logiciel de l'agent lors de la protection d'un agent. Redémarrez la machine d'agent après avoir déployé le logiciel d'agent, puis passez à l'étape suivante.

5. Dans la boîte de dialogue **Protéger**, modifiez les paramètres suivants vos besoins, comme décrit dans le tableau suivant.

Champ	Description
Nom d'affichage	La valeur Nom d'hôte ou Adresse IP indiquée dans la boîte de dialogue **Connexion** s'affiche dans ce champ. (Facultatif) Entrez un nouveau nom pour la machine, qui sera affiché dans la console Core. REMARQUE : Vous pouvez également modifier le nom d'affichage ultérieurement, en accédant à l'onglet **Configuration** d'une machine existante.
Référentiel	Sélectionnez le référentiel sur le Core dans lequel les données de cet ordinateur doivent être stockées.
Clé de chiffrement	Indiquez si le chiffrement doit être appliqué aux données pour chaque volume de cette machine qui seront stockées dans le référentiel. REMARQUE : Les paramètres de cryptage d'un référentiel sont définis sur l'onglet **Configuration** de Core Console.
Suspendre initialement la protection	Une fois que vous avez ajouté une machine à la liste de protection, AppAssure commence automatiquement à prendre un instantané de base des données. Vous pouvez cocher cette case pour suspendre initialement la protection. Vous devrez ensuite forcer manuellement la prise d'un instantané lorsque vous serez prêt à commencer à protéger vos données. Pour plus d'informations sur le forçage manuel d'un instantané, voir Forcer un instantané .
Groupes de volumes	Sous Groupes de volumes, vous pouvez spécifier les volumes à protéger et établir une planification de protection. Pour définir une planification par défaut de protection qui se déclenche toutes les 60 minutes pour tous les volumes de la machine, cliquez sur **Appliquer la valeur par défaut**. Vous pouvez également sélectionner le volume de votre choix sur la machine et définir des paramètres de protection spécifiques pour ce volume. Les paramètres initiaux appliquent la planification de protection par défaut, qui se déclenche toutes les 60 minutes. Pour modifier la planification pour un volume donné, cliquez sur **Modifier** pour ce volume. Vous pouvez alors définir plus précisément l'intervalle entre deux instantanés (y compris définir une planification différente pour les weekends) ou indiquer l'heure à laquelle prendre un instantané quotidiennement.

Champ	Description
	Pour plus d'informations sur la modification de la planification de protection du volume sélectionné, reportez-vous à la section Création d'horaires personnalisés pour les volumes.

6. Cliquez sur **Protéger**.
   Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (instantané de toutes les données des volumes protégés) son transfert démarre immédiatement vers le référentiel sur le Core, sauf si vous avez demandé la suspension initiale de la protection.

   PRÉCAUTION : Si vous avez protégé une machine Linux, vous ne devez pas démonter manuellement un volume protégé. Si vous devez démonter le volume, veillez à exécuter la commande suivante avant le démontage : bsctl -d [path_to_volume]. Dans cette commande, [chemin_du_volume] ne désigne pas le point de montage du volume mais plutôt le descripteur de fichier de ce volume ; il doit être dans un format semblable à cet exemple : /dev/sda1.

Déploiement du logiciel de l'agent lors de la protection d'un agent

Vous pouvez télécharger et déployer des agents au cours du processus d'ajout d'un agent à protéger.

REMARQUE : Cette procédure n'est pas requise si vous avez déjà installé le logiciel de l'agent sur un ordinateur que vous souhaitez protéger.

Pour déployer des agents au cours du processus d'ajout d'un agent à protéger :

1. Dans la boîte de dialogue **Protéger un ordinateur** → **Connecter**, après avoir entré les paramètres de connexion appropriés, cliquez sur **Connecter**.
   La boîte de dialogue **Déployer l'agent** s'affiche.
2. Cliquez sur **Oui** pour déployer à distance le logiciel d'agent sur l'ordinateur.
   La boîte de dialogue **Déployer l'agent** s'affiche.
3. Entrez les paramètres de connexion et de protection de la façon suivante :
   - **Nom d'hôte** : indique le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
   - **Port** : indique le numéro du port sur lequel le Core communique avec l'agent sur l'ordinateur. La valeur par défaut est 8006.
   - **Nom d'utilisateur** : indique le nom d'utilisateur utilisé pour établir la connexion à cet ordinateur, par exemple, administrateur.
   - **Mot de passe** : indique le mot de passe utilisé pour se connecter à cet ordinateur.
   - **Nom d'affichage** : indique le nom de l'ordinateur qui s'affiche dans Core Console. Ce nom peut être identique au nom d'hôte.
   - **Protéger l'ordinateur après l'installation** : si vous sélectionnez cette option, l'AppAssure peut prendre un instantané de base des données dès que vous ajoutez l'ordinateur aux éléments à protéger. Cette option est sélectionnée par défaut. Si vous la désélectionnez, vous devez forcer manuellement la prise d'un instantané lorsque vous êtes prêt à démarrer la protection des données. Pour en savoir plus sur le forçage manuel d'un instantané, voir « Forçage d'un instantané » dans le *Guide d'utilisation de l'appliance Dell DL4300*.
   - **Référentiel** : sélectionnez le référentiel dans lequel stocker les données de cet agent.

REMARQUE : Vous pouvez stocker les données de plusieurs agents dans un même référentiel.

- **Clé de cryptage** : indique si le cryptage doit être appliqué aux données de chaque volume de cet ordinateur à stocker dans le référentiel.

REMARQUE : Vous définissez les paramètres de cryptage d'un référentiel dans l'onglet **Configuration** de la console Core.

4. Cliquez sur **Déployer**.

   La boîte de dialogue **Déployer un agent** se ferme. Il peut y avoir un délai avant l'affichage de l'agent sélectionné dans la liste d'ordinateurs protégés.

Création d'horaires personnalisés pour les volumes

Pour créer des horaires personnalisés pour les volumes :

1. Dans la boîte de dialogue **Protéger une machine** (voir la section pour plus d'informations sur l'accès à cette boîte de dialogue),voir Protéger une machine sous Groupes de volumes, sélectionnez le volume à protéger, puis cliquez sur **Modifier**.

   La boîte de dialogue **Planification de protection** s'affiche.

2. Dans la boîte de dialogue **Planification de protection**, sélectionnez l'une des options de planification suivantes pour protéger vos données, comme suit :

Zone de texte	Description
Fréquence	Choisissez parmi les options suivantes : • **Jour de la semaine** : pour protéger les données à intervalle donné, sélectionnez **Intervalle**, puis : – Pour personnaliser l'horaire de protection des données pendant les heures de forte utilisation, indiquez une **heure de début**, une **heure de fin** et un **intervalle** depuis les menus déroulants. – Pour protéger les données pendant les heures de faible utilisation, cochez la case **Intervalle de protection pendant les heures de faible utilisation**, puis sélectionnez un intervalle de protection depuis le menu déroulant **Heure**. • **Week-ends** : pour protéger les données pendant le week-end également, cochez la case **Intervalle de protection pendant le week-end**, puis sélectionnez un **intervalle** depuis le menu déroulant.
Tous les jours	Pour protéger les données quotidiennement, sélectionnez l'option **Protection quotidienne**, puis, dans le menu déroulant **Heure**, sélectionnez l'heure à laquelle la protection des données doit commencer.
Aucune protection	Pour ne plus protéger ce volume, sélectionnez l'option **Aucune protection**.

   Si vous souhaitez appliquer ces paramètres personnalisés à tous les volumes de cette machine, cochez la case **Appliquer à tous les volumes**.

3. Lorsque vous avez effectué toutes les modifications nécessaires, cliquez sur **OK.**
4. Répétez les étapes 2 et 3 pour tout volume supplémentaire que vous souhaitez personnaliser.
5. Dans la boîte de dialogue **Protéger la machine**, cliquez sur **Protéger**.

Modification des paramètres d' un serveur Exchange

Pour protéger les données d'un serveur Microsoft Exchange, vous devez configurer des paramètres supplémentaires dans Core Console.

Pour modifier les paramètres d'Exchange Server

1. Une fois que vous avez ajouté la machine Exchange Server à la liste des machines sous protection, sélectionnez-la dans le panneau **Navigation** de Core Console.

   L'onglet **Récapitulatif** correspondant à la machine s'affiche.
2. Dans l'onglet **Résumé**, cliquez sur le lien **Paramètres d'Exchange Server**.

   La boîte de dialogue **Paramètres d'Exchange Server** s'affiche.
3. Dans la boîte de dialogue **Paramètres d'Exchange Server**, vous pouvez sélectionner ou désélectionner les paramètres suivants :
   - Activer la vérification de montabilité automatique
   - Activer la vérification de somme de contrôle nocturne. Vous pouvez continuer à personnaliser ce paramètre en sélectionnant les options suivantes :
     - Tronquer automatiquement les journaux Exchange après une vérification de somme de contrôle réussie
     - Tronquer le journal avant la fin de la vérification des sommes de contrôle
4. Vous pourrez également modifier les références de connexion d'Exchange Server. Pour ce faire, faites défiler jusqu'à la section **Informations d'Exchange Server** puis cliquez sur **Changer les références**.

   La boîte de dialogue **Définir les références d'Exchange** s'affiche.
5. Entrez les nouvelles références, puis cliquez sur **OK**.

Modification des paramètres de SQL Server

Si vous souhaitez protéger les données depuis Microsoft SQL Server, il existe des paramètres supplémentaires que vous devez configurer dans Core Console.

Pour modifier les paramètres SQL Server

1. Une fois que vous avez ajouté la machine SQL Server à la liste des machines sous protection, sélectionnez-la dans le panneau **Navigation** de Core Console.

   L'onglet **Récapitulatif** correspondant à la machine s'affiche.
2. Depuis l'onglet **Résumé**, cliquez sur le lien Paramètres SQL Server.

   La boîte de dialogue **Paramètres SQL Server** s'affiche.
3. Dans la boîte de dialogue **Paramètres SQL Server**, vous pouvez modifier les paramètres suivants au besoin :
   - Activer la vérification de capacité d'attachement nocturne
   - Tronquer le journal après réussite de la vérification de capacité d'attachement (modèle de restauration simple uniquement)
4. Vous pouvez également modifier les références de connexion d'Exchange Server. Pour ce faire, effectuez un défilement jusqu'à la section **Informations SQL Server** puis cliquez sur **Modifier les références**.

   La boîte de dialogue **Définir les références de SQL Server**s'affiche.
5. Entrez les nouvelles références, puis cliquez sur **OK.**

Déploiement d'un agent (installation en mode Pousser)

AppAssure nécessite microsoft.net pour l'installation de l'agent. Microsoft.net doit être installé sur tous les machines client avant l'installation manuelle ou en mode Push de l'agent.
AppAssure permet de déployer AppAssure Agent Installer sur les machines individuelles Windows à protéger. Exécutez les étapes dans la procédure suivante pour pousser le programme d'installation vers un agent. Pour déployer des agents sur plusieurs machines simultanément, reportez-vous à Déploiement sur plusieurs machines.

REMARQUE : Les agents doivent être configurés avec une règle de sécurité permettant l'installation à distante.

Pour déployer un agent

1. Dans la console Core, cliquez sur l'onglet **Ordinateurs/Machines**.
2. Dans le menu déroulant **Actions**, cliquez sur **Déployer l'agent**.
   La boîte de dialogue **Déployer l'agent** s'ouvre.
3. Dans la boîte de dialogue **Déployer l'agent**, saisissez les paramètres de connexion tel que décrit dans le tableau suivant.

Zone de texte	Description
Ordinateur	Entrez le nom d'hôte ou l'adresse IP de la machine que vous souhaitez déployer.
Nom d'utilisateur	Entrez le nom d'utilisateur utilisé pour se connecter à cette machine (par exemple, administrateur).
Mot de passe	Mot de passe utilisé pour se connecter à cette machine.
Redémarrage automatique après installation	Sélectionnez cette option indiquer si le core démarre à la fin du déploiement et de l'installation d'AppAssure Agent Installer.

4. Cliquez sur **Vérifier** pour valider les références que vous avez saisies.
   La boîte de dialogue **Déployer l'agent** affiche un message indiquant que la validation est en cours d'exécution.
5. Cliquez sur **Abandonner** si vous souhaitez annuler le processus de vérification.
   Une fois le processus de vérification terminé, un message s'affiche, signalant que la vérification est finie.
6. Cliquez sur **Déployer**.
   Un message s'affiche, signalant le démarrage du déploiement. Vous pouvez afficher la progression dans l'onglet **Événements**.
7. Cliquez sur **Afficher les détails** pour voir plus d'informations sur l'état du déploiement de l'agent.
8. Cliquez sur **OK**.

Réplication d'un nouvel agent

Lorsque vous ajoutez un AppAssure Agent pour la protection sur un core source, AppAssure offre l'option de répliquer le nouvel agent vers un core cible existant.

Pour répliquer un nouvel agent :

1. Accédez à Core Console, puis sélectionnez l'onglet **Machines**.
2. Dans le menu déroulant **Actions,** cliquez sur **Protéger l'ordinateur**.
3. Dans la boîte de dialogue **Protéger la machine**, entrez les informations comme décrit dans le tableau suivant.

Zone de texte	Description
Hôte	Entrez le nom d'hôte ou l'adresse IP de la machine que vous souhaitez protéger.
Port	Entrez le numéro du port qu'utilise AppAssur Core pour communiquer avec l'agent sur la machine.
Nom d'utilisateur	Entrez le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, administrateur.
Mot de passe	Entrez le mot de passe utilisé pour se connecter à cette machine.

4. Cliquez sur **Connecter** pour établir une connexion à cette machine.
5. Cliquez sur **Afficher les options avancées**, puis modifiez les paramètres suivants au besoin :

Zone de texte	Description
Nom d'affichage	Entrez le nom de la machine à afficher dans Core Console.
Référentiel	Sélectionnez le référentiel dans AppAssure Core dans lequel les données de cette machine sont stockées.
Clé de chiffrement	Indiquez si le chiffrement doit être appliqué aux données de chaque volume de cette machine qui est stocké dans le référentiel. REMARQUE : Les paramètres de cryptage d'un référentiel sont définis sur l'onglet **Configuration** de Core Console.
Core distant	Spécifiez le core cible vers lequel vous souhaitez répliquer l'agent.
Référentiel distant	Le nom du référentiel souhaité sur le core cible dans lequel les données répliquées de cette machine doivent être stockées.
Pause	Cochez cette case si vous souhaitez suspendre la réplication, par exemple, après qu'AppAssure a créé une image de base du nouvel agent.
Planification	Sélectionnez l'une des options suivantes : • Protéger tous les volumes avec la planification par défaut • Protéger des volumes spécifiques avec une planification personnalisée REMARQUE : La planification par défaut est toutes les15 minutes.
Suspendre initialement la protection	Cochez cette case si vous souhaitez suspendre la protection, par exemple, pour permettre à AppAssure de créer l'image de base après les heures de forte utilisation.

6. Cliquez sur **Protéger**.

Gestion des machines

Cette section décrit diverses tâches que vous pouvez effectuer pour gérer des ordinateurs, par exemple, le retrait d'un ordinateur de votre environnement AppAssure, l'établissement de la réplication, le forçage de la troncature de journaux, l'annulation d'opérations, et plus encore.

Retrait d'une machine

1. Accédez à Core Console, puis sélectionnez l'onglet **Machines**.
2. Dans l'onglet **Machines**, effectuez l'une des actions suivantes :
   - Cliquez sur le lien hypertexte de la machine à retirer.
   - Ou bien, dans le panneau de navigation, sélectionnez la machine à retirer.
3. Dans le menu déroulant **Actions**, cliquez sur **Supprimer des machines**, puis sélectionnez l'une des options décrites dans le tableau suivant.

Option	Description
Relation seulement	Retire le core source de la réplication mais conserve les points de restauration répliqués.
Avec les points de restauration	Retire le core source de la réplication et supprime tous les points de restauration reçus depuis cet ordinateur.

Réplication de données d'agent d'une machine

La réplication est la relation entre les cores cible et source sur un même site ou sur deux sites liés avec une connexion lente, agent par agent. Lorsque la réplication est configurée entre deux cores, le core source transmet de manière asynchrone les données d'instantané incrémentiel des agents sélectionnés au core cible ou source. Vous pouvez configurer la réplication sortante vers un fournisseur de services géré qui offre un service de sauvegarde hors site et de récupération après sinistre, ou bien vers un core autogéré. Pour répliquer les données d'agent sur une machine :

1. Dans la console Core, cliquez sur l'onglet **Ordinateurs/Machines**.
2. Sélectionnez la machine que vous souhaitez répliquer.
3. Dans le menu déroulant **Actions**, cliquez sur **Réplication**, puis effectuez l'une des opérations suivantes :
   - Si vous configurez une réplication, cliquez sur **Activer**.
   - Notez que si vous avez déjà établi une réplication existante, vous devez cliquer sur **Copier**.

   La boîte de dialogue **Activer les réplications** s'ouvre.
4. Dans le champ **Hôte**, entrez un nom d'hôte.
5. Sous **Agents**, sélectionnez la machine qui contient l'agent et les données à répliquer.
6. Le cas échéant, cochez la case **Utiliser un lecteur de départ pour le transfert initial**.
7. Cliquez sur **Add** (Ajouter).
8. Pour suspendre ou reprendre la réplication, cliquez sur **Réplication** dans le menu déroulant **Actions**, puis sélectionnez **Suspendre** ou **Reprendre**, selon vos besoins.

Définir la priorité de réplication d'un agent

Pour établir la priorité de réplication d'un agent :

1. Dans Core Console, sélectionnez la machine protégée pour laquelle vous souhaitez définir une priorité de réplication, puis cliquez sur l'onglet **Configuration**.
2. Cliquez sur **Sélectionner les paramètres de transfert**, puis dans le menu déroulant **Priorité**, sélectionnez l'une des options suivantes :
   - **Par défaut**
   - **La plus élevée**
   - **La plus faible**
   - **1**
   - **2**
   - **3**
   - **4**

   REMARQUE : La priorité par défaut est 5. Si la priorité 1 est attribuée à un agent et que la priorité « la plus élevée » est attribuée à un autre agent, ce dernier est répliqué avant l'agent dont la priorité est 1.
3. Cliquez sur **OK**.

Annulation d'opérations d'un ordinateur

Vous pouvez annuler les opérations en cours d'un ordinateur. Vous pouvez spécifier d'annuler seulement l'instantané actual ou d'annuler toutes les opérations en cours, qui comprennent les exportations, les réplications et ainsi de suite.

Pour annuler les opérations d'une machine :

1. Dans la console Core, cliquez sur l'onglet **Ordinateurs/Machines**.
2. Sélectionnez la machine pour laquelle vous souhaitez annuler les opérations.
3. Dans le menu déroulant **Actions**, cliquez sur **Annuler**, puis sélectionnez l'une des options suivantes :

Zone de texte	Description
Toutes les opérations	Annule toutes les opérations actives de cette machine.
Instantané	Annule l'instantané en cours.

Affichage de l'état d'une machine et d'autres détails

Pour afficher l'état de la machine et d'autres détails :

1. Dans le panneau de navigation de Core Console, effectuez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Machines**, puis sur le lien hypertexte de la machine à afficher.
   - Dans le panneau de navigation, cliquez sur la machine à afficher.

L'onglet **Résumé**s'affiche.

Les informations concernant la machine s'affichent dans la page **Récapitulatif**. Les détails affichés sont les suivants :

- Nom de l'hôte
- Dernier instantané pris
- Prochain instantané planifié
- État de cryptage
- Numéro de version
- État de la vérification de montabilité
- État de la vérification de somme de contrôle
- Date de la dernière troncature des journaux

Les informations détaillées concernant les volumes contenus dans cette machine s'affichent également. Il s'agit des détails suivants :

- Taille totale
- Espace utilisé
- Espace libre

Si vous avez installé SQL Server sur la machine, l'écran affiche aussi des détails sur ce serveur, notamment :

- Nom
- Chemin d'installation
- Version
- Numéro de version
- Nom de la base de données
- État en ligne

Si vous avez installé Exchange Server sur la machine, l'écran affiche aussi des détails sur ce serveur et sur les banques de messages, notamment :

- Nom
- Chemin d'installation
- Chemin de données
- Chemin des bases de données Exchange
- Chemin des fichiers journaux
- Préfixe de journal
- Chemin système
- Type de banque de messages

Gestion de plusieurs machines

Cette rubrique décrit les tâches que les administrateurs exécutent pour déployer le logiciel Agent simultanément sur plusieurs machines.

Pour déployer et protéger plusieurs agents, vous devez effectuer les tâches suivantes :

1. Déployer AppAssure sur plusieurs machines.
   Voir Déploiement sur plusieurs machines
2. Suivre l'activité de déploiement par lots.
   Voir Surveillance du déploiement de plusieurs machines

3. Protéger plusieurs ordinateurs.
   Voir Protection de plusieurs machines

   REMARQUE : Cette étape peut être ignorée si vous sélectionnez l'option Protéger l'ordinateur après l'installation au cours du déploiement.
4. Suivre l'activité de protection par lots.
   Voir Surveillance de la protection de plusieurs machines

Déploiement sur plusieurs machines

Vous pouvez simplifier la tâche de déploiement du logiciel AppAssure Agent sur plusieurs machines Windows en utilisant la fonction de déploiement en masse d'AppAssure. Vous pouvez effectuer des déploiement en masse sur :

- des machines sur un hôte virtuel VMware vCenter/ESXi
- des machines sur un domaine Active Directory
- des machines sur n'importe quel autre hôte

La fonction de déploiement en masse détecte automatiquement les machines sur un hôte et vous permet de sélectionner celles vers lesquelles vous souhaitez effectuer un déploiement. Vous pouvez aussi entrer manuellement des informations d'hôte et de machines.

REMARQUE : Les machines que vous déployez doivent avoir accès à Internet pour télécharger et installer les différents éléments, car AppAssure utilise la version Web du programme d'installation de l'agent AppAssure pour déployer les composants d'installation. Si aucun accès à Internet n'est disponible, vous pouvez installer le programme d'installation de l'agent AppAssure en mode Push depuis la machine core. Pour plus d'information sur l'installation en mode Push de l'agent depuis la machine core, voir Pousser l'agent d'installation du programme vers une machine Core. Vous pouvez télécharger les mises à jour du core et de l'agent depuis le portail de licences.

Installation en mode Push (pousser) du programme d'installation de l'agent depuis la machine core

Si les serveurs que vous déployez n'ont pas d'accès Internet, vous pouvez installer en mode Push le fichier d'installation d'agent proprement dit depuis la machine Core. Votre appliance inclut le fichier de programme d'installation de l'agent.

REMARQUE : Téléchargez les mises à niveau du Core et de l'agent depuis le portail de licences.

Pour installer en mode Push le programme d'installation de l'agent depuis la machine Core :

1. Sur la machine Core, copiez le fichier d'installation de l'agent **Agent-X64–5.x.x.xxxxx.exe** dans le répertoire **C:\Program Files\apprecovery\core\installers**.
2. Dans la Core Console, sélectionnez l'onglet **Configuration**, puis cliquez sur **Paramètres**.
3. Dans la section **Paramètres de déploiement**, modifiez le **Nom du programme d'installation de l'agent**.

Déploiement sur des machines d'un domaine Active Directory

Avant de démarrer cette procédure, vous devez vous munir des informations du domaine et des références de connexion du serveur Active Directory.

Pour déployer l'agent sur plusieurs machines dans un domaine Active Directory :

1. Depuis la console Core, cliquez sur l'onglet **Outils**, puis sur **Déployer en masse**.
2. Dans la fenêtre **Déployer l'agent sur les machines**, cliquez sur **Active Directory**.
3. Dans la boîte de dialogue **Connexion à Active Directory**, entrez les informations de domaine et les références de connexion comme l'indique le tableau suivant :

Zone de texte	Description
Domaine	Le nom d'hôte ou l'adresse IP du domaine Active Directory.
Nom d'utilisateur	Nom d'utilisateur qui sert à la connexion à ce domaine, par exemple, administrateur.
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à ce domaine.

4. Cliquez sur **Connexion** .
5. Dans la boîte de dialogue **Ajouter des machines depuis Active Directory**, sélectionnez les machines vers lesquels déployer l'agent AppAssure, puis cliquez sur **Ajouter**.

   Les machines que vous ajoutez s'affichent dans la fenêtre **Déployer l'agent sur les machines**.
6. Pour entrer le mot de passe de la machine, sélectionner un référentiel, ajouter une clé de cryptage ou modifier d'autres paramètres pour la machine, cliquez sur le lien **Modifier** correspondant à cette machine, puis procédez comme suit.
   a. Dans la boîte de dialogue **Modifier les paramètres**, spécifiez les paramètres comme indiqué dans le tableau suivant :

Zone de texte	Description
Nom de l'hôte	Fourni automatiquement depuis l'Étape 3.
Nom d'affichage	Attribué automatiquement en fonction du nom d'hôte entré à l'étape 3.
Port	Numéro du port sur lequel le Core communique avec l'agent sur la machine.
Nom d'utilisateur	Fourni automatiquement depuis l'Étape 3.
Mot de passe	Entrez le mot de passe de la machine.
Redémarrage automatique après installation	Spécifiez si vous souhaitez redémarrer la machine automatiquement après le déploiement. REMARQUE : Cette option est obligatoire si vous souhaitez protéger la machine automatiquement après le déploiement en cochant la case **Protéger la machine après l'installation**.
Protéger la machine après l'installation	Spécifiez si vous souhaitez protéger la machine automatiquement après le déploiement. Ceci vous permet d'ignorer l'étape **Protection de plusieurs machines**.
Référentiel	Utilisez la liste déroulante pour sélectionner le référentiel Core où les données provenant de ces machines doivent être stockées. Le référentiel que vous choisissez est utilisé pour tous les machines protégées. REMARQUE : Cette option est disponible uniquement si vous sélectionnez **Protéger la machine après l'installation**.

Zone de texte	Description
Clé de chiffrement	(Facultatif) Utilisez la liste déroulante pour spécifier si un cryptage doit être appliqué aux données de la machine à stocker dans le référentiel. La clé de cryptage est attribuée à toutes les machines protégées. REMARQUE : Cette option est disponible uniquement si vous sélectionnez **Protéger la machine après l'installation**.

b. Cliquez sur **Enregistrer**.

7. Pour vérifier qu'AppAssure réussit à se connecter à chacun des machines, sélectionnez chaque machine dans la fenêtre **Déployer l'agent sur les machines** et cliquez sur **Vérifier**.
8. La fenêtre **Déployer un agent sur des machines** affiche une icône en regard de chaque machine, indiquant s'il est prêt pour le déploiement, comme suit :

Zone de texte	Description
Icône verte	AppAssure peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure n'est pas en mesure de se connecter à la machine. Ceci provient peut-être du fait que les références de connexion sont incorrectes, que la machine est arrêtée, que le pare-feu bloque le trafic ou d'un autre problème. Pour corriger le problème, cliquez sur **Modifier les paramètres** sur la barre d'outils ou le lien **Modifier** en regard de la machine.

9. Une fois les machines vérifiées avec succès, sélectionnez chacune des machines où vous voulez déployer l'agent AppAssure, puis cliquez sur **Déployer**.
10. Si vous avez choisi l'option **Protéger la machine après l'installation**, les machines redémarrent automatiquement si le déploiement réussit et la protection est activée.

Déploiement sur des machines d'un vCenter VMware Ou Hôte virtuel ESXi

Avant de démarrer cette procédure, vous devez vous munir des informations sur l'emplacement de l'hôte et des références de connexion de l'hôte virtuel ESXi/vCenter VMware.

REMARQUE : Des outils VM doivent être installés sur toutes les machines virtuelles ; sinon, AppAssure ne peut pas détecter le nom d'hôte de la machine virtuelle sur laquelle effectuer le déploiement. Au lieu du nom d'hôte, AppAssure utilise le nom de la machine virtuelle, ce qui peut entraîner des problèmes si le nom d'hôte est différent de celui de la machine virtuelle.

Pour effectuer un déploiement sur des machines virtuelles sur un hôte virtuel ESXi/vCenter :

1. Depuis la console Core, cliquez sur l'onglet **Outils**, puis sur **Déployer en masse**.
2. Dans la fenêtre **Déployer l'agent sur des machines**, cliquez sur **vCenter/ESXi**.
3. Dans la boîte de dialogue **Se connecter au VMware vCenter Server/ESXi**, entrez les informations d'hôte et les références de connexion tel qu'indiqué ci-dessous et cliquez sur **OK**.

Zone de texte	Description
Hôte	Entrez le nom ou l'adresse IP du serveur VMware vCenter ou de l'hôte virtuel ESX(i).
Nom d'utilisateur	Entrez le nom d'utilisateur qui permet de se connecter à l'hôte virtuel ; par exemple, administrateur.

Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à cet hôte virtuel.

4. Dans la boîte de dialogue **Ajouter des machines depuis un serveur VMware vCenter/ESXi**, cochez la case en regard des machines où vous souhaitez déployer l'agent AppAssure, puis cliquez sur **Ajouter**.
5. Dans la fenêtre **Déployer l'agent sur les machines**, vous pouvez afficher les machines que vous avez ajoutées. Pour sélectionner un référentiel, une clé de cryptage ou d'autres paramètres pour une machine, cochez la case correspondant à cette machine, puis cliquez sur **Modifier les paramètres**.

   Pour en savoir plus sur chaque paramètre, reportez-vous à la section Déploiement sur des machines d'un domaine Active Directory.
6. Vérifiez qu'AppAssure peut réussir à se connecter à chacune des machines. Sélectionnez chaque machine dans la fenêtre **Déployer l'agent sur les machines** et cliquez sur **Vérifier**.
7. La fenêtre **Déployer un agent sur des machines** affiche une icône en regard de chaque machine, indiquant s'il est prêt pour le déploiement, comme suit :

Zone de texte	Description
Icône verte	AppAssure peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure n'est pas en mesure de se connecter à la machine. Ceci provient peut-être du fait que les références de connexion sont incorrectes, que la machine est arrêtée, que le pare-feu bloque le trafic ou d'un autre problème. Pour corriger le problème, cliquez sur **Modifier les paramètres** sur la barre d'outils ou le lien **Modifier** en regard de la machine.

8. Une fois les machines vérifiées avec succès, sélectionnez chaque machine et cliquez sur **Déployer**.
9. Si vous avez choisi l'option **Protéger la machine après l'installation**, les machines redémarrent automatiquement si le déploiement réussit et la protection est activée.

Déploiement sur des machines sur n'importe quel autre hôte

Pour effectuer un déploiement sur plusieurs machines sur n'importe quel autre hôte :

1. Depuis la Core Console, cliquez sur l'onglet **Outils**, puis sur **Déployer en masse**.
2. Dans la fenêtre **Déployer un agent sur des machines**, réalisez l'une des actions suivantes :
   - Cliquez sur **Nouveau** pour spécifier plusieurs machines en utilisant la boîte de dialogue **Ajouter une machine** ; ceci vous permet d'entrer un nouvel hôte de machine, des références de connexion, un référentiel, une clé de chiffrement et d'autres informations. Pour en savoir plus sur chaque paramètre, voir Déploiement sur des machines d'un domaine Active Directory .

     Après avoir saisi ces informations, cliquez sur **OK** pour les ajouter à la liste **Déployer un agent sur des machines**, ou cliquez sur **OK et Nouveau** pour ajouter une nouvelle machine.

     REMARQUE : Si vous souhaitez protéger automatiquement la machine après le déploiement, cochez la case **Protéger l'ordinateur après installation**. Si vous cochez la case, le système est redémarré automatiquement avant d'activer la protection.
   - Cliquez sur **Manuellement** pour spécifier plusieurs machines dans une liste ; chaque ligne représente une machine vers laquelle effectuer le déploiement. Dans la boîte de dialogue **Ajouter des machines manuellement**, entrez l'adresse IP ou le nom de la machine, le nom d'utilisateur et le mot de passe séparés par le délimiteur double deux-points, puis le port, comme suit :

     ```
     hostname::username::password::port For example:
     10.255.255.255::administrator::&11@yYz90z::8006 abc-
     host-00-1::administrator::99!zU$o83r::168
     ```
3. Dans la fenêtre **Déployer un agent sur des machines**, vous pouvez afficher les machines que vous avez ajoutées. Si vous souhaitez sélectionner un référentiel, une clé de chiffrement ou d'autres

paramètres d'une machine, cochez la case en regard de la machine et cliquez sur **Modifier les paramètres**.

Pour en savoir plus sur chaque paramètre, reportez-vous à la section Déploiement sur des machines d'un domaine Active Directory.

4. Vérifiez qu'AppAssure peut se connecter à chacune des machines. Sélectionnez chaque machine dans la fenêtre **Déployer l'agent sur les machines** et cliquez sur **Vérifier**.

   La fenêtre **Déployer un agent sur des machines** affiche une icône en regard de chaque machine, indiquant s'il est prêt pour le déploiement, comme suit :

Zone de texte	Description
Icône verte	AppAssure peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure n'est pas en mesure de se connecter à la machine. Ceci provient peut-être du fait que les références de connexion sont incorrectes, que la machine est arrêtée, que le pare-feu bloque le trafic ou d'un autre problème. Pour corriger le problème, cliquez sur **Modifier les paramètres** sur la barre d'outils ou le lien **Modifier** en regard de la machine.

5. Après avoir bien vérifié les machines, cochez la case en regard de chaque machine et cliquez sur **Déployer**.
6. Si vous avez choisi l'option **Protéger la machine après l'installation**, les machines redémarrent automatiquement si le déploiement réussit et la protection est activée.

Surveillance du déploiement de plusieurs machines

Vous pouvez afficher l'avancement du déploiement du logiciel AppAssure Agent vers les machines.

Pour surveiller le déploiement de plusieurs machines :

1. Depuis Core Console, cliquez sur l'onglet **Événements**, localisez la tâche de déploiement dans la liste, puis cliquez sur le bouton dans la colonne **Détails**.

   La fenêtre **Surveiller la tâche active** affiche les détails du déploiement.

   Cela inclut les informations sur l'ensemble de l'avancement ainsi que l'état de chaque déploiement individuel, notamment :

   - Heure de début
   - Heure de fin
   - Temps écoulé
   - Temps restant
   - Avancement
   - Phase

2. Effectuez l'une des opérations suivantes :
   - Cliquez sur **Ouvrir dans une nouvelle fenêtre** pour lancer une nouvelle fenêtre et afficher l'avancement du déploiement
   - Cliquez sur **Fermer** ; les tâches de déploiement se poursuivent en arrière-plan.

Protection de plusieurs machines

Après un déploiement en masse du logiciel de l'agent vers les machines Windows, vous devez les protéger pour protéger vos données. Si vous avez sélectionné **Protéger la machine après l'installation** lorsque vous avez déployé l'agent, vous pouvez ignorer cette procédure.

REMARQUE : Les machines agents doivent être configurées avec une règle de sécurité permettant l'installation à distance.

Pour protéger plusieurs machines :

1. Depuis Core Console, cliquez sur l'onglet **Outils**, puis sur **Protéger en masse**.
   La fenêtre **Protéger les machines** s'ouvre.
2. Ajoutez les machines que vous souhaitez protéger en cliquant sur l'une des options suivantes :
   Pour plus d'informations sur l'exécution de chaque option, reportez-vous à la section Déploiement sur plusieurs machines.
   - Cliquez sur **Annuaire actif** pour spécifier les machines sur un domaine d'annuaire actif.
   - Cliquez sur **vCenter/ESXi** pour spécifier les machines virtuelles sur un hôte virtuel vCenter/ESXi.
   - Cliquez sur **Nouveau** pour spécifier plusieurs machines en utilisant la boîte de dialogue Ajouter un machine.
   - Cliquez sur **Manuellement** pour spécifier plusieurs machines dans une liste en tapant les noms d'hôte et références.
3. Dans la fenêtre **Protéger les machines**, vous pouvez afficher les machines que vous avez ajoutées. Si vous souhaitez sélectionner un référentiel, une clé de chiffrement ou d'autres paramètres avancés pour une machine, cochez la case en regard de la machine et cliquez sur **Modifier les paramètres**.
4. Spécifiez les paramètres comme suit et cliquez sur **OK**.

Zone de texte	Description
Nom d'utilisateur	Entrez le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, administrateur.
Mot de passe	Entrez le mot de passe sécurisé utilisé pour se connecter à cette machine.
Port	Spécifiez le numéro du port sur lequel le Core communique avec l'agent sur la machine.
Référentiel	Sélectionnez le référentiel sur le Core dans lequel les données des machines sont stockées. Le référentiel que vous choisissez est utilisé pour toutes les machines protégées.
Clé de chiffrement	Spécifiez si le chiffrement est appliqué à l'agent sur les machines qui sont stockées dans le référentiel. La clé de chiffrement est attribuée à toutes les machines protégées.
Planification de la protection	Spécifiez la planification d'application de la protection. La planification par défaut déclenche la protection toutes les 60 minutes pendant les heures pleines et toutes les 60 minutes pendant les week-ends. Pour modifier la planification afin de satisfaire aux besoins de votre entreprise, cliquez sur **Modifier**. REMARQUE : Pour plus d'informations, voir Modifier la planification de protection.
Suspendre initialement la protection	(Facultatif) Vous pouvez choisir de suspendre la protection à la première exécution : le core ne prend pas d'instantanés des machines tant que vous n'avez pas repris manuellement la protection.

5. L'étape suivante consiste à vérifier qu'AppAssure se connecte avec succès à chaque machine. Pour ce faire, cochez la case en regard de chaque machine dans la fenêtre **Protéger les machines**, puis cliquez sur **Vérifier**.

6. La fenêtre **Protéger les machines** affiche une icône en regard de chaque machine qui indique sa disponibilité de déploiement, comme suit :

Icon	Description
Icône verte	AppAssure est en mesure de se connecter à la machine et est prêt à être protégé.
Icône jaune	AppAssure est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure n'est pas en mesure de se connecter à la machine. Ceci provient peut-être du fait que les références de connexion sont incorrectes, que la machine est arrêtée, que le pare-feu bloque le trafic ou d'un autre problème. Pour corriger le problème, cliquez sur **Modifier les paramètres** sur la barre d'outils ou le lien **Modifier** en regard de la machine.

7. Si votre vérification des machines réussit, cochez la case en regard de chaque machine, puis cliquez sur **Protéger**.

Surveillance de la protection de plusieurs machines

Vous pouvez surveiller l'avancement de l'application des stratégies et des horaires aux machines par AppAssure.

Pour surveiller la protection de plusieurs ordinateurs :

1. Sélectionnez l'onglet **Machines** (Ordinateurs) pour afficher l'état et l'avancement de la protection.
   La page **Machines protégées** s'affiche.
2. Sélectionnez l'onglet **Événements** pour afficher les tâches, les événements et les alertes associés.
   La page **Tâches** s'affiche.

Zone de texte	Description
Pour afficher les informations sur la tâche	Au fur et à mesure que les volumes sont transférés, l'état, les heures de début et les heures de fin s'affichent dans le volet **Tâches**. Cliquez sur **Détails** pour afficher des informations plus spécifiques sur la tâche.
Pour afficher les informations sur les alertes	Au fur et à mesure que chaque ordinateur est ajouté, une alerte est journalisée indiquant si l'opération a réussi ou si des erreurs ont été journalisées. Le niveau de l'alerte est affiché, ainsi que la date et le message transactionnels. Si vous souhaitez supprimer toutes les alertes de la page, cliquez sur **Ignorer tout**.
Pour afficher les informations sur les événements	Les détails concernant la machine et les données transférées apparaissent dans le panneau **Événements**. Un message s'affiche, indiquant le niveau de l'événement, la date de la transaction et l'heure.

Gestion des instantanés et points de restauration

Un point de restauration est un ensemble d'instantanés de volumes de disque stockés dans le référentiel. Les instantanés capturent et stockent l'état d'un volume de disque à un point dans le temps, alors que l'application qui génère les données est toujours en cours d'exécution. Dans AppAssure, vous pouvez forcer la création d'un instantané, suspendre temporairement les instantanés et afficher la liste des points de restauration actuels stockés dans le référentiel et les supprimer, si nécessaire. Les points de restauration servent à restaurer les machines protégées ou à effectuer un montage sur un système de fichiers local.

AppAssure capture les instantanés au niveau du bloc avec reconnaissance de l'application. Cela signifie que toutes les transactions et tous les journaux de transaction de cumul ouverts sont terminés, et que les caches sont vidés sur le disque avant la création de l'instantané.

AppAssure utilise un pilote de filtre de volume de bas niveau qui s'attache aux volumes montés et suit toutes les modifications au niveau du bloc pour le prochain instantané prévu. Microsoft Volume Shadow Services (VSS) est utilisé pour faciliter la création d'instantanés cohérents en cas de blocage des applications.

Affichage de points de restauration

Pour afficher les points de restauration :

1. Dans la zone de navigation de gauche de la console AppAssure Core, sélectionnez la machine dont vous souhaitez afficher les points de restauration, puis cliquez sur l'onglet **Points de restauration**.

Vous pouvez afficher des informations sur les points de restauration de la machine, comme indiqué dans le tableau suivant :

Informatif	Description
Condition	Indique l'état actuel du point de restauration.
Crypté	Indique si le point de restauration est crypté.
Contenu	Répertorie les volumes inclus dans le point de restauration.
Type	Définit un point de restauration comme point de restauration de base ou différentiel.
Date de création	Affiche la date à laquelle le point de restauration a été créé.
Taille	Affiche la quantité d'espace que le point de restauration consomme dans le référentiel.

Affichage d'un point de restauration spécifique

Pour afficher un point de restauration particulier :

1. Dans la zone de navigation de gauche de Core Console, sélectionnez la machine dont vous souhaitez afficher les points de restauration, puis cliquez sur l'onglet **Points de restauration**.
2. Cliquez sur **>** en regard d'un point de restauration dans la liste pour développer la vue.

   Vous visualisez des informations plus détaillées concernant le contenu des points de restauration de la machine sélectionnée et vous pouvez accéder à diverses opérations pouvant être exécutées sur un point de restauration. Ces opérations sont décrites dans le tableau suivant :

Informatif	Description
Actions	Le menu **Actions** inclut les opérations suivantes, que vous pouvez réaliser sur le point de restauration sélectionné : **Monter** : sélectionnez cette option pour monter le point de restauration sélectionné. Pour plus d'informations sur le montage du point de restauration sélectionné, voir Montage d'un point de restauration d'une machine Windows.

Exporter : l'option Exporter vous permet d'exporter le point de restauration sélectionné vers ESXi, VMware Workstation ou HyperV. Pour plus d'informations sur l'exportation des points de restauration sélectionnés, reportez-vous à la section Exportation des informations de sauvegarde pour votre machine Windows vers une machine virtuelle.

Restaurer (Rollback) : sélectionnez cette option pour exécuter une restauration depuis le point de restauration sélectionné, sur le volume que vous spécifiez. Pour plus d'informations sur l'exécution de restaurations à partir des points de restauration sélectionnés, voir Lancement de restaurations à partir de AppAssure Core.

3. Cliquez sur **>** en regard d'un volume du point de restauration sélectionné pour développer la vue.

Vous pouvez afficher des informations sur le volume sélectionné dans le point de restauration développé, comme l'indique le tableau suivant :

Zone de texte	Description
Titre	Indique le volume spécifique concerné, dans le point de restauration.
Capacité brute	Indique la quantité d'espace de stockage brut qui existe sur l'ensemble du volume.
Capacité formatée	Indique la quantité d'espace de stockage brut du volume qui est disponible pour les données après formatage du volume.
Capacité utilisée	Indique la quantité d'espace de stockage actuellement utilisée sur le volume.

Montage d'un point de restauration pour une machine Windows

Dans AppAssure, vous pouvez monter un point de restauration pour une machine Windows pour accéder aux données stockées via un système de fichiers local.

Pour monter un point de restauration pour une machine Windows :

1. Dans la console Core, effectuez l'une des opérations suivantes :
   - Sélectionnez l'onglet **Machines**.

     a. En regard de la machine ou du cluster contenant le point de restauration à monter, sélectionnez **Monter** dans le menu déroulant **Actions**.
     b. Sélectionnez un point de restauration dans la liste de la boîte de dialogue **Monter un point de restauration**, puis cliquez sur **Suivant**.

     La boîte de dialogue **Monter des points de restauration** s'ouvre.
   - Dans Core Console, sélectionnez la machine à monter sur un système de fichiers local.

     L'onglet **Récapitulatif** correspondant à la machine sélectionnée apparaît.

     a. Cliquez sur l'onglet **Points de restauration**.
     b. Dans la liste des points de restauration, développez le point à monter.
     c. Dans les détails de ce point de restauration, cliquez sur **Monter**.

     La boîte de dialogue **Monter des points de restauration** s'ouvre.
2. Dans la boîte de dialogue **Monter**, modifiez les champs afin de monter le point de restauration comme indiqué dans le tableau suivant :

Zone de texte	Description
Emplacement de montage : fichier local	Indiquez le chemin qui sera utilisé pour accéder au point de restauration monté.
Images de volume	Spécifiez les images de volume que vous souhaitez monter.
Type de montage	Spécifiez la façon d'accéder au point de restauration monté : • Monter en lecture seule. • Monter en lecture seule avec les écritures précédentes. • Monter en écriture.
Créez un partage Windows pour ce montage.	(Facultatif) Cochez cette case pour indiquer si le point de restauration monté peut être partagé, puis définissez les droits d'accès à ce point, notamment le nom de partage et les groupes d'accès.

3. Cliquez sur **Monter** pour monter le point de restauration.

Démontage des points de restauration sélectionnés

Vous pouvez démonter les points de restauration sélectionnés montés localement sur le core.
Pour effectuer un démontage, sélectionnez des points de restauration :

1. Dans Core Console, sélectionnez l'onglet **Outils**.
2. Depuis l'option **Outils**, sélectionnez **Infos système**.
3. Localisez et sélectionnez l'affichage monté pour le point de restauration à démonter, puis cliquez sur **Démonter**.

Démontage de tous les points de restauration

Vous pouvez démonter tous les points de restauration montés localement sur le core.
Pour démonter tous les points de restauration

1. Dans Core Console, sélectionnez l'onglet **Outils**.
2. Depuis l'option **Outils**, sélectionnez **Infos système**.
3. Dans la section **Montages locaux**, cliquez sur **Démonter tout**.

Montage d'un volume de points de restauration sur une machine Linux

1. Créez un nouveau répertoire pour le montage du 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 **aamount** en tant que root ou super utilisateur, par exemple :
   ```
   sudo aamount
   ```
4. À l'invite de montage d'AppAssure, entrez la commande suivante pour répertorier les ordinateurs protégés.
   ```
   lm
   ```
5. Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte de votre serveur AppAssure Core.

6. Entrez les références de connexion du serveur Core, c'est-à-dire le nom d'utilisateur et mot de passe.

   Une liste apparaît et affiche les ordinateurs protégés par ce serveur AppAssure. Les ordinateurs sont répertoriés par numéro d'objet de ligne, adresse IP/d'hôte et un numéro d'identification pour l'ordinateur (par exemple : `293cc667-44b4-48ab-91d8-44bc74252a4f`).

7. Saisissez la commande suivante pour afficher la liste des points de restauration montées actuellement d'un ordinateur donné :

   ```
   lr <line_number_of_machine>
   ```

   REMARQUE : Vous pouvez également entrer dans cette commande le numéro d'ID de la machine au lieu du numéro d'article figurant sur une ligne.

   Une liste apparaît et affiche les points de restauration de base et incrémentiels de cet ordinateur-là. Cette liste comprend un numéro d'objet de ligne, une date/horodatage, l'emplacement du volume, la taille du point de restauration et un numéro d'identification du volume qui comprend un numéro de séquence à la fin (par exemple, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), qui identifie le point de restauration.

8. Saisissez la commande suivante pour sélectionner et monter le point de restauration spécifié au point/chemin de montage spécifié.

   ```
   m <volume_recovery_point_ID_number> <path>
   ```

   REMARQUE : Vous pouvez aussi spécifier un numéro de ligne dans la commande au lieu du numéro d'identification du point de restauration pour identifier celui-ci. Dans ce cas, utilisez le numéro de ligne de l'agent/ordinateur (depuis la sortie lm), suivi par le numéro de ligne de point de restauration et la lettre de volume, suivis par le chemin, tel que `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`. Par exemple, si la sortie `lm` énumère trois ordinateurs d'agent et que vous saisissez la commande `lr` pour le numéro 2 et que vous souhaitez monter le volume b du point de restauration 23 à **/tmp/mount_dir**, la commande est la suivante : `m 2 23 b /tmp/mount_dir`.

   PRÉCAUTION : Vous ne devez pas démonter un volume Linux protégé manuellement. Au cas où vous auriez besoin de le faire, vous devrez exécuter la commande suivante avant de démonter le volume : `bsctl -d <path to volume>`. Dans cette commande, `<path to volume>` ne fait pas référence au point de montage du volume mais plutôt au descripteur de fichier du volume ; il doit suivre un format semblable à cet exemple : /dev/sda1.

Suppression de points de restauration

Vous pouvez facilement supprimer des points de restauration d'une machine à partir du référentiel. Lorsque vous supprimez des points de restauration dans AppAssure vous pouvez spécifier l'une des options suivantes :

Zone de texte	Description
Supprimer tous les points de restauration	Supprime tous les points de restauration de l'ordinateur agent sélectionné du référentiel.
Supprimer une plage de points de restauration	Supprime tous les points de restauration d'une plage spécifiée avant le point de restauration actuel, et jusqu'à l'image de base incluse (c'est-à-dire toutes les données de l'ordinateur), ainsi que tous les points de restauration après le point de restauration actuel jusqu'à l'image de base.

REMARQUE : Vous ne pouvez pas récupérer les points de restauration que vous avez supprimés.

Pour supprimer des points de restauration :

1. Dans la zone de navigation de gauche de la console AppAssure Core, sélectionnez la machine dont vous souhaitez afficher les points de restauration, puis cliquez sur l'onglet **Points de restauration**.
2. Cliquez sur le menu **Actions**.
3. Sélectionnez l'une des options suivantes :
   - Pour supprimer tous les points de restauration actuellement stockés, cliquez sur **Supprimer tout**.
   - Pour supprimer un ensemble de points de restauration dans une plage de données spécifique, cliquez sur **Supprimer une plage**. La boîte de dialogue **Supprimer** s'affiche. Dans la boîte de dialogue **Supprimer une plage**, spécifiez la plage de points de restauration que vous souhaitez supprimer à l'aide d'une date et heure de début et d'une date et heure de fin, puis cliquez sur **Supprimer**.

Suppression d'une chaîne de points de restauration orphelins

Un point de restauration orphelin est un instantané incrémentiel qui n'est associé à aucune image de base. Les instantanés suivants continuent à s'empiler sur ce point de restauration. Sans image de base, les points de restauration qui en résultent sont incomplets et ne contiendront sans doute pas toutes les données nécessaires pour effectuer une restauration. Ces points de restauration sont considérés comme membres de la chaîne de points de restauration orphelins. Dans cette situation, la meilleure solution consiste à supprimer la chaîne et à créer une nouvelle image de base.

REMARQUE : L'option de suppression d'une chaîne de points de restauration orphelins n'est pas disponible pour les points de restauration répliqués sur un core cible.

Pour supprimer une chaîne de points de restauration orphelins :

1. Dans Core console, sélectionnez la machine protégée dont vous souhaitez supprimer la chaîne de points de restauration orphelins.
2. Cliquez sur l'onglet **Points de restauration**.
3. Sous **Points de restauration**, développez le point de restauration orphelin.

   Ce point de restauration est marqué (dans la colonne **Type**) de la mention **Incrémentiel orphelin**.
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 de ce point de restauration supprime l'ensemble de la chaîne de points de restauration, y compris les points de restauration incrémentiels qui se produisent avant ou après, jusqu'à l'image de base suivante. Cette opération ne peut pas être annulée.

   La chaîne de points de restauration orphelins est supprimée.

Forcer un instantané

Le fait de forcer un instantané vous permet de forcer un transfert de données pour la machine actuellement protégée. Lorsque vous forcez un instantané, le transfert démarre immédiatement ou est ajouté à la file d'attente. Seules les données déplacées d'un point de restauration précédent sont transférées. S'il n'existe aucun point de restauration précédent, toutes les données des volumes protégés sont transférées : cette opération s'appelle une image de base.

Pour forcer un instantané :

1. Dans Core Console, cliquez sur l'onglet **Machines**, puis, dans la liste des machines protégées, sélectionnez la machine ou le cluster qui contient le point de restauration pour lequel vous souhaitez forcer un instantané.
2. Cliquez sur le menu déroulant **Actions** de cette machine, sélectionnez **Forcer un instantané**, puis choisissez l'une des options décrites ci-dessous :
   - **Forcer un instantané** : prend un instantané incrémentiel des données mises à jour depuis la prise du dernier instantané.
   - **Forcer une image de base** : prend un instantané complet de toutes les données des volumes de la machine.
3. Lorsque la notification indiquant que l'instantané a été mis dans la file d'attente s'affiche, dans la boîte de dialogue **État du transfert**, cliquez sur **OK**.

   Une barre de progression apparaît à côté de la machine dans l'onglet **Machines** pour illustrer l'avancement de l'instantané.

Suspension et reprise de la protection

Lorsque vous suspendez la protection, vous arrêtez temporairement tous les transferts de données depuis la machine actuelle.

Pour suspendre et relancer la protection :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Sélectionnez la machine pour laquelle vous souhaitez suspendre la protection.

   L'onglet **Récapitulatif** correspondant à cette machine s'affiche.
3. Dans le menu déroulant **Actions** de cet ordinateur, cliquez sur **Suspendre**.
4. Pour reprendre la protection, cliquez sur **Reprendre** dans le menu **Actions**.

Restauration des données

Vous pouvez immédiatement restaurer des données sur vos machines physiques (Windows ou Linux) ou sur les machines de points de restauration stockés pour les machines Windows. Les rubriques de cette section décrivent comment exporter un point de restauration spécifique d'une machine Windows à une machine virtuelle ou comment effectuer une restauration automatique vers un point de restauration antérieur.

Si vous avez configuré la réplication entre deux cores (source et cible), vous pouvez uniquement exporter les données depuis le core cible une fois que la réplication initiale est terminée. Pour plus de détails, voir Réplication des données d'agent sur une machine.

REMARQUE : Les systèmes d'exploitation Windows 8 et Windows Server 2012 amorcés depuis des partitions FAT32 EFI ne peuvent pas faire l'objet de la protection ni de la récupération, de même que les volumes de Resilient File System (ReFS).

Sauvegarde

L'onglet Sauvegarde vous permet de configurer la stratégie de sauvegarde et de restaurer le système à l'aide de la clé USB RASR ou IDSDM. Pour que vous puissiez utiliser cette fonctionnalité, il doit exister un disque virtuel de Sauvegarde Windows. Le disque virtuel de Sauvegarde Windows est créé au cours de l'exécution de l'**Assistant Configuration de l'appliance AppAssure**. Pour plus d'informations, reportez-vous à la section Appliance Self Rapid Recovery (Restauration automatique de Rapid Appliance) dans le

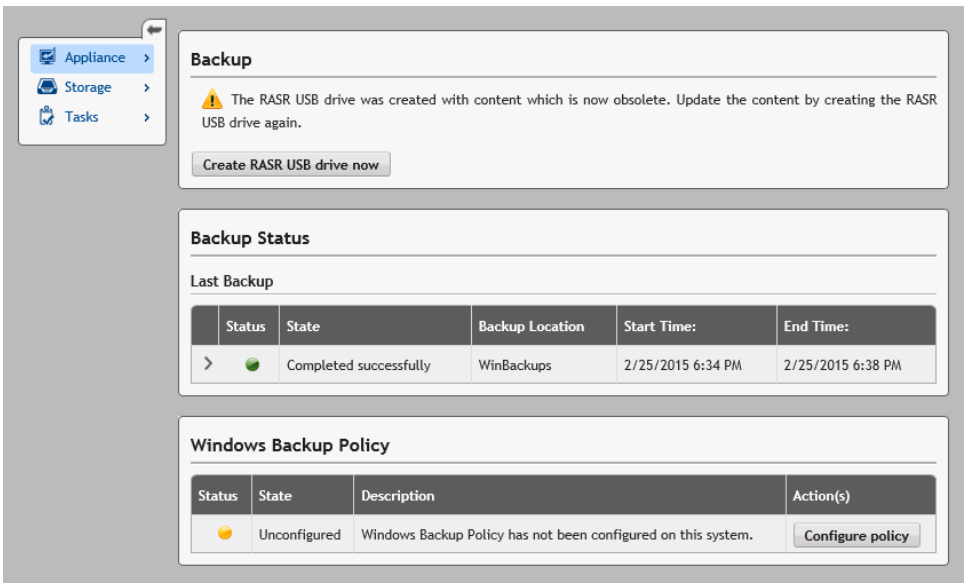
Guide de déploiement Dell DL43000. En l'absence d'un disque virtuel de Sauvegarde Windows, vous ne pouvez pas configurer une stratégie ni créer des sauvegardes Windows.

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 Core Console, naviguez jusqu'à l'onglet **Appliance** → **Sauvegarde** .
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 :
   - Condition
   - 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 Windows soit exécutée ou non.



Si une sauvegarde est en cours d'exécution, les informations concernant l'**Avancement 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 Core Console, naviguez jusqu'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 :	• OS (C :) • RESTAURATION • Restauration sans système d'exploitation (BMR) • État du système Tous les éléments ci-dessus sont sélectionnés par défaut.
Sélectionnez l'heure de programmation de la sauvegarde :	Entrez la durée pour planifier une sauvegarde.

4. Cliquez sur **Configurer**.
   Une fois la configuration effectuée, vous avez la possibilité de **Sauvegarder maintenant**, **Supprimer la stratégie** ou **Afficher la stratégie** à partir de la fenêtre **Stratégie de sauvegarde Windows** .

À propos de l'exportation des données protégées de machines Windows vers des machines virtuelles

AppAssure prend en charge l'exportation ponctuelle ou l'exportation en continu (pour prendre en charge les disques virtuels de secours) des informations de sauvegarde Windows vers une machine virtuelle. L'exportation des données vers une machine de secours virtuelle fournit une copie haute disponibilité des données. Si une machine protégée tombe en panne, vous pouvez amorcer la machine virtuelle, puis réaliser une restauration.

Le diagramme suivant montre un déploiement typique d'exportation de données vers une machine virtuelle.

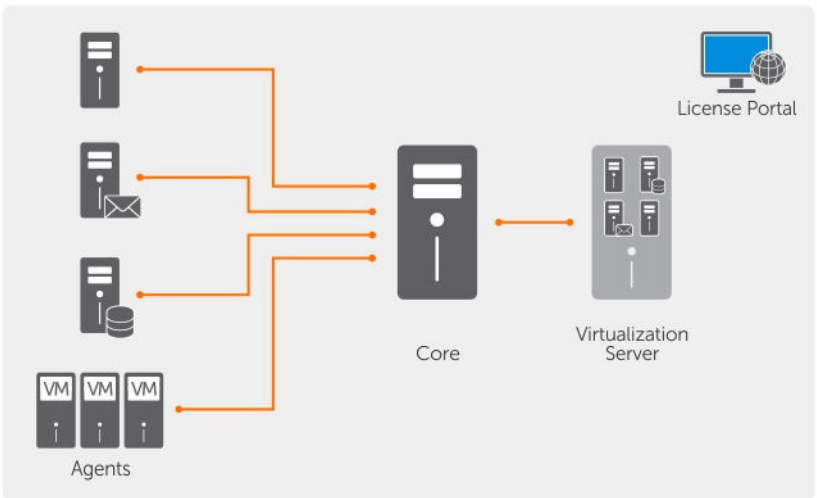


Figure 9. Exportation de données vers une machine virtuelle

Vous créez un disque virtuel de secours en exportant en continu les données protégées depuis votre machine Windows vers une machine virtuelle. Lorsque vous exportez les données vers une machine virtuelle, le programme exporte toutes les données de sauvegarde d'un point de restauration, ainsi que les paramètres définis pour la planification de protection de votre machine.

Vous pouvez effectuer l'exportation virtuelle de points de récupération pour vos machines protégées Linux ou Windows vers VMware, ESXi, Hyper-V et Oracle VirtualBox.

REMARQUE : L'onglet Appliance affiche toutes les machines virtuelles, mais ne prend en charge que la gestion des machines virtuelles 'Hyper-V et ESXi. Pour gérer les autres machines virtuelles, utilisez les outils de gestion de l'hyperviseur.

REMARQUE : La machine virtuelle cible de l'exportation doit être une version sous licence d'ESXi, VMWare Workstation ou Hyper-V, et pas une version d'évaluation ou gratuite.

Limites de support des volumes dynamiques et de base

AppAssure prend en charge la prise d'instantanés de tous les volumes de base et dynamiques. AppAssure prend également en charge l'exportation des volumes dynamiques simples sur un seul disque physique. Comme son nom l'indique, les volumes dynamiques simples ne sont pas répartis, en miroir ou des volumes étendus. Les volumes dynamiques non simples comportent des géométries de disque arbitraires impossibles à interpréter entièrement, ce qui ne peuvent pas être exportées. AppAssure a la possibilité d'exporter des volumes dynamiques complexes ou non simples.

Dans AppAssure version 5.3.1.60393, nous avons ajouté une case à cocher dans l'interface utilisateur, afin de vous informer que les exportations sont limitées aux volumes dynamiques simples. Avant ce changement dans l'interface de la nouvelle version, l'option d'exportation de disques dynamiques complexes ou non simples aurait semblé disponible, mais toute tentative d'exportation de ces disques aurait échoué.

Exportation des informations de sauvegarde de votre machine Microsoft Windows vers une machine virtuelle

Dans AppAssure, vous pouvez exporter des données à partir vos ordinateurs Microsoft Windows vers une machine virtuelle (VMware, ESXi, Hyper-V et Oracle VirtualBox) en exportant toutes les informations de sauvegarde à partir d'un point de restauration, ainsi que les paramètres définis pour l'horaire de protection de votre ordinateur.

Pour exporter les informations de sauvegarde Windows vers une machine virtuelle :

1. Dans la console Core, cliquez sur l'onglet **Machines** (Ordinateurs).
2. Dans la liste des machines protégés, sélectionnez la machine ou le cluster ayant le point de restauration dont vous souhaitez forcer un instantané.
3. Dans le menu déroulant **Actions** de cette machine, cliquez sur **Exporter** et sélectionnez le type d'exportation que vous souhaitez effectuer. Vous avez le choix entre :
   - Exportation ESXi
   - Exportation VMware Workstation
   - Exportation Hyper-V
   - Exportation Oracle VirtualBox

   La boîte de dialogue **Sélectionner le type d'exportation** s'affiche.

Exportation des données Windows à l'aide de l'exportation ESXi

Dans AppAssure, vous pouvez choisir d'exporter les données en utilisant ESXi Export en effectuant une exportation ponctuelle ou continue.

Exécution d'une exportation ESXi ponctuelle

Pour effectuer une exportation ESXi ponctuelle :

1. Dans la boîte de dialogue **Sélectionner le type d'exportation**, cliquez sur **Exportation ponctuelle**.
2. Cliquez sur **Suivant**.
   La boîte de dialogue **Exportation ESXi - Sélectionner un point de restauration** s'affiche.
3. Sélectionnez un point de restauration pour exporter, puis cliquez sur **Suivant.**
   La boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware vCenter Server/ESXi** s'affiche.

Définition des informations de machine virtuelle pour effectuer une exportation ESXi

Pour définir les informations de machine virtuelle afin d'effectuer une exportation ESXi :

1. Dans la boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware vCenter Server/ESXi**, entrez les paramètres permettant d'accéder à la machine virtuelle, comme suit :

Zone de texte	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Saisissez le port pour la machine hôte. Le port par défaut est 443.
Nom d'utilisateur	Entrez les références de connexion de la machine hôte.
Mot de passe	Entrez les références de connexion de la machine hôte.

2. Cliquez sur **Connexion** .

Exécution d'une exportation ESXi continue (disque de secours virtuel)

Pour effectuer une exportation ESXi continue (disque de secours virtuel) :

1. Dans la boîte de dialogue **Sélectionner le type d'exportation**, cliquez sur **Continu (disque de secours virtuel)**.
2. Cliquez sur **Suivant**.
   La boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware vCenter Server/ESXi** s'affiche.
3. Saisissez les paramètres nécessaires pour accéder à la machine virtuelle tel que décrit ci-dessous.

Zone de texte	Description
Nom de l'hôte	Entrez un nom pour la machine hôte.
Port	Saisissez le port pour la machine hôte. Le port par défaut est 443.
Nom d'utilisateur	Entrez les références de connexion de la machine hôte.
Mot de passe	Entrez les références de connexion de la machine hôte.

4. Cliquez sur sur Connexion .
5. Dans l'onglet **Options**, saisissez les informations sur la machine virtuelle tel que décrit.

Zone de texte	Description
Nom de la machine virtuelle	Saisissez un nom pour la machine virtuelle en cours de création ; par exemple, 'VM-0A1B2C3D4. REMARQUE : Il est recommandé d'utiliser un nom dérivé du nom de l'agent ou un nom qui correspond au nom de l'agent. Vous pouvez également créer un nom dérivé du type de l'hyperviseur, de l'adresse IP ou du nom DNS.
Mémoire	Spécifiez l'utilisation de la mémoire. Vous avez le choix entre : • Utiliser la même quantité de RAM que l'ordinateur source • Cliquez sur **Utiliser une quantité spécifique de RAM** pour spécifier la quantité de RAM à utiliser, par exemple, 4096 Mo. La quantité minimale autorisée est de 512 Mo et le maximum est déterminé par la capacité et les limites des machines hôte.
Centre de données ESXi	Entrez le nom du centre de données ESXi.
Hôte ESXi	Entrez les références de l'hôte ESXi.
Stockage des données	Entrez les détails du stockage des données.
Version	Sélectionnez la version de la machine virtuelle. REMARQUE : Pour utiliser le client vSphere pour gérer des machines virtuelles, sélectionnez la version 8 ou une version antérieure.
Pool de ressources	Entrez un nom pour le pool de ressources.

6. Cliquez sur **Lancer l'exportation**.

Exportation des données à l'aide de l'exportation VMware Workstation

Dans AppAssure, vous pouvez choisir d'exporter les données à l'aide de VMware Workstation Export en effectuant une exportation ponctuelle ou continue. Effectuez les étapes des procédures suivantes pour exporter à l'aide de VMware Workstation Export pour le type d'exportation approprié.

Effectuer une exportation ponctuelle de VMware workstation (station de travail VMware)

Pour effectuer une exportation VMware Workstation ponctuelle

1. Dans la boîte de dialogue **Sélectionner le type d'exportation**, cliquez sur **Exportation ponctuelle**.
2. Cliquez sur **Suivant**.
   La boîte de dialogue **Exportation VM - Sélectionner un point de restauration** s'affiche.
3. Sélectionnez un point de restauration pour exporter, puis cliquez sur **Suivant.**
   La boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware Workstation/ Server** s'affiche.

Définition des paramètres ponctuels d'exportation de station de travail VMware

Définition des paramètres ponctuels d'exportation de la station de travail VMware :

1. Dans la boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware Workstation/Server**, entrez les paramètres permettant d'accéder à la machine virtuelle, comme suit :

Zone de texte	Description
Chemin d'accès cible	Spécifiez le chemin du dossier local ou du partage réseau dans lequel créer la machine virtuelle. REMARQUE : Si vous avez spécifié un chemin de partage réseau, saisissez des références de connexion valides d'un compte enregistré sur la machine cible. Le compte doit être doté de droits de lecture et d'écriture sur le partage réseau.
Nom d'utilisateur	Saisissez les références de connexion de la machine virtuelle. • Si vous avez spécifié un chemin de partage réseau, vous devez saisir un nom d'utilisateur valide pour un compte inscrit auprès de la machine cible. • Si vous entrez un chemin local, un nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les références de connexion de la machine virtuelle. • Si vous avez spécifié un chemin de partage réseau, vous devez saisir un mot de passe valide pour un compte inscrit auprès de la machine cible. • Si vous entrez un chemin local, un mot de passe n'est pas nécessaire.

2. Dans le volet **Exporter des volumes**, sélectionnez les volumes à exporter ; par exemple, C:\ et D:\.
3. Dans le volet Options, entrez les informations pour la machine virtuelle et l'utilisation de mémoire tel que décrit dans le tableau suivant.

Zone de texte	Description
Machine virtuelle	Saisissez un nom pour la machine virtuelle en cours de création ; par exemple, VM-0A1B2C3D4. REMARQUE : Il est recommandé d'utiliser un nom dérivé du nom de l'agent ou un nom qui correspond au nom de l'agent. Vous pouvez également créer un nom dérivé du type de l'hyperviseur, de l'adresse IP ou du nom DNS.
Mémoire	Spécifiez la mémoire de la machine virtuelle. • Cliquez sur **Utiliser la même quantité de RAM que la machine source** pour spécifier que la configuration RAM est la même que pour la machine source. • Cliquez sur **Utiliser une quantité spécifique de RAM** pour spécifier la quantité de RAM à utiliser. Par exemple, 4096 Mo. La quantité minimale autorisée est de 512 Mo et le maximum est déterminé par la capacité et les limites de l'ordinateur hôte.

4. Cliquez sur **Exporter**.

Effectuer une exportation continue de station de travail VMware (disque de secours virtuel)

Pour effectuer une exportation VMware Workstation continue (disque de secours virtuel) :

1. Dans la boîte de dialogue **Sélectionner le type d'exportation**, cliquez sur **Continu (disque de secours virtuel)**, puis cliquez sur **Suivant**.

   La boîte de dialogue **Exportation VM - Sélectionner un point de restauration** s'affiche.
2. Sélectionnez un point de restauration pour exporter, puis cliquez sur **Suivant.**

   La boîte de dialogue **Point de restauration du disque de secours virtuel vers VMware Workstation/ Server** s'affiche.
3. Saisissez les paramètres d'accès à la machine virtuelle, comme suit :

Zone de texte	Description
Chemin d'accès cible	Spécifiez le chemin du dossier local ou du partage réseau dans lequel créer la machine virtuelle. REMARQUE : Si vous avez spécifié un chemin de partage réseau, saisissez des références de connexion valides d'un compte enregistré sur la machine cible. Le compte doit être doté de droits de lecture et d'écriture sur le partage réseau.
Nom d'utilisateur	Saisissez les références de connexion de la machine virtuelle. • Si vous avez spécifié un chemin de partage réseau, vous devez saisir un nom d'utilisateur valide pour un compte inscrit auprès de la machine cible. • Si vous entrez un chemin local, un nom d'utilisateur n'est pas nécessaire.
Mot de passe	Saisissez les références de connexion de la machine virtuelle. • Si vous avez spécifié un chemin de partage réseau, vous devez saisir un mot de passe valide pour un compte inscrit auprès de la machine cible. • Si vous entrez un chemin local, un mot de passe n'est pas nécessaire.

4. Dans le volet **Exporter des volumes**, sélectionnez les volumes à exporter ; par exemple, C:\ et D:\.
5. Dans le volet **Options**, entrez les informations de la machine virtuelle et l'utilisation de mémoire tel que décrit dans le tableau suivant.

Zone de texte	Description
Machine virtuelle	Saisissez un nom pour la machine virtuelle en cours de création ; par exemple, `VM-0A1B2C3D4`. REMARQUE : Il est recommandé d'utiliser un nom dérivé du nom de l'agent ou un nom qui correspond au nom de l'agent. Vous pouvez également créer un nom dérivé du type de l'hyperviseur, de l'adresse IP ou du nom DNS.
Mémoire	Spécifiez la mémoire de la machine virtuelle. • Cliquez sur **Utiliser la même quantité de RAM que la machine source** pour spécifier que la configuration RAM est la même que pour la machine source. • Cliquez sur **Utiliser une quantité spécifique de RAM** pour spécifier la quantité de RAM à utiliser, par exemple, 4 096 Mo. La quantité minimale

Zone de texte	Description
	autorisée est de 512 Mo, et le maximum dépend de la capacité et des limites de la machine hôte. (recommandé)

6. Cliquez sur **Effectuer une exportation ad-hoc initiale** pour tester l'exportation des données.
7. Cliquez sur **Enregistrer**.

Exportation des données Windows à l'aide de l'exportation Hyper-V

Vous pouvez choisir d'exporter les données à l'aide d'Hyper-V Export en effectuant une exportation ponctuelle ou continue. Effectuez les étapes des procédures suivantes pour exporter à l'aide de l'Hyper-V Export pour le type d'exportation approprié.
L'appliance DL prend en charge l'exportation des 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

La deuxième génération DL prend en charge l'exportation Hyper-V vers les hôtes suivants :

- Windows 8.1
- Windows Server 2012 R2

REMARQUE : Toutes les machines protégées ne peuvent pas être exportées vers des hôtes Hyper-V de deuxième génération.

Seuls les ordinateurs protégés avec le système d'exploitation UEFI (Unified Extensible Firmware Interface) prennent en charge l'exportation virtuelles vers des hôtes Hyper-V de deuxième génération :

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

REMARQUE : L'exportation Hyper-V vers une VM de deuxième génération peut échouer si l'hôte Hyper-V ne dispose pas de suffisamment de RAM allouée pour effectuer l'exportation.

Effectuez les étapes des procédures suivantes pour le type d'exportation appropriée.

Exécution d'une exportation Hyper-V ponctuelle

Pour effectuer une exportation Hyper-V ponctuelle

1. Dans la Core Console, accédez à la machine à exporter.
2. Dans l'onglet Récapitulatif, cliquez sur **Actions → Exporter → Une fois**.
   L'**Assistant Exportation** affiche la page **Machines protégées**.
3. Sélectionnez une machine pour l'exportation, puis cliquez sur **Suivant**.
4. Sur la page **Points de restauration**, sélectionnez le point de restauration à exporter, puis cliquez sur **Suivant**.

Définition de paramètres ponctuels pour effectuer une exportation Hyper-V

Pour définir des paramètres ponctuels pour effectuer une exportation Hyper-V

1. Dans la boîte de dialogue Hyper-V, cliquez sur **Utiliser la machine locale** pour effectuer l'exportation Hyper-V vers une machine local auquel le rôle Hyper-V est attribué.
2. Cliquez sur l'option **Hôte distant** pour indiquer que le serveur Hyper-V est situé sur une machine distante. Si vous avez sélectionné cette option, entrez les paramètres de l'hôte distant, comme suit :

Zone de texte	Description
Nom d'hôte	Entrez une adresse IP ou un nom d'hôte pour le serveur Hyper-V. Ceci représente l'adresse IP ou le nom d'hôte du serveur Hyper-V distant.
Port	Entrez un numéro de port pour la machine. Il représente le port par l'intermédiaire duquel le core communique avec cette machine.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'utilisateur doté de privilèges d'administration de la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe du compte d'utilisateur doté de privilèges d'administration sur la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.

3. Cliquez sur **Suivant**.
4. Sur la page **Options de machines virtuelles** dans la zone de texte **Emplacement de la machine VM**, entrez le chemin d'accès ou l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement VM doit disposer de suffisamment d'espace pour contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
5. Entrez le nom de la machine virtuelle dans la zone de texte **Nom de la machine virtuelle** .

   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
6. Sélectionnez l'une des options suivantes :
   - **Utiliser la même quantité de RAM que la machine source** pour spécifier que l'utilisation de RAM est identique pour la machine virtuelle et la machine source.
   - Cliquez sur **Utiliser une quantité de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo. (recommandé).
7. Pour spécifier le format de disque, en regard de **Format de disque**, cliquez sur l'une des options suivantes :
   - **VHDX**
   - **VHD**

   REMARQUE : Hyper-V Export prend en charge les formats de disque si la machine cible exécute Windows 8 (Windows Server 2012) ou une version supérieure. Si VHDX n'est pas pris en charge pour votre environnement, cette option est désactivée.
8. Sur la page **Volumes**, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une sauvegarde efficace de la machine protégée, incluez le lecteur d'amorçage de la machine protégée, par exemple : C:\.

   Les volumes sélectionnés ne doivent pas dépasser 2 040 Go pour le disque dur virtuel. Si les volumes sélectionnés dépassent 2 040 Go et que vous sélectionnez le format VHD, vous recevez un message d'erreur.
9. Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

Exécution d'une exportation Hyper-V continue (disque de secours virtuel)

REMARQUE : Seules les configurations du DL1000 incluant 3 To d'espace avec 2 VM (machines virtuelles) prennent en charge l'exportation ponctuelle et l'exportation en continu (disque de secours virtuel).

Pour effectuer une exportation continue Hyper-V (disque de secours virtuel) :

1. dans Core Console, sur l'onglet **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l' **Assistant Exportation**. Sur la page **Machines protégées** de l'**Assistant Exportation**.
2. Sélectionnez la machine à exporter, puis cliquez sur **Suivant**.
3. Dans l'onglet **Récapitulatif**, cliquez sur **Exporter → Disque de secours virtuel**.
4. Dans la boîte de dialogue Hyper-V, cliquez sur **Utiliser la machine locale** pour effectuer l'exportation Hyper-V vers une machine local auquel le rôle Hyper-V est attribué.
5. Cliquez sur l'option **Hôte distant** pour indiquer que le serveur Hyper-V est situé sur une machine distante. Si vous avez sélectionné cette option, entrez les paramètres de l'hôte distant, comme suit :

Zone de texte	Description
Nom d'hôte	Entrez une adresse IP ou un nom d'hôte pour le serveur Hyper-V. Ceci représente l'adresse IP ou le nom d'hôte du serveur Hyper-V distant.
Port	Entrez un numéro de port pour la machine. Il représente le port par l'intermédiaire duquel le core communique avec cette machine.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'utilisateur doté de privilèges d'administration de la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe du compte d'utilisateur doté de privilèges d'administration sur la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.

6. Sur la page **Options de machines virtuelles** dans la zone de texte **Emplacement de la machine VM**, entrez le chemin d'accès ou l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement VM doit disposer de suffisamment d'espace pour contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
7. Entrez le nom de la machine virtuelle dans la zone de texte **Nom de la machine virtuelle** .

   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
8. Sélectionnez l'une des options suivantes :
   - **Utiliser la même quantité de RAM que la machine source** pour spécifier que l'utilisation de RAM est identique pour la machine virtuelle et la machine source.
   - Cliquez sur **Utiliser une quantité de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo (recommandé).
9. Pour spécifier la génération, cliquez sur l'une des options suivantes :
   - Génération 1 (recommandé)
   - Génération 2
10. Pour spécifier le format de disque, en regard de **Format de disque**, cliquez sur l'une des options suivantes :
    - **VHDX** (par défaut)
    - **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 version ultérieure. Si la VHDX n'est pas prise en charge pour votre environnement, cette option est désactivée. Sur la page Adaptateurs réseau, sélectionnez l'adaptateur virtuel à connecter à un commutateur.

11. Sur la page **Volumes**, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une sauvegarde efficace de la machine protégée, incluez le lecteur d'amorçage de la machine protégée, par exemple : C:\.

    Les volumes sélectionnés ne doivent pas dépasser 2 040 Go pour le disque dur virtuel. Si les volumes sélectionnés dépassent 2 040 Go et que vous sélectionnez le format VHD, vous recevez un message d'erreur.

12. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

    REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

Exportation des données Microsoft Windows à l'aide d'une exportation Oracle VirtualBox

Dans AppAssure, vous pouvez choisir d'exporter les données à l'aide d'une exportation Oracle VirtualBox en effectuant une exportation ponctuelle ou en établissant une exportation en continu (pour les disques virtuels de secours).

Effectuez les étapes des procédures suivantes pour le type d'exportation appropriée.

REMARQUE : Pour que vous puissiez effectuer ce type d'exportation, Oracle VirtualBox doit être installé sur la machine Core. VirtualBox Version 4.2.18 ou ultérieure est pris en charge pour les hôtes Windows.

Exécution d'une exportation Oracle VirtualBox ponctuelle

Suivez les étapes de cette procédure pour effectuer une exportation ponctuelle.

Pour effectuer une exportation Oracle VirtualBox ponctuelle :

1. Dans la Core Console AppAssure, effectuez l'une des opérations suivantes :
   - Dans la barre de boutons, cliquez sur **Exporter** pour lancer l'Assistant Exportation, puis procédez comme suit :
     1. Sur la page **Sélectionner le type d'exportation** , cliquez sur **Exportation ponctuelle**, puis cliquez sur **Suivant**.
     2. Sur la page **Machines protégées**, sélectionnez la machine protégée que vous souhaitez exporter vers une machine virtuelle, puis cliquez sur **Suivant**.
   - Accédez à la machine que vous souhaitez exporter, puis, dans l'onglet **Résumé** , dans le menu déroulant **Actions** de cette machine, sélectionnez **Exporter** > **Une seule fois**.

   L'Assistant Exportation apparaît sur la page **Points de restauration** .
2. Sur la page **Points de restauration**, sélectionnez le point de restauration du Core AppAssure à exporter, puis cliquez sur **Suivant**.
3. Sur la page **Destination** de l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers la machine virtuelle**, sélectionnez VirtualBox, puis cliquez sur **Suivant**.
4. Sur la page **Options de la machine virtuelle**, sélectionnez **Utiliser une machine Windows.**
5. Entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

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 d'accès cible	Spécifiez un chemin cible local ou distant pour créer la machine virtuelle. REMARQUE : Le chemin d 'accès cible ne doit pas être un répertoire racine. Si vous spécifiez un chemin de partage réseau, vous devez entrer les informations d'identification valides (nom d'utilisateur et mot de passe) d'un compte enregistré dans la machine cible. Le compte doit avoir les autorisations en lecture et en écriture sur le partage réseau.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Cliquez sur **Utiliser la même quantité de RAM que la machine source** pour spécifier que la configuration RAM est la même que pour la machine source. • Cliquez sur **Utiliser une quantité spécifique de RAM** pour spécifier la quantité de RAM à utiliser, par exemple, 4 096 Mo. La quantité minimale autorisée est de 512 Mo, et le maximum dépend de la capacité et des limites de la machine hôte. (recommandé)

6. Pour spécifier un compte d'utilisateur pour la machine virtuelle, sélectionnez **Spécifier le compte d'utilisateur sous lequel la machine virtuelle est exportée**, puis entrez les informations suivantes. Elles font référence à un compte d'utilisateur spécifique pour lequel la machine virtuelle sera enregistrée dans le cas où il existe plusieurs comptes d'utilisateur sur la machine virtuelle. Lorsque ce compte d'utilisateur est connecté, seul cet utilisateur voit la machine virtuelle dans le gestionnaire VirtualBox. Si aucun compte n'est spécifié, la machine virtuelle est enregistrée pour tous les utilisateurs existants sur la machine Windows avec Oracle VirtualBox.
   - **Nom d'utilisateur** : entrez le nom d'utilisateur pour lequel la machine virtuelle est enregistrée.
   - **Mot de passe** : entrez le mot de passe de ce compte d'utilisateur.
7. Cliquez sur **Suivant**.

   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
8. Sur la page Volumes, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une sauvegarde efficace de la machine protégée, incluez le lecteur d'amorçage de la machine protégée. Exemple : C:\.
9. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour terminer l'Assistant et démarrer l'exportation.

   REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

Exécution d'une exportation Oracle VirtualBox continue (disque de secours virtuel)

Effectuez les étapes de cette procédure pour créer un disque virtuel de secours et effectuer une exportation continue vers Oracle VirtualBox.

Pour effectuer une exportation VirtualBox continue (disque de secours virtuel) :

1. Dans la console AppAssure Core, effectuez une des opérations suivantes :
   - Sous l'onglet **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'Assistant Exportation. Sur la page **Machines protégées** de l'Assistant Exportation, sélectionnez la machine protégée à exporter, puis cliquez sur **Suivant**.
   - Accédez à la machine à exporter, puis, dans l'onglet **Récapitulatif** dans le menu déroulant **Actions** de la machine, cliquez sur **Exporter** > **Disque de secours virtuel**.
2. Sur la page **Destination** de l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers la machine virtuelle**, sélectionnez VirtualBox, puis cliquez sur **Suivant**.
3. Sur la page **Options de la machine virtuelle**, sélectionnez **Utiliser une machine Windows.**
4. Entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

Option	Description
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer. REMARQUE : Il est recommandé d'utiliser un nom dérivé du nom de l'agent ou un nom qui correspond au nom de l'agent. Vous pouvez également créer un nom dérivé du type de l'hyperviseur, de l'adresse IP ou du nom DNS.
Chemin d'accès cible	Spécifiez un chemin cible local ou distant pour créer la machine virtuelle. REMARQUE : Le chemin d 'accès cible ne doit pas être un répertoire racine. Si vous spécifiez un chemin de partage réseau, vous devez entrer les informations d'identification valides (nom d'utilisateur et mot de passe) d'un compte enregistré dans la machine cible. Le compte doit avoir les autorisations en lecture et en écriture sur le partage réseau.
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Cliquez sur **Utiliser la même quantité de RAM que la machine source** pour spécifier que l'utilisation de RAM est identique pour la machine virtuelle et la machine source. • Cliquez sur **Utiliser une quantité spécifique de RAM** pour spécifier la quantité de RAM à utiliser. Par exemple, 4 096 Mo. La quantité minimale autorisée est de 512 Mo, et le maximum dépend de la capacité et des limites de la machine hôte.

5. Pour spécifier un compte d'utilisateur pour la machine virtuelle, sélectionnez **Spécifier le compte d'utilisateur sous lequel la machine virtuelle est exportée**, puis entrez les informations suivantes. Elles font référence à un compte d'utilisateur spécifique pour lequel la machine virtuelle sera enregistrée dans le cas où il existe plusieurs comptes utilisateur sur la machine virtuelle. Lorsque ce compte d'utilisateur est connecté, seul cet utilisateur voit la machine virtuelle dans le gestionnaire VirtualBox. Si aucun compte n'est spécifié, la machine virtuelle est enregistrée pour tous les utilisateurs existants sur la machine Windows avec VirtualBox.
   - **Nom d'utilisateur** : entrez le nom d'utilisateur pour lequel la machine virtuelle est enregistrée.
   - **Mot de passe** : entrez le mot de passe de ce compte d'utilisateur.
6. Sélectionnez **Effectuer une exportation ponctuelle initiale** pour effectuer l'exportation immédiatement au lieu d'attendre le prochain instantané planifié.

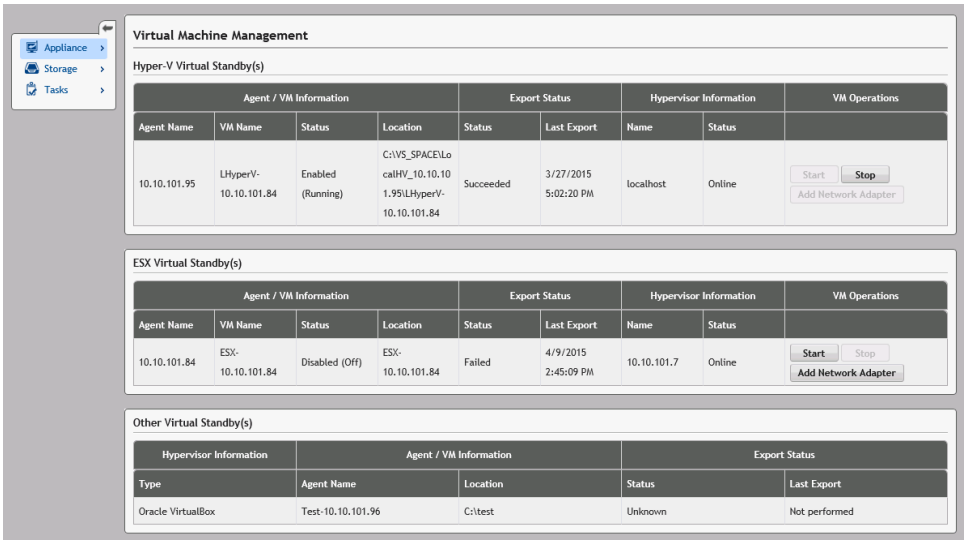
7. Sur la page Volumes, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une solution efficace de sauvegarde de l'ordinateur protégé, incluez la lettre du lecteur d'amorçage de la machine protégée. Exemple : C:\.
8. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

Gestion de machines virtuelles

L'onglet **Gestion des VM** affiche l'état des machines protégées. Vous pouvez démarrer, arrêter et ajouter des cartes réseau (applicable pour les machines virtuelles Hyper-V et ESXi uniquement). Pour accéder à l'onglet Gestion des machines virtuelles, cliquez sur **Appliance → Gestion des machines virtuelles**.

REMARQUE : Les boutons Démarrer, Arrêter et Ajouter une carte réseau peuvent prendre jusqu'à 30 secondes pour apparaître chaque fois que l'onglet **Appliance → Gestion des machines virtuelles** est sélectionné.



Gestion VM pour machines virtuelles de secours Hyper-V et ESXi

Champ	Description
Informations sur l'agent/la machine virtuelle	**Nom de l'agent** : indique le nom de la machine protégée pour laquelle vous avez créé le disque virtuel de secours. **Nom de VM** : indique le nom de la machine virtuelle. REMARQUE : Il est recommandé d'utiliser un nom dérivé du nom de l'agent ou un nom qui correspond au nom de l'agent. Vous pouvez également créer un nom dérivé du type de l'hyperviseur, de l'adresse IP ou du nom DNS. **État** : indique l'état de la machine virtuelle. Les valeurs possibles sont : • En cours d'exécution • Arrêté • Démarrage

Champ	Description
	• Suspended (Interrompu) • Arrêt • Inconnu (condition temporaire) REMARQUE : Les valeurs d'état ci-dessus dépendent du type d'hyperviseur. Certains hyperviseurs n'affichent pas toutes les valeurs de l'état. **Emplacement** : indique l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement e VM doit disposer de suffisamment d'espace pour contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
Condition de l'exportation	**Condition** 1. Indique l'état suivant d'un processus d'exportation : • Complete (Terminé) • En panne • En cours • Pas effectué 2. Si une exportation est actuellement en cours, le pourcentage d'exportation s'affiche. **Dernière Exportation** : indique l'heure de la dernière exportation.
Informations de l'hyperviseur	**Nom** : indique le nom de l'hyperviseur sur lequel la VM est créée. **Condition** : indique la condition de la connexion pour les hyperviseurs Hyper-V et ESXi. • En ligne • Hors ligne • Inconnu (condition temporaire) REMARQUE : La condition est affichée uniquement pour les hyperviseurs Hyper-V et ESXi.
Opérations sur les machines virtuelles	Permet de démarrer ou d'arrêter la machine virtuelle et d'ajouter une carte réseau.

Gestion des machines virtuelles pour les autres disques virtuels de secours

Champ	Description
Informations de l'hyperviseur	**Type** : indique le type de l'hyperviseur.
Informations sur l'agent/la machine virtuelle	**Nom de l'agent** : indique le nom de la machine protégée pour laquelle vous avez créé le disque virtuel de secours. **Emplacement** : indique l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement e VM doit disposer de suffisamment d'espace pour

Champ	Description
	contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
Condition de l'exportation	**Condition** 1. Indique l'état suivant d'un processus d'exportation : • Complete (Terminé) • En panne • En cours • Non exécuté 2. Si une exportation est actuellement en cours, le pourcentage d'exportation s'affiche sous la forme d'une barre d'avancement. **Dernière Exportation** : indique l'heure de la dernière exportation.

Création d'une carte réseau virtuelle

Les machines virtuelles doivent avoir une ou plusieurs cartes réseau virtuelles (VNA) pour se connecter à Internet. Une machine virtuelle doit posséder une carte réseau virtuelle pour chaque carte réseau réelle (RNA) sur l'ordinateur protégé. La VNA et la RNA correspondante doivent avoir une configuration similaire. Vous pouvez ajouter des VNA à votre machine virtuelle quand vous créez le disque virtuel de secours ou vous pouvez ajouter des VNA ultérieurement.

Lors de la création d'un disque virtuel de secours, il existe une suggestion de carte pour chaque carte dans l'ordinateur protégé, lors de la configuration d'une machine virtuelle. Vous pouvez ajouter ou supprimer tout ou partie de ces cartes suggérées. Le nombre maximal de VNA par machine virtuelle dépend du type d'hyperviseur. Pour Hyper-V vous pouvez ajouter jusqu'à 8 cartes pour chaque machine virtuelle.

Pour créer une carte de réseau virtuelle :

1. Accédez à la page **Gestion des VM** .
2. Cliquez sur le bouton **Ajouter une carte réseau** associé à la machine virtuelle afin d'ajouter une VNA.

   REMARQUE : N'ajoutez pas de cartes à une VM pour un disque virtuel de secours qui est toujours en train d'exécuter des sauvegardes ou des exportations de machines protégées. Les VNA supplémentaires peuvent entraîner l'échec des futures opérations d'exportation.

   REMARQUE : Nous vous conseillons d'ajouter les VNA juste avant de lancer la machine virtuelle en remplacement de la machine protégée. Assurez-vous d'arrêter ou de suspendre les exportations en attente pour la MV à l'aide de l'onglet de veille virtuelle.

   La fenêtre **Cartes réseau et commutateurs virtuels** apparaît.
3. Cliquez sur **Créer** pour créer une carte réseau virtuelle.
   La fenêtre **Créer une carte réseau virtuelle** s'affiche.
4. Choisissez un commutateur virtuel existant dans le menu déroulant.

   REMARQUE : Au cours de la sélection des commutateurs virtuels pour ESXi, la liste déroulante ne répertorie que les commutateurs dont le nom comprend « VM » ou « Machine virtuelle ». Ne sélectionnez qu'un commutateur de type **Groupe de ports de machines virtuelles**, vous pouvez vérifier le type du commutateur via l'interface utilisateur graphique de l'hyperviseur ESXi.
5. Cliquez sur **Créer**.

REMARQUE : Pour supprimer une carte réseau virtuelle, utilisez l'interface de gestion d'hyperviseur.

Lancement d'une opération de machine virtuelle

Pour démarrer une opération de machine virtuelle :

1. Accédez à la fenêtre **Gestion des machines virtuelles** .
2. Cliquez sur le bouton **Démarrer** associé à la machine virtuelle à démarrer.

REMARQUE : L'interface utilisateur graphique risque d'être en décalage, notamment, pour afficher le statut correct de la machine. Le bouton Démarrer peut rester désactivé jusqu'à 30 secondes après que les boutons ont été utilisés. Le bouton Démarrer est activé uniquement si la machine virtuelle peut être démarrée

REMARQUE : Ne cliquez pas sur le bouton Démarrer si une tâche d'exportation vers la machine virtuelle est en cours d'exécution ou devrait bientôt démarrer. Vérifiez la date planifiée de la prochaine tâche d'exportation en affichant l'onglet **Machines protégées** et l'onglet **Disque de secours virtuel**. Si une tâche d'exportation a été planifiée dans un futur proche, annulez ou ignorez la tâche d'exportation ou attendez que la tâche d'exportation se termine avant de démarrer la machine virtuelle. L'exportation de données échoue si elle est lancée lorsque la machine virtuelle est en cours d'exécution mais vous pouvez démarrer une machine virtuelle lorsqu'une tâche d'exportation est en cours d'exécution.

REMARQUE : Il est recommandé de ne pas démarrer la VM qui est gérée sous la forme d'un disque virtuel de secours. Les VM virtuelles de secours sont destinées à être des machines virtuelles actives ou démarrées en tant que remplacement d'une machine protégée en panne. Si la machine protégée est toujours active, vous devez d'abord arrêter ou suspendre toutes les exportations en cours pour la MV à l'aide de l'onglet Disque de secours virtuel avant de démarrer la machine virtuelle.

Arrêt d'une opération de machine virtuelle

Pour arrêter une opération de machine virtuelle :

1. Accédez à la fenêtre **Gestion des machines virtuelles** .
2. Cliquez sur le bouton **Arrêter** associé à la machine virtuelle à arrêter.

REMARQUE : Le bouton Arrêter est activé uniquement si la machine virtuelle est en cours d'exécution et disponible sous les 30 secondes d'une actualisation après le démarrage de la machine virtuelle.

REMARQUE : Le bouton Démarrer est activée dans les 30 secondes (approximativement) qui suivent l'arrêt de la machine virtuelle.

REMARQUE : Une fois le site protégé VM restauré, supprimez la VM de l'hyperviseur et son disque de secours virtuel correspondant. Recréez le disque virtuel de secours pour la machine protégée restaurée. Ceci permet de s'assurer que la machine virtuelle de secours est une image exacte de la machine protégée.

Exécution d'une restauration

Dans AppAssure, une restauration consiste à restaurer les volumes sur un ordinateur depuis des points de restauration.

REMARQUE : La fonctionnalité BMR est aussi prise en charge par les machines Linux protégées à l'aide de l'utilitaire de ligne de commande `aamount`. Pour en savoir plus, reportez-vous à Lancement d'une restauration BMR pour une machine Linux à l'aide de l'utilitaire de ligne de commande.

Pour effectuer une restauration (rollback) :

1. Dans la console Core, effectuez l'une des opérations suivantes :
   - Cliquez sur l'onglet **Machines**, puis procédez comme suit :

   a. Dans la liste des machines protégées, cochez la case en regard de la machine à exporter.
   b. Dans le menu déroulant **Actions** de cet ordinateur, cliquez sur **Restauration**.
   c. Dans la boîte de dialogue **Rollback — Sélectionner le point de restauration à exporter**, choisissez un point de restauration, puis cliquez sur **Suivant**.
      - Dans la zone de navigation de gauche de la console AppAssure Core, sélectionnez la machine à restaurer afin d'ouvrir l'onglet **Récapitulatif** de cette machine.
   d. Cliquez sur l'onglet **Points de restauration**, puis choisissez un point dans la liste.
   e. Développez les détails de ce point de restauration, puis cliquez sur **Restaurer (rollback)**.
2. Modifiez les options de restauration telles que décrites dans le tableau suivant.

Zone de texte	Description
Machine protégée	Spécifiez la machine d'agent d'origine comme destination de la restauration (rollback). La source est l'agent depuis lequel vous avez créé le point de restauration qui sert à la restauration (rollback).
Instance de console de restauration	Pour restaurer le point de restauration sur toutes les machines amorcées en mode URC, entrez le nom d'utilisateur et le mot de passe.

3. Cliquez sur **Charger les volumes**.
   La boîte de dialogue **Adressage des volumes** s'affiche.

   REMARQUE : La console Core n'adresse pas automatiquement les volumes Linux. Pour trouver un volume Linux, naviguez jusqu'au volume à restaurer (rollback).
4. Sélectionnez les volumes à restaurer (rollback).
5. Utilisez les options **Destination** pour choisir le volume de destination où restaurer (rollback) le volume sélectionné.
6. Sélectionnez l'une des options suivantes :
   - **Live Recovery** (Restauration dynamique). Lorsque vous sélectionnez cette option, la restauration (rollback) des volumes Windows est effectuée immédiatement. Option sélectionnée par défaut.

     REMARQUE : L'option **Live Recovery** n'est pas disponible pour les volumes Linux.
   - **Forcer le démontage**. Lorsque vous sélectionnez cette option, le programme force le démontage de tous les points de restauration montés, avant d'effectuer la restauration (rollback). Option sélectionnée par défaut.
7. Cliquez sur **Restaurer**.
   Le système commence à restaurer (rollback) les données telles qu'elles étaient lors du point de restauration sélectionné.

Exécution d'une restauration (rollback) pour une machine Linux avec la ligne de commande

Une restauration consiste à restaurer les volumes qui figurent sur une machine à partir de points de restauration. Dans AppAssure, vous pouvez effectuer une restauration de volumes sur vos machines Linux protégées à l'aide de l'utilitaire de ligne de commande `aamount`.

PRÉCAUTION : Ne tentez pas d'effectuer une restauration sur le volume système ou root (/).

REMARQUE : La fonctionnalité de restauration est prise en charge pour vos machines Windows protégées au sein de Core Console. Pour en savoir plus, voir Exécuter une restauration (rollback).

Pour restaurer un volume sur une machine Linux :

1. Exécutez l'utilitaire `aamount` d'AppAssure comme root, par exemple :

   ```
   sudo aamount
   ```

2. En réponse à l'invite de montage d'AppAssure, 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 AppAssure Core.
4. Entrez les références de connexion, c'est-à-dire le nom d'utilisateur et le mot de passe de ce serveur.

   La liste qui s'affiche indique les machines protégées par ce serveur AppAssure. Elle répertorie les machines d'agent trouvées en affichant le numéro d'article, l'adresse IP/nom d'hôte et l'ID de machine (par exemple : `293cc667-44b4-48ab-91d8-44bc74252a4f`).
5. Pour répertorier les points de restauration actuellement montés sur la machine spécifiée, entrez la commande suivante :

   ```
   lr <machine_line_item_number>
   ```

   REMARQUE : Vous pouvez également entrer dans cette commande le numéro d'ID de la machine au lieu du numéro d'article figurant sur une ligne.

   La liste qui s'affiche indique les points de restauration de base et incrémentiels de cette machine. Cette liste inclut un numéro d'article figurant sur une ligne, l'horodatage/date, l'emplacement du volume, la taille de point de restauration et un numéro d'ID de volume comprenant en dernier lieu un numéro de séquence (par exemple, `"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`), qui identifie le point de restauration.
6. Pour sélectionner le point de restauration à restaurer (rollback), entrez la commande suivante :

   ```
   r [volume_recovery_point_ID_number] [path]
   ```

   Cette commande entraîne la restauration (rollback) de l'image de volume spécifiée par l'ID entré, du core vers le chemin d'accès spécifié. Le chemin de restauration (rollback) est celui du descripteur de fichier de périphérique et non celui du répertoire dans lequel il est monté.

REMARQUE : Pour identifier le point de restauration, vous pouvez également indiquer un numéro de ligne dans la commande au lieu de l'ID du point de restauration. Dans ce cas, utilisez le numéro de ligne de l'agent/la machine (figure dans la sortie `lm`), suivi du numéro de ligne du point de restauration et de la lettre de volume, puis du chemin d'accès. Par exemple, **r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]**. Dans cette commande, [chemin] est le descripteur de fichier du volume réel.

Par exemple, si la sortie `lm` répertorie trois machines d'agent, que vous entrez la commande `lr` pour Numéro 2 et que vous souhaitez restaurer (rollback) le point de restauration 23 du volume b vers le volume monté dans le répertoire `/mnt/data`, la commande est la suivante : `r2 23 b /mnt/data`.

REMARQUE : Il est possible d'effectuer une restauration vers /, mais uniquement lors d'une restauration BMR au cours d'un amorçage avec un CD Live. Pour plus d'informations, reportez-vous à la section Exécution d'une restauration BMR pour une machine Linux.

7. Lorsque vous êtes invité à continuer, entrez `y` pour Yes (o pour Oui).

   Une série de messages s'affiche au cours de la restauration pour vous informer de l'état.

8. Lorsque la restauration (rollback) réussit, l'utilitaire `aamount` monte automatiquement le module de noyau et le réattache au volume restauré (rollback) si la cible a été préalablement protégée et montée. Sinon, montez le volume restauré (rollback) sur le disque local et vérifiez que les fichiers ont été restaurés.

   Par exemple, vous pouvez utiliser la commande `sudo mount` puis la commande `ls`.

   PRÉCAUTION : Ne démontez pas manuellement un volume Linux protégé. Si vous devez le faire, veillez à exécuter la commande suivante avant de démonter le volume : `bsctl -d [path to volume]`.

   Dans cette commande, [chemin d'accès au volume] ne désigne pas le point de montage du volume mais le descripteur de fichier du volume ; il doit se présenter sous une forme similaire à la suivante : `/dev/sda1`.

À propos de la restauration complète pour les machines Windows

Lorsqu'ils fonctionnent correctement, les serveurs exécutent et effectuent les tâches pour lesquelles ils sont configurés. Lorsqu'un événement grave se produit et désactive le fonctionnement du serveur, vous devez immédiatement prendre des mesures pour restaurer le serveur à sa condition de fonctionnement précédente. En général, ce processus consiste à reformater l'ordinateur, réinstaller le système d'exploitation, restaurer les données au moyen de sauvegardes et réinstaller les applications logicielles.

AppAssure permet d'effectuer une restauration complète (BMR) pour les machines Windows que le matériel soit similaire ou non. Ce processus consiste à créer une image de CD d'amorçage, graver l'image sur un disque, amorcer le serveur cible à partir du disque, se connecter à l'instance de console de restauration, adresser les volumes, initialiser la restauration, puis surveiller le processus. À la fin de la restauration, vous pouvez poursuivre en exécutant la tâche de chargement du système d'exploitation et des applications logicielles sur le serveur restauré, puis vos paramètres et votre configuration uniques.

Vous pouvez aussi choisir d'effectuer une restauration sans système d'exploitation dans le cadre d'une mise à niveau matérielle ou d'un remplacement de serveur.

La fonctionnalité BMR est aussi prise en charge par les machines Linux protégées à l'aide de l'utilitaire de ligne de commande `aamount`. Pour en savoir plus, reportez-vous à Lancement d'une restauration complète (BMR) pour une machine Linux.

Conditions requises pour l'exécution d'une restauration BMR d'un ordinateur Windows

Avant de démarrer une restauration sans système d'exploitation d'un ordinateur Windows, vous devez vous assurer que les conditions et critères suivants existent :

- Sauvegardes du serveur et du Core en fonctionnement
- Le matériel à restaurer (nouveau ou ancien, similaire ou non)
- CD vierge et logiciel de gravure CD
- VNC viewer (facultatif)
- Stockage de lecteurs compatibles avec Windows 7 PE (32 bits) et lecteurs de cartes réseau pour l'ordinateur cible
- Pilotes de contrôleur de stockage, RAID, AHCI et jeux de puces pour le système d'exploitation cible

REMARQUE : Les pilotes de contrôleur de stockage ne sont nécessaires que si la restauration est effectuée vers un matériel dissemblable.

Stratégie d'exécution d'une restauration complète (BMR) d'une machine Windows

pour effectuer une BMR d'un ordinateur Windows :

1. créez un CD d'amorçage. Reportez-vous à Création d'un CD d'image ISO amorçable.
2. gravez l'image sur le disque.
3. démarrez le serveur cible depuis le CD d'amorçage. Voir Chargement d'un CD d'amorçage.
4. connectez-vous au disque de restauration.
5. adressez les volumes. Voir Adressage de volumes.
6. initiez la restauration. Voir Lancement d'une restauration à partir de l'AppAssure Core.
7. surveillez l'avancement. Voir Affichage de l'avancement de la restauration.

Création d'un CD d'image ISO amorçable

Pour exécuter une restauration BMR d'une machine Windows, vous devez créer une image CD/ISO amorçable dans Core Console, qui contient l'interface AppAssure Universal Recovery Console. Cette console est un environnement qui permet de restaurer le lecteur système ou l'ensemble du serveur directement depuis AppAssure Core.

L'image ISO que vous créez est adaptée à la machine que vous restaurez ; par conséquent, elle doit contenir les pilotes de réseau et de stockage de masse corrects. Si vous prévoyez d'effectuer la restauration sur un matériel différent de celui de la machine où vous créez le CD d'amorçage, vous devez inclure le contrôleur de stockage et d'autres pilotes sur le CD d'amorçage.

REMARQUE : L'ISO (International Organization for Standardization) est un organisme international réunissant des représentants de différentes organisations nationales, qui détermine et définit les normes des systèmes de fichiers. La norme ISO 9660 est une norme de système de fichiers utilisée pour les supports de disque optique pour l'échange de données. Elle prend en charge divers systèmes d'exploitation, notamment Windows. Une image ISO est un fichier d'archive ou une image de disque qui contient des données pour chaque secteur du disque, ainsi que pour le système de fichiers du disque.

Pour créer une image ISO de CD amorçable :

1. Dans Core Console où se trouve le serveur à restaurer, sélectionnez le **Core**, puis cliquez sur l'onglet **Outils**.
2. Cliquez sur **CD d'amorçage**.
3. Sélectionnez **Actions**, puis cliquez sur **Créer une image ISO d'amorçage**.

   La boîte de dialogue **Créer un CD d'amorçage** s'affiche. Pour remplir les champs de cette boîte de dialogue, appliquez les procédures suivantes.

Attribution d'un nom au fichier de CD d'amorçage et définition du chemin

Pour nommer le CD d'amorçage et configurer le chemin :

Dans la boîte de dialogue **Créer un CD d'amorçage**, entrez le chemin ISO où l'image d'amorçage sera stockée sur le serveur core.

Si le partage sur lequel vous souhaitez stocker l'image manque de l'espace de disque, vous pouvez définir le chemin au besoin ; par exemple, D:\nomdufichier.iso.

REMARQUE : L'extension de fichier doit être .iso. 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 ne sont pas sensibles à la casse. N'utilisez aucun espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

Création de connexions

Pour créer des connexions :

1. Sous **Options de connexion**, effectuez l'une des opérations suivantes :
   - Pour obtenir dynamiquement l'adresse IP avec le protocole DHCP (Dynamic Host Configuration Protocol, protocole de configuration dynamique de l'hôte), sélectionnez **Obtenir automatiquement l'adresse IP**.
   - (Facultatif) Pour spécifier une adresse IP statique pour la console de restauration, sélectionnez **Utiliser l'adresse IP suivante**, puis entrez l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS dans les champs prévus à cet effet. Vous devez remplir tous ces champs.
2. Si nécessaire, sous **Options UltraVNC**, sélectionnez **Ajouter UltraVNC** et entrez les options appropriées. Les paramètres UltraVNC vous permettent de gérer la console de restauration à distance lorsqu'elle est en cours d'exécution.

   REMARQUE : Cette étape est facultative. Si vous avez besoin d'un accès à distance à la console de restauration, vous devez configurer et utiliser UltraVNC. Vous ne pouvez pas vous connecter à l'aide des services de terminal Microsoft lorsque vous utilisez le CD d'amorçage.

Insertion de pilotes dans le CD d'amorçage

L'insertion de pilotes est utilisée pour faciliter les opérations entre la console de restauration, la carte réseau et le stockage sur le serveur cible.

Si vous prévoyez de restaurer les données sur un matériel différent, vous devez injecter les pilotes de contrôleur de stockage, de RAID, d'AHCI, de jeu de puces et autres dans le CD d'amorçage. Ces pilotes permettent au système d'exploitation de détecter et de faire fonctionner les périphériques avec succès.

REMARQUE : N'oubliez pas que le CD d'amorçage contient automatiquement les pilotes Windows 7 PE 32 bits.

Pour insérer des pilotes dans un CD d'amorçage

1. Téléchargez les pilotes pour le serveur depuis le site Web du fabricant, puis décompressez-les.
2. Compressez le dossier qui contient les pilotes, à l'aide d'un utilitaire de compression tel que WinZip.
3. Dans la boîte de dialogue **Créer un CD d'amorçage**, accédez au panneau **Pilotes** et cliquez sur **Ajouter un pilote**.
4. Pour trouver le fichier de pilote compressé, naviguez dans le système de fichiers. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

   Les pilotes insérés apparaissent en surbrillance dans le volet **Pilotes**.

Création du CD d'amorçage

Pour créer un CD d'amorçage, vous devez, après avoir nommé le CD d'amorçage et spécifié le chemin, créé une connexion et (facultatif) injecté les pilotes, ouvrir l'écran **Créer un CD d'amorçage** et cliquer sur **Créer un CD d'amorçage**. L'image ISO est créée.

Affichage de l'avancement de la création de l'image ISO

Pour afficher l'avancement de la création de l'image ISO, sélectionnez l'onglet **Événements**, puis **Tâches**.

REMARQUE : Vous pouvez également afficher l'avancement de la création de l'image ISO image dans la boîte de dialogue **Surveiller la tâche active**.

Lorsque la création de l'image ISO est terminée, cette image apparaît dans la page **CD d'amorçage**, accessible depuis le menu **Outils**.

Accès à l'image ISO

Pour accéder à l'image ISO, naviguez jusqu'au chemin de sortie que vous avez indiqué ou cliquez sur le lien pour télécharger l'image à un emplacement à partir duquel vous pourrez la charger sur le nouveau système, par exemple, un lecteur de réseau.

Chargement d'un CD d'amorçage

Après avoir créé l'image du CD d'amorçage, amorcez le serveur cible avec le CD d'amorçage nouvellement créé.

REMARQUE : Si vous avez créé le CD d'amorçage avec DHCP, notez l'adresse IP et le mot de passe.

Pour charger un CD d'amorçage :

1. Naviguez jusqu'au nouveau serveur, chargez le CD d'amorçage, puis démarrez la machine.
2. Activez l'option **Amorcer à partir du CD-ROM**, qui charge les éléments suivants :
   - Windows 7 PE
   - Logiciel AppAssure Agent

   La console AppAssure Universal Recovery démarre, et affiche l'adresse IP et le mot de passe d'authentification de la machine.

3. Prenez note de l'adresse IP qui s'affiche dans le panneau des paramètres d'adaptateur réseau, ainsi que du mot de passe d'authentification affiché dans le panneau Authentification. Vous utiliserez ces informations ultérieurement au cours du processus de restauration des données, pour vous reconnecter à la console.
4. Pour 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, la console Universal Recovery l'utilise et l'affiche dans l'écran **Paramètres d'adaptateur réseau**.

Injection de pilotes sur votre serveur cible

Si vous restaurez les données sur un matériel différent, vous devez injecter les pilotes de contrôleur de stockage, de RAID, d'AHCI, de jeu de puces et autres dans le CD d'amorçage s'ils n'y figurent pas. Ces pilotes permettent au système d'exploitation de faire fonctionner avec succès tous les périphériques du serveur cible.

Si vous n'êtes pas certain des pilotes dont votre serveur cible a besoin, cliquez sur l'onglet Infos système dans la console Universal Recovery. Cet onglet affiche tout le matériel système et tous les types de périphérique du serveur cible sur lequel vous souhaitez restaurer les données.

REMARQUE : N'oubliez pas que votre serveur cible contient automatiquement les pilotes Windows 7 PE 32 bits.

Pour injecter des pilotes dans votre serveur cible :

1. Téléchargez les pilotes pour le serveur depuis le site Web du fabricant, puis décompressez-les.
2. Compressez le dossier qui contient les pilotes, à l'aide d'un utilitaire de compression tel que WinZip, puis copiez-le vers le serveur cible.
3. Dans la console Universal Recovery, cliquez sur **Injection de pilotes**.
4. Pour trouver le fichier de pilote compressé, naviguez dans le système de fichiers et sélectionnez le fichier.
5. Si vous avez cliqué sur **Injection de pilotes** à l'étape 3, cliquez sur **Ajouter un pilote**. Si vous avez choisi **Charger un pilote** à l'étape 3, cliquez sur **Ouvrir**.

   Les pilotes sélectionnés sont injectés ; ils sont chargés dans le système d'exploitation lorsque vous redémarrez le serveur cible.

Lancement d'une restauration à partir d'AppAssure Core

Pour lancer une restauration à partir d'AppAssure Core

1. Si les cartes réseau qui figurent sur tout système en cours de restauration sont associées (liées), retirez tous les câbles, à l'exception d'un d'entre eux.

   REMARQUE : AppAssure Restore ne reconnaît pas les cartes réseau associées. En présence de plus d'une connexion, le processus ne peut pas savoir quel carte réseau utiliser.
2. Accédez au serveur Core, puis ouvrez Core Console.
3. Dans l'onglet **Machines**, sélectionnez l'ordinateur à partir duquel vous souhaitez restaurer les données.
4. Cliquez sur le menu **Actions** de l'ordinateur, puis sélectionnez **Points de restauration** pour afficher la liste de tous les points de restauration de cet ordinateur.
5. Développez le point de restauration à partir duquel vous souhaitez effectuer la restauration, puis cliquez sur **Restaurer**.
6. Dans la boîte de dialogue **Restaurer**, sous Choisir une **destination**, sélectionnez **Instance Recovery Console**.

7. Dans les champs **Hôte** et **Mot de passe**, entrez l'adresse IP et le mot de passe d'authentification du nouveau serveur sur lequel vous restaurerez les données.

   REMARQUE : Les valeurs Hôte et Mot de passe sont les références que vous avez enregistrées au cours de la tâche précédente. Pour en savoir plus, voir .

8. Cliquez sur **Charger les volumes** pour charger les volumes cibles sur le nouvel ordinateur.

Mappage/adressage de volumes

Vous pouvez choisir d'adresser des volumes sur les disques du serveur cible automatiquement ou manuellement. Pour l'alignement automatique des disques, le disque est nettoyé et repartitionné, et toutes les données sont supprimées. L'alignement est réalisé dans l'ordre où les volumes sont répertoriés, puis les volumes sont alloués aux disques de manière appropriée, en fonction de la taille, etc. Plusieurs volumes peuvent utiliser un même disque. Si vous adressez manuellement les lecteurs, vous ne pouvez pas utiliser deux fois le même disque.

Pour l'adressage manuel, vous devez avoir au préalable formaté correctement la machine, avant de la restaurer. Pour plus d'informations, reportez-vous à la section Lancement d'une restauration à partir de l'AppAssure Core.

Pour adresser les volumes :

1. Pour adresser automatiquement des volumes, procédez comme suit :
   a. Dans la boîte de dialogue **RollbackURC**, sélectionnez l'onglet **Adresser automatiquement les volumes**.
   b. Dans la zone **Adressage des disques**, sous **Volume source**, vérifiez que le volume source est sélectionné, et que les volumes appropriés sont à la fois répertoriés sous cette entrée et sélectionnés.
   c. Si le disque de destination adressé automatiquement est le volume cible correct, sélectionnez **Disque de destination**.
   d. Cliquez sur **Cumul (rollback)**, puis passez à l'étape 3.
2. Pour adresser manuellement des volumes, procédez comme suit :
   a. Dans la boîte de dialogue **RollbackURC**, sélectionnez l'onglet **Adresser manuellement les volumes**.
   b. Dans la zone **Adressage des volumes**, sous **Volume source**, vérifiez que le volume source est sélectionné, et que les volumes appropriés sont à la fois répertoriés sous cette entrée et sélectionnés.
   c. Sous **Destination**, dans le menu déroulant, sélectionnez la destination appropriée, à savoir le volume cible où effectuer la restauration sans système d'exploitation (BMR) du point de restauration sélectionné, puis cliquez sur **Cumul (rollback)**.
3. Dans la boîte de dialogue de confirmation **RollbackURC**, vérifiez l'adressage de la source du point de restauration et du volume de destination du cumul (rollback). Pour effectuer le cumul, cliquez sur **Démarrer le cumul (rollback)**.

   AVERTISSEMENT : Si vous sélectionnez Démarrer le cumul (rollback), 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.

Affichage de l'avancement de la restauration

Pour afficher l'avancement de la restauration :

1. Une fois que vous avez lancé le processus de restauration (rollback), la boîte de dialogue **Tâche active** s'affiche et montre que l'action de restauration (rollback) a été démarrée.

   REMARQUE : Cet affichage de la boîte de dialogue **Tâche active** n'indique pas que la tâche s'est achevée avec succès.

2. (Facultatif) Pour surveiller l'avancement de la tâche de restauration (rollback), ouvrez la boîte de dialogue Tâche active et cliquez sur **Ouvrir la fenêtre de surveillance**. Vous pouvez affiche l'état de la restauration, ainsi que l'heure de début et de fin, dans la fenêtre **Surveiller la tâche ouverte**.

   REMARQUE : Pour revenir aux points de restauration correspondant à la machine source depuis la boîte dialogue **Tâche active**, cliquez sur **Fermer**.

Démarrage du serveur cible restauré

Pour démarrer le serveur cible restauré :

1. Naviguez pour revenir au serveur cible, puis, dans l'interface de la **console AppAssure Universal Recovery**, cliquez sur **Redémarrer** pour démarrer la machine.
2. Spécifiez que Windows doit démarrer normalement.
3. Connectez-vous à la machine.

   Le système est restauré à son état tel qu'il était avant la restauration sans système d'exploitation.

Réparation des problèmes de démarrage

Notez que si vous avez restauré les données sur un matériel différent, vous devez avoir injecté les pilotes de contrôleur de stockage, RAID, AHCI, de jeu de puces et d'autres pilotes s'ils n'y figurent pas sur le CD d'amorçage. Ces pilotes permettent au système d'exploitation de faire fonctionner tous les périphériques du serveur cible.

Pour réparer les problèmes de démarrage :

1. Si vous rencontrez des difficultés lors du démarrage du serveur cible restauré, ouvrez la console Universal Recovery en rechargeant le CD d'amorçage.
2. Dans la console Universal Recovery, cliquez sur **Injection de pilotes**.
3. Dans la boîte de dialogue Injection de pilotes, cliquez sur **Reparer les problèmes d'amorçage**.

   Les paramètres de démarrage figurant dans l'enregistrement de serveur cible sont automatiquement réparés.
4. Dans la console Universal Recovery, cliquez sur **Redémarrer**.

Exécution d'une restauration complète pour une machine Linux

Vous pouvez exécuter une restauration BMR pour une machine Linux, y compris la restauration du volume système. À l'aide de l'utilitaire de ligne de commande AppAssure, `aamount`, effectuez la restauration de l'image de base du volume d'amorçage. Avant toute restauration BMR, vous devez effectuer les opérations suivantes :

- Obtenir un fichier Live CD BMR auprès du service de support AppAssure ; ce fichier inclut une version amorçable de Linux.

  REMARQUE : Vous pouvez également télécharger le fichier Live CD Linux depuis le portail de licences, à l'adresse **https://licenseportal.com**.
- Assurez-vous que l'espace sur le disque dur est suffisant pour créer les partitions de destination sur la machine cible et pour y stocker les volumes source. Chaque partition de destination doit être au moins aussi volumineuse que la partition source d'origine.

- Identifiez le chemin de restauration (rollback), c'est-à-dire le chemin du descripteur de fichier du périphérique. Pour identifier ce chemin, utilisez la commande `fdisk` à partir d'une fenêtre de terminal.

  REMARQUE : Avant de commencer à utiliser les commandes AppAssure, vous pouvez installer cet utilitaire d'écran. Il vous permet de faire défiler l'écran pour afficher de plus grandes quantités de données, comme la liste des points de restauration. Pour plus d'informations sur l'installation de l'utilitaire d'écran, voir Installation de l'utilitaire d'écran.

Pour effectuer la restauration sans système d'exploitation d'une machine Linux :

1. À l'aide du fichier Live CD que vous avez reçu d'AppAssure, démarrez la machine Linux et ouvrez une fenêtre de terminal.
2. Si nécessaire, créez une nouvelle partition de disque, par exemple en exécutant la commande `fdisk` en tant qu'utilisateur root, puis rendez cette partition amorçable en utilisant la commande `a`.
3. Exécutez l'utilitaire `aamount` d'AppAssure comme root, par exemple :

   ```
   sudo aamount
   ```
4. En réponse à l'invite de montage d'AppAssure, 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 AppAssure Core.
6. Entrez les références de connexion, c'est-à-dire le nom d'utilisateur et le mot de passe de ce serveur.

   La liste qui s'affiche indique les machines protégées par ce serveur AppAssure Core. Elle répertorie les machines trouvées en affichant le numéro d'article, l'adresse IP/nom d'hôte et l'ID de machine (par exemple : `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Pour répertorier les points de restauration récemment montés pour la machine à restaurer, entrez la commande suivante :

   ```
   lr <machine_line_item_number>
   ```

   REMARQUE : Vous pouvez également entrer dans cette commande le numéro d'ID de la machine au lieu du numéro d'article figurant sur une ligne.

   La liste qui s'affiche indique les points de restauration de base et incrémentiels de cette machine. Cette liste inclut un numéro d'article figurant sur une ligne, l'horodatage/date, l'emplacement du volume, la taille de point de restauration et un numéro d'ID de volume comprenant en dernier lieu un numéro de séquence (par exemple, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), qui identifie le point de restauration.
8. Pour sélectionner le point de restauration d'image de base à restaurer (rollback), entrez la commande suivante :

   ```
   r <volume_base_image_recovery_point_ID_number> <path>
   ```

   PRÉCAUTION : Vous devez vous assurer que le volume système n'est pas monté.

   Cette commande entraîne la restauration (rollback) de l'image de volume spécifiée par l'ID entré, du core vers le chemin d'accès spécifié. Le chemin de restauration (rollback) est celui du descripteur de fichier de périphérique et non celui du répertoire dans lequel il est monté.

REMARQUE : Pour identifier le point de restauration, vous pouvez également indiquer un numéro de ligne dans la commande au lieu du numéro d'ID du point de restauration. Dans ce cas, utilisez le numéro de ligne de l'agent/la machine (à partir de la sortie lm), suivi du numéro de ligne du point de restauration et de la lettre du volume, puis du chemin d'accès, par exemple,**r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. Dans cette commande, **<path>** est le descripteur de fichier du volume réel.

9. Lorsque vous êtes invité à continuer, entrez `y` pour Yes (o pour Oui).

   Une série de messages s'affiche au cours de la restauration pour vous informer de l'état.

10. Une fois la restauration réussie, le cas échéant, mettez à jour l'enregistrement d'amorçage principal à l'aide du chargeur de démarrage.

    REMARQUE : Il n'est nécessaire de réparer ou configurer le chargeur de démarrage que si ce disque est nouveau. S'il s'agit d'une simple restauration vers le même disque, il n'est pas nécessaire de configurer le chargeur de démarrage.

    PRÉCAUTION : Ne démontez pas manuellement un volume Linux protégé. Si vous devez le faire, veillez à exécuter la commande suivante avant de démonter le volume : bsctl -d <path to volume>.

    Dans cette commande, `<path to volume>` (chemin d'accès au volume) ne désigne pas le point de montage du volume mais le descripteur de fichier du volume ; il doit se présenter sous une forme similaire à la suivante : **/dev/sda1**.

Installation de l'utilitaire d'écran

Avant de commencer à utiliser les commandes AppAssure, vous pouvez installer l'utilitaire d'écran. Il vous permet de faire défiler l'écran pour afficher de plus grandes quantités de données, comme la liste des points de restauration.

Pour installer l'utilitaire d'écran :

1. Utilisez le fichier Live CD pour démarrer la machine Linux.

   Une fenêtre de terminal s'ouvre.

2. Entrez la commande suivante : `sudo apt-get install screen`
3. Pour démarrer l'utilitaire d'écran, entrez `screen` à l'invite de commande.

Création de partitions amorçables sur une machine Linux

Pour créer des partitions amorçables sur une machine Linux à l'aide de la ligne de commande :

1. Rattachez tous les périphériques à l'aide de l'utilitaire **bsctl** en exécutant la commande suivante en tant qu'utilisateur root : `sudo bsctl --attach-to-device /dev/<restored volume>`

   REMARQUE : Répétez cette étape pour chaque volume restauré.

2. Montez chaque volume restauré à l'aide des commandes suivantes :

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   REMARQUE : Certaines configurations système peuvent inclure le répertoire d'amorçage comme élément du volume racine.

3. Montez les métadonnées d'instantané de chaque volume restauré à l'aide des commandes suivantes :

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>

sudo bsctl --map-bitmap-store /dev/<restored volume>
```

4. Vérifiez que l'UUID (Universally Unique Identifier, ID universel unique) contient bien les nouveaux volumes, à l'aide de la commande `blkid` ou de la commande `ll /dev/disk/by-uuid`.
5. Vérifiez que le dossier `/etc/fstab` contient les UUID corrects pour le volume racine et le volume d'amorçage.
6. Installez GRUB (Grand Unified Bootloader, grand chargeur d'amorçage unifié) à l'aide des commandes suivantes :

```
mount --bind /dev/ /mnt/dev

mount --bind /proc/ /mnt/proc

chroot/mnt/bin/bash

grub-install/dev/sda
```

7. Vérifiez que le fichier **/boot/grub/grub.conf** contient l'UUID correct pour le volume racine ou mettez-le à niveau selon vos besoins à l'aide d'un éditeur de texte.
8. Retirez le disque Live CD du lecteur de CD-ROM et redémarrez la machine Linux.

Affichage d'événements et d'alertes

Pour afficher des événements et des alertes

1. Effectuez l'une des opérations suivantes :
   - Dans l'onglet Machines de Core Console, cliquez sur le lien hypertexte de l'ordinateur dont vous souhaitez afficher les événements.
   - Dans la zone **Navigation** à gauche de Core Console, sélectionnez l'ordinateur dont vous souhaitez afficher les événements.
2. Cliquez sur l'onglet **Événements**.

   Le journal de tous les événements des tâches et alertes actuelles s'affiche.

5

Protection des clusters de serveurs

À propos de la protection de clusters de serveurs

Dans AppAssure, la protection de clusters de serveurs est associée aux agents AppAssure installés sur des nœuds de clusters individuels (c'est-à-dire des ordinateurs individuels dans le cluster) et Core (qui protège ces agents), tout comme s'il s'agissait d'un seul ordinateur composite.

Vous pouvez facilement configurer un Core afin de protéger et de gérer un cluster. Dans Core Console, un cluster est organisé en tant qu'entité séparée, qui agit comme « conteneur » pour inclure des nœuds apparentés. Par exemple, dans la zone de navigation de gauche, le Core figure en haut de l'arborescence de navigation ; les clusters figurent sous le Core et contiennent les divers nœuds associés (où les agents AppAssure sont installés).

Aux niveaux Core et cluster, vous pouvez afficher les informations sur le cluster, telles que la liste de nœuds connexes et volumes partagés. Un cluster s'affiche dans la console Core dans l'onglet Machines, et vous pouvez activer ou désactiver la vue (à l'aide des options Afficher/Cacher) pour afficher les nœuds compris dans le cluster. Au niveau cluster, vous pouvez également afficher les métadonnées de cluster Exchange et SQL des nœuds du cluster. Vous pouvez spécifier des paramètres pour le cluster et les volumes partagés de celui-ci, ou vous pouvez naviguer vers un nœud individuel (machine) dans le cluster pour configurer les paramètres de ce nœud et les volumes locaux associés.

Applications et types de clusters pris en charge

Pour que votre cluster soit bien protégé, le logiciel AppAssure Agent doit être installé sur chaque machine ou nœud dans le cluster. AppAssure prend en charge les versions d'applications et configurations de cluster énumérées dans le tableau suivant.

Tableau 4. Applications et types de clusters pris en charge

Application	Version d'application et configuration de cluster associé	Cluster de basculement Windows
Microsoft Exchange	2007 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2007 Cluster Continuous Replication (CCR)	
	2010 Database Availability Group (DAG)	2008, 2008 R2
Microsoft SQL	2005, 2008, 2008 R2 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2012 Single Copy Cluster (SCC)	2008, 2008 R2, 2012

Les types de disques pris en charge incluent :

- Disques de tableau de partition GUID (GPT) supérieurs à 2 To

- Disques dynamiques
- Disques de base

Les types de montage pris en charge incluent :

- Les pilotes partagés connectés en tant que lettres de lecteur (par exemple : D:)
- Les volumes dynamiques simples sur un seul disque physique (volumes non divisés en bandes, non mis en miroir et non fractionnés)
- Les lecteurs partagés qui sont connectés en tant que points de montage

Protection d'un cluster

Cette rubrique décrit comment ajouter un cluster pour la protection dans AppAssure. Lorsque vous ajoutez un cluster pour la protection, vous devez spécifier le nom d'hôte ou l'adresse IP du cluster, l'application du cluster ou un des nœuds ou machines de cluster qui contient l'agent AppAssure.

REMARQUE : Un référentiel est utilisé pour stocker les instantanés de données capturées depuis vos nœuds protégés. Avant de commencer à protéger les données de votre cluster, installez au moins un référentiel associé à votre AppAssure Core.

Pour en savoir plus sur la configuration des référentiels, voir À propos des référentiels.

Pour protéger un cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, naviguez jusqu'à l'onglet **Accueil**, puis cliquez sur le bouton **Protéger le cluster**.
   - Dans la Core Console, à l'onglet **Machines**, cliquez sur **Actions**, puis cliquez sur **Protéger le cluster**.
2. Dans la boîte de dialogue **Se connecter au cluster**, entrez les informations suivantes :

Zone de texte	Description
Hôte	Le nom d'hôte et l'adresse IP du cluster, l'application de cluster ou l'un des nœuds de cluster que vous souhaitez protéger. REMARQUE : Si vous utilisez l'adresse IP de l'un des nœuds, un agent AppAssure doit être installé sur celui-ci et doit être démarré.
Port	Le Numéro du port sur la machine sur laquelle l'AppAssure Core communique avec l'agent.
Nom d'utilisateur	Le nom d'utilisateur de l'administrateur du domaine utilisé pour se connecter à cette machine, par exemple, **nom_de_domaine\administrateur** ou **administrateur@nom_de_domaine.com** REMARQUE : Le nom du domaine est obligatoire. Vous ne pouvez pas vous connecter au cluster en utilisant le nom d'utilisateur administrateur local.
Mot de passe	Le mot de passe utilisé pour vous connecter à cet ordinateur

3. Dans la boîte de dialogue **Protéger le cluster**, sélectionnez un référentiel pour ce cluster.
4. Pour protéger le cluster sur la base des paramètres par défaut, sélectionnez les nœuds auxquels appliquer la protection par défaut, puis cliquez sur **Protéger**.

REMARQUE : Les paramètres par défaut assurent que tous les volumes sont protégés avec un horaire par défaut de toutes les 60 minutes.

5. Pour entrer les paramètres personnalisés du cluster (par exemple, pour personnaliser l'horaire de protection des volumes protégés), effectuez les tâches suivantes :
   a. Cliquez sur **Paramètres**.
   b. Dans la boîte de dialogue **Volumes**, sélectionnez le(s) volume(s) à protéger, puis cliquez sur **Modifier**.
   c. Dans la boîte de dialogue **Horaire de protection**, sélectionnez l'une des options d'horaire suivantes pour la protection de vos données tel que décrit dans le tableau suivant.

Zone de texte	Description
Fréquence	Choisissez parmi les options suivantes : • **Jour de la semaine** : pour protéger les données à intervalle donné, sélectionnez **Intervalle**, puis : – Pour personnaliser l'horaire de protection des données pendant les heures de forte utilisation, vous pouvez indiquer une heure de début, une heure de fin et un intervalle. – Pour protéger les données pendant les heures de faible utilisation, cochez la case **Protéger pendant les heures de faible utilisation**, puis sélectionnez un intervalle de protection. • **Week-ends** : pour protéger les données pendant le week-end également, cochez la case **Protéger pendant les week-ends**, puis sélectionnez un intervalle.
Tous les jours	Pour protéger les données quotidiennement, sélectionnez l'option **Quotidiennement**, puis, pour **Heure de protection**, sélectionnez une heure de début de protection des données.
Aucune protection	Pour ne plus protéger ce volume, sélectionnez l'option **Aucune protection**.

6. Lorsque vous avez effectué toutes les modifications nécessaires, cliquez sur **Enregistrer**.
7. Pour entrer des paramètres personnalisés pour un nœud du cluster, sélectionnez ce nœud, puis cliquez sur le lien **Paramètres** affiché en regard de ce nœud.
   • Répétez l'étape 5 pour modifier la planification de protection.

   Pour plus d'informations sur la personnalisation des nœuds, reportez-vous à la section Protection des nœuds dans un cluster.
8. Dans la boîte de dialogue **Protéger le cluster**, cliquez sur **Protéger**.

Protection des nœuds dans un cluster

Cette rubrique décrit comment protéger les données dans un nœud de cluster ou une machine sur lequel est installé un AppAssure Agent. Lorsque vous ajoutez une protection, vous devez sélectionner un nœud d'une liste de nœuds disponibles et également spécifier le nom d'hôte, le nom d'utilisateur et le mot de passe de l'administrateur de domaine.

Pour protéger des nœuds dans un cluster :

1. Après avoir ajouté un cluster, naviguez vers ce cluster et cliquez sur l'onglet **Ordinateurs**.
2. Cliquez sur le menu **Actions**, puis cliquez sur **Protéger le nœud de cluster**.
3. Dans la boîte de dialogue **Protéger le nœud de cluster**, sélectionnez ou entrez les informations suivantes, puis cliquez sur **Connecter** pour ajouter une machine ou un nœud.

Zone de texte	Description
Hôte	Une liste déroulante de nœuds de cluster disponibles pour la protection.
Port	Numéro du port sur lequel le Core communique avec l'agent sur le nœud.
Nom d'utilisateur	Le nom d'utilisateur de l'administrateur du domaine utilisé pour se connecter à ce nœud, par exemple, **example_domain\administrator** ou **administrateur@exemple_domaine.com**.
Mot de passe	Le mot de passe utilisé pour vous connecter à cet ordinateur

4. Cliquez sur **Protéger** pour démarrer la protection de cette machine avec les paramètres de protection par défaut.

   REMARQUE : Les paramètres par défaut assurent que tous les volumes de cette machine sont protégés avec une planification par défaut de toutes les 60 minutes.

5. Pour entrer les paramètres personnalisés pour cette machine, (par exemple, pour modifier le nom d'affichage, ajouter le chiffrement ou personnaliser la planification de protection), cliquez sur **Afficher les options avancées**.
6. Modifiez les paramètres suivants selon les besoins tel que décrit ci-dessous.

Zone de texte	Description
Nom d'affichage	Entrez un nouveau nom pour la machine ; ce nom s'affichera dans la Core Console.
Référentiel	Sélectionnez le référentiel sur le Core dans lequel les données de cette machine doivent être stockées.
Cryptage	Indiquez si le chiffrement doit être appliqué aux données dans le cas de chaque volume de cette machine qui sera stocké dans le référentiel. REMARQUE : Les paramètres de cryptage d'un référentiel sont définis sur l'onglet **Configuration** de Core Console.
Planification	Sélectionnez l'une des options suivantes : • Protéger tous les volumes avec la planification par défaut • Protéger des volumes spécifiques avec une planification personnalisée. Dans la zone **Volumes**, sélectionnez un volume et cliquez sur **Modifier**. Pour plus d'informations sur la définition d'intervalles personnalisés, voir Protection d'un cluster.

Processus de modification des paramètres de nœud de cluster

Après avoir ajouté la protection de nœuds de cluster, vous pouvez facilement modifier les paramètres de configuration de base pour ces ordinateurs/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 l'ordinateur, en ajoutant ou en supprimant des volumes, et/ou en suspendant la protection) et plus encore.

Pour modifier les paramètres de nœud de cluster, vous devez effectuer les tâches suivantes :

1. Effectuez l'une des opérations suivantes :

- Naviguez jusqu'au cluster qui contient le nœud que vous souhaitez modifier, cliquez sur l'onglet **Machines** (Ordinateurs), puis sélectionnez l'ordinateur ou le nœud que vous souhaitez modifier.
- Ou bien, dans le volet de **Navigation**, sous l'en-tête **Cluster**, sélectionnez l'ordinateur ou le nœud que vous souhaitez modifier.

2. Pour modifier et afficher les paramètres de configuration, reportez-vous à la section Affichage et modification des paramètres de configuration.
3. Pour configurer des groupes de notification pour les événements système, reportez-vous à la section Configuration des groupes de notification pour les événements système.
4. Pour personnaliser les paramètres de stratégie de rétention, reportez-vous à la section Personnalisation des paramètres de stratégie de rétention.
5. Pour modifier l'horaire de protection, reportez-vous à la section Modification des horaires de protection.
6. Pour modifier les paramètres de transfert, reportez-vous à la section Modification des paramètres de transfert.

Stratégie de configuration des paramètres de cluster

La tratégie de configuration des paramètres de cluster comprend les tâches suivantes :

- Modification des paramètres de cluster
- Configuration des notifications d'événements de cluster
- Modification de la stratégie de rétention du cluster
- Modification des horaires de protection du cluster
- Modification des paramètres de transfert de cluster

Modification des paramètres de cluster

Après avoir ajouté un cluster, vous pouvez, entre autres, aisément modifier les paramètres de base (par exemple, le nom d'affichage), les paramètres de protection (par exemple, les calendriers de protection, l'ajout ou la suppression de volumes et la mise en pause de la protection).

Pour modifier les paramètres d'un cluster

1. Effectuez l'une des opérations suivantes :
   - Dans la **Core Console**, cliquez sur l'onglet Machines, puis sélectionnez le cluster que vous souhaitez modifier.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster à modifier.
2. Cliquez sur l'onglet **Configuration**.

   L'écran **Paramètres** s'affiche.
3. Cliquez sur **Modifier** pour modifier les paramètres du cluster sur cette page, tel que décrit dans le tableau suivant :

Zone de texte	Description
Nom d'affichage	Entrez un nom d'affichage pour le cluster. Le nom de ce cluster s'affiche dans Core Console. Par défaut, il s'agit du nom d'hôte du cluster. Vous pouvez le rendre plus descriptif, le cas échéant.
Nom d'hôte	Ce paramètre représente le nom d'hôte du cluster. Il est indiqué ici uniquement à titre informatif et ne peut pas être modifié.

Zone de texte	Description
Référentiel	Entrez le référentiel du core lié au cluster. REMARQUE : Si des instantanés sont déjà utilisés pour ce cluster, ce paramètre est répertorié ici uniquement à titre informatif et ne peut pas être modifié.
Clé de chiffrement	Modifiez, puis sélectionnez une clé de chiffrement si nécessaire. Indique si le chiffrement doit être appliqué aux données dans le cas de chaque volume de ce cluster qui sera stocké dans le référentiel.

Configuration des notifications d'événements de cluster

Vous pouvez configurer la façon de rapporter les événements système de votre cluster en créant des groupes de notification. Ces événements peuvent être des alertes de système ou des erreurs.

Pour configurer les notifications d'événements de cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la **Core Console**, cliquez sur l'onglet Machines, puis sélectionnez le cluster que vous souhaitez modifier.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster à modifier.
2. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Événements**.
3. Sélectionnez l'une des options décrites dans le tableau suivant.

Zone de texte	Description
Utiliser les paramètres d'alerte du core	Les paramètres utilisés par le core associé sont alors adoptés : a. Cliquez sur **Appliquer**. b. Effectuez l'étape 5.
Utiliser les paramètres d'alerte personnalisés	Cela vous permet de configurer des paramètres personnalisés. Passez à l'étape 4.

4. Si vous sélectionnez **Paramètres d'alerte personnalisés**, cliquez sur **Ajouter un groupe** pour ajouter un nouveau groupe de notification pour l'envoi d'une liste d'événements système.

   La boîte de dialogue **Ajouter un groupe de notifications** s'ouvre.
5. Ajoutez les options de notification tel que décrit dans le tableau suivant.

Zone de texte	Description
Nom	Entrez un nom pour le groupe de notification.
Description	Entrez une description du groupe de notification.
Activez les événements	Sélectionnez les événements pour lesquels des notifications doivent être envoyées, par exemple, Clusters. Vous pouvez également choisir de sélectionner par type : • **Erreur**

Zone de texte	Description
	• **Avertissement** • **Informatif** REMARQUE : Lorsque vous choisissez de sélectionner par type, par défaut, les événements appropriés sont automatiquement activés. Par exemple, si vous choisissez Avertissement, les événements de Capacité d'attachement, Tâches, Licences, Archive, CoreService, Exportation, Protection, Réplication et Restauration sont activés.
Options de notification	Sélectionnez une méthode pour spécifier la façon de traiter les notifications. Vous pouvez choisir parmi les options suivantes : • **Notifier par courrier électronique** : spécifiez à quelles adresses électroniques envoyer les événements dans les zones de texte À, Cc et, éventuellement, Cci. • **Notifier via le journal d'événements Windows** : le journal d'événements Windows contrôle la notification. • **Notifier par syslogd** : spécifiez à quels nom d'hôte et port envoyer les événements.

6. Cliquez sur **OK** pour enregistrer vos modifications, puis cliquez sur **Appliquer**.
7. Pour modifier un groupe de notifications existant, cliquez sur **Modifier** en regard d'un groupe de notification de la liste.

   La boîte de dialogue **Modifier le groupe de notifications** s'affiche et vous pouvez modifier les paramètres.

Modification de la stratégie de rétention du cluster

La stratégie de rétention d'un cluster spécifie la durée de stockage des points de restauration des volumes partagés dans le référentiel. Les stratégies de rétention sont utilisées pour conserver les instantanés pendant plus longtemps et pour aider la gestion de ces instantanés de sauvegarde. La stratégie de rétention est activée par un processus cumulatif servant à supprimer les anciennes sauvegardes.

1. Effectuez l'une des opérations suivantes :
   - Dans la **Core Console**, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster que vous souhaitez modifier.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster à modifier.
2. Sélectionnez l'onglet **Configuration**, puis cliquez sur **Stratégie de rétention**.
3. Sélectionnez l'une des options dans le tableau suivant :

Zone de texte	Description
Utiliser la stratégie de rétention par défaut	Cela adopte les paramètres utilisés par le core associé. Cliquez sur **Appliquer**.
Utiliser une stratégie de rétention personnalisée	Cela vous permet de configurer des paramètres personnalisés.

REMARQUE : Si vous avez sélectionné les **Paramètres d'alerte personnalisés**, suivez les instructions de configuration de la stratégie de rétention personnalisée tel que décrit dans Personnalisation des paramètres des stratégies de rétention, en commençant par l'étape 4.

Modification des horaires de protection du cluster

Vous pouvez modifiez les horaires de protection uniquement si votre cluster possède des volumes partagés.

Pour modifier des horaires de protection de cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la **Core Console**, cliquez sur l'onglet Machines, puis sélectionnez le cluster que vous souhaitez modifier.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster à modifier.
2. Cliquez sur l'onglet **Configuration**, puis cliquez sur **Paramètres de protection**.
3. Suivez ces instructions pour modifier les paramètres de protection tels que décrits dans Modification des horaires de protection, en commençant par l'étape 2.

Modification des paramètres de transfert de cluster

Dans AppAssure, vous pouvez modifier les paramètres pour gérer les processus de transfert de données d'un cluster protégé.

REMARQUE : Vous pouvez modifier les paramètres de transfert du cluster uniquement si votre cluster possède des volumes partagés.

Il existe trois types de transferts dans le système AppAssure :

Zone de texte	Description
Instantanés	Sauvegarde les données sur votre cluster protégé.
Exportation VM	Crée une machine virtuelle avec toutes les informations de sauvegarde et les paramètres comme spécifié par l'horaire défini pour la protection de l'ordinateur.
Restauration	Restaure les informations de sauvegarde d'un cluster protégé.

Pour modifier les paramètres de transfert d'un cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la **Core Console**, cliquez sur l'onglet Machines, puis sélectionnez le cluster que vous souhaitez modifier.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster à modifier.
2. Cliquez sur l'onglet **Configuration**, puis sur **Paramètres de transfert**.
3. Modifiez les paramètres de protection comme l'indique la rubrique Modification des horaires de protection, en commençant par l'étape 2.

Conversion d'un nœud de cluster protégé en agent

Dans AppAssure 5, vous pouvez convertir un nœud de cluster protégé en agent AppAssure pour qu'il continue à être géré par le Core mais ne fasse plus partie du cluster. Cela est utile lorsque vous devez retirer le nœud de cluster du cluster mais que vous devez toujours le protéger.

Pour convertir un nœud de cluster protégé en agent :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Ordinateurs**, puis sélectionnez le cluster contenant l'ordinateur que vous souhaitez convertir. Ensuite, cliquez sur l'onglet **Machines** du cluster.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster qui contient l'ordinateur que vous souhaitez convertir, puis cliquez sur l'onglet **Machines**.
2. Sélectionnez l'ordinateur à convertir, puis, dans le menu déroulant **Actions** en haut de l'onglet Machines, cliquez sur **Convertir en agent**.
3. Pour rajouter l'ordinateur au cluster, sélectionnez l'ordinateur, puis cliquez sur l'onglet **Résumé**, le menu **Actions**, puis **Convertir en nœud**.

Affichage des Informations de cluster de serveur

Affichage des informations système de cluster

Pour afficher les informations système de cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster que vous souhaitez afficher.
   - Ou bien, dans la zone de **navigation** à gauche, sélectionnez le cluster que vous souhaitez afficher.
2. Cliquez sur l'onglet **Outils**.

   La page des **Informations système** qui s'affiche contient les informations détaillées du système sur le cluster, tel que le nom, les nœuds inclus avec leur état associé et les versions de Windows, les informations sur l'interface réseau et sur la capacité des volumes.

Affichage d'événements et d'alertes de cluster

Pour en savoir plus sur l'affichage des événements et les alertes d'un ordinateur ou d'un nœud particulier dans un cluster, voir Affichage d'événements et d'alertes.

Pour afficher des événements et alertes :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster que vous souhaitez afficher.
   - Ou bien, dans la zone de **Navigation** à gauche, sous **Clusters**, sélectionnez le cluster que vous souhaitez afficher.
2. Cliquez sur l'onglet **Événements**.

   Un journal affiche tous les événements des tâches actuelles, ainsi que toute alerte du cluster.
3. Pour filtrer la liste des événements, cochez ou décochez les cases **Actif**, **Terminé** ou **En échec**, selon le cas.
4. Dans le tableau **Alertes**, cliquez sur **Éliminer tout** pour éliminer toutes les alertes de la liste.

Affichage du résumé des informations

Pour afficher le résumé des informations

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster que vous souhaitez afficher.

- Ou bien, dans la zone de **Navigation** à gauche, sous **Clusters**, sélectionnez le cluster que vous souhaitez afficher.

2. Dans l'onglet **Récapitulatif**, vous pouvez visualiser des informations telles que le nom de cluster, le type de cluster, le type de quorum (le cas échéant) et le chemin d'accès au quorum (le cas échéant).

   Cet onglet affiche aussi les informations d'ensemble sur les volumes de ce cluster, y compris la taille et l'horaire de protection.

3. Pour rafraîchir ces informations, dans le menu déroulant **Actions**, cliquez sur **Rafraîchir les métadonnées**.

   Pour en savoir plus sur l'affichage du résumé et les informations sur l'état d'un ordinateur ou d'un nœud particulier dans le cluster, reportez-vous à la section Affichage de l'état d'une machine et d'autres détails.

Travailler avec des points de restauration de cluster

Un point de restauration, aussi nommé instantané, est une copie d'un point dans le temps des dossiers et fichiers des volumes partagés d'un cluster, stockés dans le référentiel. Les points de restauration servent à restaurer les machines protégées ou à effectuer un montage sur un système de fichiers local. Dans AppAssure, vous pouvez afficher les listes de points de restauration du référentiel. Effectuez les étapes de la procédure suivante pour vérifier les points de restauration.

REMARQUE : Si vous protégez des données d'un cluster de serveur DAG ou CCR, les points de restauration ne s'affichent pas au niveau du cluster. Ils sont visibles uniquement au niveau du nœud ou de la machine.

Pour en savoir plus sur l'affichage des points de restauration pour des machines individuelles dans un cluster, voir Affichage des points de restauration.

Pour travailler avec des points de restauration de cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
   - Ou bien, dans la zone de navigation à gauche, sous **Clusters**, sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
2. Cliquez sur l'onglet **Points de restauration**.
3. Pour afficher des informations détaillées sur un point de restauration particulier, cliquez sur le symbole en forme de chevron droit **>** en regard du point de restauration dans la liste pour développer la vue.

   Pour plus d'informations sur les opérations que vous pouvez effectuer sur les points de restauration, reportez-vous à la section Affichage d'un point de restauration spécifique.
4. Sélectionnez un point de restauration à monter.

   Pour plus d'informations sur la façon de monter un point de restauration, reportez-vous à la section Montage d'un point de restauration pour une machine Windows, en commençant par l'étape 2.
5. Pour supprimer des points de restauration, voir Suppression de points de restauration.

Gestion des instantanés d'un cluster

Vous pouvez gérer des instantanés en forçant un instantané ou en suspendant les instantanés actuels. Le forçage d'un instantané vous permet de forcer un transfert de données pour le cluster actuellement protégé. Lorsque vous forcez un instantané, le transfert démarre immédiatement ou est ajouté à la file d'attente. Seules les donnés modifiées depuis un point de restauration précédent sont transférées. S'il n'existe aucun point de restauration précédent, toutes les données (image de base) des volumes protégés

sont transférées. Lorsque vous suspendez un instantané, vous arrêtez temporairement tous les transferts de données depuis l'ordinateur actuel.

Pour savoir comment forcer des instantanés des ordinateurs individuels d'un cluster, voirForcer un instantané. Pour savoir comment suspendre et reprendre des instantanés des instantanés d'ordinateurs individuels d'un cluster, voirSuspendre et reprendre un instantané.

Forçage d'un instantané de cluster

Pour forcer un instantané d'un cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
   - Ou bien, dans la zone de navigation à gauche, sous **Clusters**, sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
2. Dans l'onglet **Résumé**, cliquez sur le menu déroulant **Actions**, puis cliquez sur **Forcer un instantané**.

Suspension et reprise d'instantanés de cluster

Pour suspendre et relancer des instantanés de cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
   - Ou bien, dans la zone de navigation à gauche, sous **Clusters**, sélectionnez le cluster dont vous souhaitez afficher les points de restauration.
2. Dans l'onglet **Résumé**, cliquez sur le menu déroulant Actions, puis cliquez sur **Suspendre les instantanés**.
3. Dans la boîte de dialogue **Suspendre la protection**, sélectionnez l'une des options décrites ci-dessous.

Zone de texte	Description
Suspendre jusqu'à la reprise	Suspend l'instantané jusqu'à ce que vous repreniez manuellement la protection. Pour reprendre la protection, cliquez sur le menu **Actions**, puis cliquez sur **Reprendre**.
Suspendre pendant	Vous permet d'indiquer la durée en jours, heures et minutes de la suspension des instantanés.

Démontage des points de restauration locaux

Pour démonter les points de restauration locaux :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Ordinateurs**, puis sélectionnez le cluster dont vous souhaitez démonter les points de restauration.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster dont vous souhaitez démonter les points de restauration.
2. Sous l'onglet **Outils**, dans le menu **Outils**, sélectionnez **Montages**.
3. Dans la liste de montages locaux, effectuez l'une des actions suivantes :
   - Dans la liste des montages locaux, localisez et sélectionnez le montage du point de restauration que vous souhaitez démonter, puis cliquez sur **Démonter**.

- Pour démonter tous les montages locaux, cliquez sur le bouton **Démonter tout**.

Exécution d'une restauration de clusters et de nœuds de cluster

Une restauration est le processus consistant à restaurer des volumes sur un ordinateur à partir de points de restauration. Pour un serveur de clusters, la restauration s'effectue au niveau du nœud ou de l'ordinateur. Cette section fournit des instructions d'exécution d'une restauration de volumes de clusters.

Effectuer une restauration automatique de clusters CCR (Exchange) et DAG

Pour effectuer une restauration de clusters SCC (Exchange, SQL) :

1. Arrêtez tous les nœuds sauf un.
2. Effectuez une restauration à l'aide de la procédure standard AppAssure pour l'ordinateur, tel que décrite à la section Exécution d'une restauration et Exécution d'une restauration pour une machine Linux à l'aide de la ligne de commande.
3. Lorsque la restauration est terminée, montez toutes les bases de données à partir des volumes de cluster.
4. Mettez sous tension tous les autres nœuds.
5. Pour Exchange, naviguez jusqu'à Exchange Management Console, puis, pour chaque base de données, effectuez l'opération **Update Database Copy** (Mise à jour de la copie de la base de données).

Exécution d'une restauration de clusters SCC (Exchange, SQL)

Pour effectuer une restauration de clusters SCC (Exchange, SQL) :

1. Arrêtez tous les nœuds sauf un.
2. Effectuez une restauration à l'aide de la procédure standard AppAssure pour l'ordinateur, tel que décrite à la section Exécution d'une restauration et Exécution d'une restauration pour une machine Linux à l'aide de la ligne de commande.
3. Lorsque la restauration est terminée, montez toutes les bases de données à partir des volumes de cluster.
4. Mettez sous tension tous les nœuds un par un.

REMARQUE : Vous ne devez pas effectuer une restauration automatique du disque de quorum. Celui-ci peut être regénéré automatiquement ou en utilisant la fonctionnalité du service de cluster.

Réplication des données de cluster

Lorsque vous répliquez les donnés d'un cluster, vous devez configurer la réplication au niveau de l'ordinateur des ordinateurs individuels de ce cluster. Vous pouvez également configurer la réplication pour qu'elle réplique les points de restauration des volumes partagés (par exemple, si vous souhaitez répliquer cinq agents de la source à la cible).

Pour plus d'informations et des instructions sur la réplication de données, reportez-vous à Réplication de données d'agent d'une machine.

Retrait de la protection d'un cluster

Pour retirer la protection d'un cluster :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster que vous souhaitez retirer.
   - Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster que vous souhaitez retirer pour afficher l'onglet **Récapitulatif**.
2. Cliquez sur le menu déroulant **Actions**, puis cliquez sur **Supprimer un ordinateur**.
3. Sélectionnez l'une des options suivantes :

Option	Description
Conserver les points de restauration	Pour conserver les points de restauration actuellement stockés pour ce cluster.
Supprimer des points de restauration	Pour supprimer du référentiel tous les points de restauration de ce cluster actuellement stockés.

Retrait des nœuds de cluster de la protection

Effectuez les étapes des procédures suivantes pour retirer les nœuds de cluster de la protection. Si vous souhaitez simplement retirer un nœud du cluster, reportez-vous à la section Conversion d'un nœud de cluster protégé en agent. Pour supprimer la protection d'un nœud de cluster.

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines** (Ordinateurs), puis sélectionnez le cluster qui contient le nœud que vous souhaitez retirer. Dans l'onglet **Machines** du cluster, sélectionnez le nœud que vous souhaitez retirer.
   - Ou bien, dans la zone de navigation à gauche, sous le cluster associé, sélectionnez le nœud que vous souhaitez retirer.
2. Cliquez sur le menu déroulant **Actions**, puis cliquez sur **Supprimer un ordinateur**.
3. Sélectionnez l'une des options décrites dans le tableau suivant.

Option	Description
Relation seulement	Retire le core source de la réplication mais conserve les points de restauration répliqués.
Avec les points de restauration	Retire le core source de la réplication et supprime tous les points de restauration reçus depuis cet ordinateur.

Retrait de la protection de tous les nœuds d'un cluster

Pour retirer tous les nœuds d'un cluster de la protection :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines** (Ordinateurs) et sélectionnez le cluster qui contient les nœuds que vous souhaitez supprimer. Ensuite, cliquez sur l'onglet **Machines** du cluster.

- Ou bien, dans la zone de navigation à gauche, sélectionnez le cluster qui contient les nœuds que vous souhaitez retirer, puis cliquez sur l'onglet **Machines**.

2. Cliquez sur le menu déroulant **Actions** en haut de l'onglet **Machines**, puis cliquez sur **Supprimer des ordinateurs**.
3. Sélectionnez l'une des options décrites dans le tableau suivant.

Option	Description
Relation seulement	Retire le core source de la réplication mais conserve les points de restauration répliqués.
Avec les points de restauration	Retire le core source de la réplication et supprime tous les points de restauration reçus depuis cet ordinateur.

Affichage d'un cluster ou d'un rapport de nœud

Vous pouvez créer et afficher des rapports de conformité et d'erreurs concernant les activités d'AppAssure de votre cluster et de vos nœuds individuels. Les rapports comprennent des informations sur l'activité d'AppAssure 5 sur le cluster, le nœud et les volumes partagés. Pour en savoir plus sur les rapports AppAssure, voir À propos des rapports.

Pour en savoir plus sur les options d'exportation et d'impression localisées dans la barre d'outil Rapports, voir À propos de la barre d'outils des rapports.

Pour afficher un rapport de cluster ou de nœud :

1. Effectuez l'une des opérations suivantes :
   - Dans la Core Console, cliquez sur l'onglet **Machines**, puis sélectionnez le cluster pour lequel vous souhaitez créer un rapport.
   - Ou bien, dans la zone de **navigation** à gauche, sélectionnez le cluster pour lequel vous souhaitez créer un rapport.
2. Cliquez sur l'onglet **Outils** et sélectionnez l'une des options suivantes sous le menu **Rapports** :
   - **Rapport de conformité**
   - **Rapport d'erreurs**
3. Dans le calendrier déroulant **Heure de début**, sélectionnez une date de début, puis entrez une heure de début pour l'exportation.

   REMARQUE : Aucune donnée n'est disponible pour la période précédant le déploiement de l'AppAssure Core ou de l'AppAssure Agent.
4. Dans le calendrier déroulant **Heure de fin**, sélectionnez une date de fin, puis entrez une heure de fin de rapport.
5. Cliquez sur **Générer un rapport**.

   Si le rapport s'étale sur plusieurs pages, cliquez sur les numéros de page ou sur les boutons flèches en haut des résultats du rapport afin de feuilleter les résultats.

   Les résultats du rapport apparaissent sur la page.
6. Pour exporter les résultats du rapport dans un des formats disponibles (PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV ou image), sélectionnez le format de l'exportation de la liste déroulante, puis effectuez l'une des actions suivantes :
   - Cliquez sur la première icône **Enregistrer** pour exporter un rapport et l'enregistrer sur un disque.
   - Cliquez sur la deuxième icône **Enregistrer** pour exporter un rapport et l'afficher dans une nouvelle fenêtre de navigation Web.

7. Pour imprimer les résultats du rapport, effectuez l'une des actions suivantes :
    - Cliquez sur la première icône **Imprimante** pour imprimer la totalité du rapport.
    - Cliquez sur la deuxième icône **Imprimante** pour imprimer la page de rapport actuelle.

6

Rapports

À propos des rapports

Le système DL permet de générer et d'afficher les informations de conformité, d'erreurs et récapitulatives de plusieurs machines core et agent.

Vous pouvez choisir d'afficher des rapports en ligne, d'imprimer des rapports ou de les exporter et de les enregistrer à l'un de plusieurs formats pris en charge. Vous pouvez choisir parmi les formats suivants :

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- txt
- CSV
- Image

À propos de la barre d'outils Rapports

La barre d'outils de tous les rapports vous permet d'imprimer et d'enregistrer de deux façons différentes. Le tableau suivant décrit les options d'impression et d'enregistrement.

Icon	Description
	Imprimer le rapport
	Imprimer la page actuelle
	Exporter un rapport et l'enregistrer sur le disque
	Exporter un rapport et l'afficher dans une nouvelle fenêtre Utilisez cette option pour copier, coller et envoyer par e-mail l'URL afin que d'autres puissent visualiser le rapport avec un navigateur Web.

À propos des rapports de conformité

Les rapports de conformité sont disponibles pour le Core et AppAssure Agent. Ils permettent de visualiser le statut des tâches effectuées par un core ou un agent sélectionné. Les tâches qui ont échoué apparaissent en rouge. Les informations du rapport de conformité du core non associé à un agent ne s'affichent pas.

Les détails sur les cores s'affichent par colonne et incluent les catégories suivantes :

- Core
- Agent protégé
- Type
- Résumé
- Condition
- Erreur
- Heure de début
- Heure de fin
- Heure
- Travail total

À propos des rapports d'erreurs

Les rapports d'erreurs sont des sous-ensembles des Rapports de conformité et sont disponibles pour les cores et les agents AppAssure. Ces rapports contiennent uniquement les tâches ayant échoué listées dans les rapports de conformité et les compilent dans un rapport unique pouvant être imprimé et exporté.

Les détails sur les erreurs s'affichent dans une vue de colonne et incluent les catégories suivantes :

- Core
- Agent
- Type
- Résumé
- Erreur
- Heure de début
- Heure de fin
- Temps écoulé
- Travail total

.

À propos du rapport de résumé de core

Le **rapport récapitulatif du core** contient des informations sur les référentiels du core sélectionné et sur les agents protégés par le core. Les informations s'affichent sous forme de deux résumés dans un rapport.

Résumé des référentiels

La partie **Référentiels** du **Rapport de résumé de core** comprend des données des référentiels se trouvant dans le core sélectionné. Les détails concernant les référentiels sont affichés dans une vue de colonne sous les catégories suivantes :

- Nom
- Chemin de données
- Chemin des métadonnées

- Espace alloué
- Espace utilisé
- Espace libre
- Ratio de compression/déduplication

Résumé des agents

La partie **Agents** du **Rapport de résumé Core** comprend les données de tous les agents protégés par le core sélectionné.

Les détails concernant les agents s'affichent en colonnes et incluent les catégories suivantes :

- Nom
- Volumes protégés
- Quantité d'espace protégé
- Quantité d'espace actuellement protégé
- Taux de changement quotidien (**Moyenne**, **Médian**)
- Statistiques de tâche (**Réussite**, **En échec**, **Annulé**)

Génération d'un rapport pour un core ou un agent

Pour générer un rapport pour un core ou un agent:

1. Accédez à Core Console et sélectionnez le core ou l'agent pour lequel vous souhaitez exécuter le rapport.
2. Cliquez sur l'onglet **Outils**.
3. Dans l'onglet **Outils**, développez **Rapports** dans la zone de navigation à gauche.
4. Dans la zone de navigation à gauche, sélectionnez le rapport à exécuter. La disponibilité des rapports dépend de la sélection effectuée à l'Étape 1. Vous trouverez la description des rapports ci-dessous.

Ordinateur	Rapports disponibles
Core	Rapport de conformité
	Rapport de résumé
	Rapport d'erreurs
Agent	Rapport de conformité
	Rapport d'erreurs

5. Dans le calendrier déroulant **Heure de début**, sélectionnez une date de début, puis entrez une heure de début pour l'exportation.

   REMARQUE : Aucune donnée n'est disponible tant que le core ou l'agent n'a pas été déployé.
6. Dans le calendrier déroulant **Heure de fin**, sélectionnez une date de fin, puis entrez une heure de fin de rapport.
7. Pour un **Rapport de résumé de core**, cochez la case **Tout le temps** si vous souhaitez que l'**Heure de début** et l'**Heure de fin** couvrent la totalité de la durée de vie du core.
8. Pour un **Rapport de conformité du core** ou un **Rapport d'erreurs du core**, utilisez la liste déroulante **Cores cibles** pour sélectionner le core dont vous souhaitez afficher les données.
9. Cliquez sur **Générer un rapport**.

Une fois le rapport généré, utilisez la barre d'outils pour imprimer ou exporter le rapport.

À propos des rapports de core de la Central Management Console

Le système DL permet de générer et afficher des informations de conformité, d'erreur et récapitulatives pour plusieurs cores. Les informations sur les cores s'affichent dans des colonnes avec les catégories décrites dans cette section.

Génération d'un rapport depuis la Central Management Console

Pour générer un rapport depuis la Central Management Console :

1. À l'écran **Bienvenue dans Central Management Console**, cliquez sur le menu déroulant situé dans le coin supérieur droit.
2. Dans le menu déroulant, cliquez sur **Rapports**, puis sélectionnez une des options suivantes :
   - **Rapport de conformité**
   - **Rapport de résumé**
   - **Rapport des échecs**
3. Dans la zone de navigation de gauche, sélectionnez le ou les cores pour lesquels vous souhaitez exécuter le rapport.
4. Dans le calendrier déroulant **Heure de début**, sélectionnez une date de début, puis entrez une heure de début pour le rapport.

   REMARQUE : Aucune donnée n'est disponible tant que les cores n'ont pas été déployés.
5. Dans le calendrier déroulant **Heure de fin**, sélectionnez une date de fin, puis entrez une heure de fin de rapport.
6. Cliquez sur **Générer un rapport**.

   Une fois le rapport généré, utilisez la barre d'outils pour imprimer ou exporter le rapport.

7

Exécution d'une restauration totale de l'appliance DL4300

Les lecteurs de données de l'appliance de sauvegarde sur disque DL4300 se trouvent dans les logements .C-11 et 14-17 et au format RAID 6, ils peuvent subir un maximum de deux échecs de lecteur sans perte de données. Le système d'exploitation réside sur les lecteurs 12 et 13, formatés sous forme d'un disque virtuel RAID 1. Si ces deux disques échouent, vous devez remplacer les lecteurs et réinstaller le logiciel nécessaire au fonctionnement de l'appliance. Pour effectuer une restauration totale de l'appliance, procédez comme suit :

- Créer une partition RAID 1 pour le système d'exploitation
- Installer le système d'exploitation.
- Exécuter le Recovery and Update Utility
- Remonter les volumes

Création d'une partition RAID 1 pour le système d'exploitation

PRÉCAUTION : Il est essentiel que vous réalisiez ces opérations uniquement sur les disques virtuels RAID 1 contenant le système d'exploitation. Ne réalisez pas ces opérations sur les disques virtuels RAID contenant des données.

Pour créer une partition RAID 1 :

1. Vérifiez que les disques installés dans les logements 12 et 13 sont des disques dont le bon état de fonctionnement est connu.
2. Amorcez l'appliance DL4300 Backup to Disk.
3. À l'invite pendant le processus d'amorçage, appuyez sur <Ctrl><R>.

   L'écran **Utilitaire de configuration BIOS PERC** s'affiche.
4. Mettez en surbrillance le contrôleur en haut de l'onglet **Gestion de disques virtuels**, appuyez sur <F2>, puis sélectionnez **Créer un nouveau disque virtuel**.

   REMARQUE : Si le disque virtuel de système d'exploitation RAID 1 est déjà présent, appliquez-lui la commande fast-init (initialisation rapide).
5. À la page **Gestion de disques virtuels**, sélectionnez RAID 1 pour le niveau RAID.
6. Sélectionnez les deux disques dans la zone **Disques Physiques**.

   REMARQUE : La taille du disque virtuel ne doit pas dépasser 278,87 Go.
7. Saisissez un nom de disque virtuel, tel que « SE », qui identifie le disque virtuel comme celui qui contient le système d'exploitation.
8. Appuyez sur <Tab> pour déplacer le curseur vers l'option Initialiser, puis appuyez sur <Entrée>.

REMARQUE : L'initialisation effectuée à ce stade est une initialisation rapide.

9. Cliquez sur **OK** pour terminer la sélection ou appuyez sur <Ctrl><N> deux fois.

   La page **Gestion des contrôles** s'affiche.

10. Naviguez jusqu'au champ **Sélectionner un périphérique d'amorçage** et sélectionnez le disque virtuel contenant le système d'exploitation.

    La capacité de ce disque est d'à peu près 278 Go.

11. Sélectionnez **Appliquer** et appuyez sur <Entrée>.
12. Quittez l'utilitaire de **Configuration BIOS PERC** et appuyez sur <Ctrl><Alt><Del> pour redémarrer le système.

Installation du système d'exploitation

Utilisez l'utilitaire Dell Unified Server Configurator - Lifecycle Controller Enabled - (USC LCE) sur votre appliance pour restaurer le système d'exploitation :

1. Munissez-vous du support d'installation du système d'exploitation.
2. Assurez-vous d'avoir un disque depuis lequel exécuter le support.

   Vous pouvez utiliser un disque optique USB ou un périphérique de support virtuel. Le support virtuel est pris en charge au moyen d'iDRAC. Pour en savoir plus sur la configuration d'un support virtuel au moyen d'iDRAC, voir le Guide d'utilisation du périphérique iDRAC de votre système.

   Si le support d'installation est corrompu ou illisible, USC(Unified Server Configurator, configurateur de serveur unifié) risque de ne pas pouvoir détecter la présence d'un lecteur optique pris en charge. Dans ce cas, un message d'erreur peut vous indiquer qu'aucun lecteur optique n'est disponible. Si le support n'est pas valide (s'il s'agit du mauvais CD ou DVD, par exemple), un message s'affiche et vous demande d'insérer le support d'installation correct.

3. Démarrez l'USC en amorçant le système et en appuyant sur la touche <F10> dans les 10 secondes qui suivent l'affichage du logo Dell.
4. Cliquez sur **OS Deployment** (Déploiement du système d'exploitation) dans le volet de gauche.
5. Cliquez sur **Deploy OS** (Déployer le système d'exploitation) dans le volet de droite.
6. Sélectionnez la langue du système d'exploitation, puis cliquez sur **Suivant**.

   USC extrait les pilotes requis par le système d'exploitation que vous avez sélectionné. Les pilotes sont extraits vers un disque USB interne nommé **OEMDRV**.

   REMARQUE : Le processus d'extraction des pilotes peut prendre plusieurs minutes.

   REMARQUE : Tous les pilotes copiés par l'Assistant Déploiement SE sont supprimés au bout de 18 heures. Vous devez compléter l'installation du système d'exploitation dans les 18 heures pour que les pilotes copiés soient disponibles. Pour supprimer les pilotes avant la fin de la période de 18 heures, redémarrez le système et appuyez sur la clé <F10> pour entrer de nouveau dans l'USC. L'utilisation de la clé <F10> pour annuler l'installation du système d'exploitation ou pour entrer de nouveau dans l'USC lors de l'amorçage supprime les pilotes au cours de la période de 18 heures.

7. Une fois les pilotes extraits, l'USC vous invite à insérer le support d'installation du système d'exploitation.

   REMARQUE : Lors de l'installation du système d'exploitation Microsoft Windows, les pilotes extraits sont automatiquement installés.

Exécution de l'utilitaire de restauration et de mise à jour

Pour exécuter le Recovery and Update Utility :

1. Téléchargez le **Recovery and Update Utility** depuis **dell.com/support**.
2. Copiez l'utilitaire sur le bureau de l'appliance DL4300 Backup to Disk et extrayez les fichiers.
3. Double-cliquez sur **launchRUU**.
4. À l'invite, cliquez sur **Oui** pour confirmer que vous n'exécutez aucun des processus énumérés.
5. Cliquez sur **Démarrer** lorsque l'écran **Recovery and Update Utility** s'affiche.
6. Lorsque le programme vous invite à redémarrer, cliquez sur **OK**.

   Les rôles et fonctionnalités Windows Server, ASP .NET MVC3, le fournisseur LSI, les applications DL, et les logiciels OpenManage Server Administrator et AppAssure Core sont installés dans le cadre de Recovery and Update Utility.
7. Redémarrez votre système à l'invite suivante.
8. Après avoir installé tous les services et applications, cliquez sur **Continuer**.

   L'Assistant **Restauration de l'appliance AppAssure** démarre.
9. Réalisez les étapes de la phase **Collecte d'informations et configuration** de l'Assistant Restauration de l'appliance AppAssure, puis cliquez sur **Suivant**.

   La phase **Restauration de disque** commence.
10. Cliquez sur **Suivant** après avoir lu l'avertissement concernant la mise hors tension des services AppAssure.

    Les disques virtuels des référentiels et toute machine virtuelle de secours sont restaurés et les services AppAssure sont redémarrés. La restauration est terminée.

8

Modification manuelle du nom d'hôte

Il vous est recommandé de sélectionner un nom d'hôte au cours de la configuration initiale de DL4300 Backup to Disk Appliance. Si vous modifiez le nom d'hôte ultérieurement à l'aide des **Propriétés du système Windows**, vous devez réaliser les étapes suivantes manuellement pour que le nouveau nom d'hôte soit appliqué et pour que l'appliance fonctionne correctement :

1. Arrêter le service AppAssure Core
2. Supprimer les certificats de serveur AppAssure
3. Supprimer le serveur Core et les clés de registre
4. Modifier le nom d'affichage dans AppAssure
5. Mettre à jour les sites de confiance dans Internet Explorer

Arrêt du service Core

Pour arrêter les services AppAssure Core :

1. Ouvrez **Windows Server Manager**.
2. Dans l'arborescence de gauche, sélectionnez **Configuration** → **Services.**
3. Effectuez un clic droit sur **AppAssure Core Service** et sélectionnez **Arrêter**.

Suppression des certificats de serveur

Pour supprimer des certifcats AppAssure Server :

1. Ouvrez une interface de ligne de commande.
2. Entrez **Certmgr** et appuyez sur <Entrée>.
3. Dans la fenêtre **Certificate Manager**, select **Autorités de certification de racine de confiance** → **Certificats.**
4. Supprimer tout certificat pour lequel la colonne **Attribuer à** affiche l'ancien nom d'hôte et la colonne **Rôle prévu** affiche **Authentification de serveur**.

Suppression du serveur Core et des clés de registre

Pour supprimer le Core Server et les clés de registre :

1. Ouvrez une interface de ligne de commande.
2. Tapez **regedit** et appuyez sur <Entrée> pour lancer l'Éditeur de registre.
3. Dans l'arborescence, naviguez jusqu'à **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** et ouvrez le répertoire Core.
4. Supprimez les répertoires **webServer** et **serviceHost**.

Lancement de Core avec le nouveau nom d'hôte

Pour lancer Core à l'aide du nouveau nom d'hôte que vous avez créé manuellement :

1. Démarrez les services AppAssure Core.
2. Effectuez un clic droit sur l'icône **AppAssure 5 Core** sur le bureau, puis cliquez sur **Propriétés**.
3. Remplacez l'ancien nom du serveur par le nouveau (`<server name:8006>`).
   Par exemple, **https://<servername:8006/apprecovery/admin/Core**.
4. Cliquez sur **OK**, puis lancez la console AppAssure Core à l'aide de l'icône **AppAssure 5 Core**.

Modification du nom d'affichage

Pour modifier le nom d'affichage :

1. Connectez-vous à la **console AppAssure** en tant qu'administrateur.
2. Sélectionnez l'onglet **Configuration**, puis cliquez sur le bouton Modifier dans la barre **Généralités**.
3. Entrez le nouveau **Nom d'affichage** et cliquez sur **OK**.

Mise à jour des sites de confiance dans Internet Explorer

Pour mettre à jour les sites de confiance dans Internet Explorer :

1. Ouvrez Internet Explorer.
2. Si les menus **Fichier**, **Modifier la vue** et autres ne sont pas affichés, appuyez sur <F10>.
3. Cliquez sur le menu **Outils** et sélectionnez **Options Internet**.
4. Dans la fenêtre **Options Internet**, cliquez sur l'onglet **Sécurité**.
5. Cliquez sur **Sites de confiance** et cliquez sur **Sites**.
6. Dans **Ajouter ce site Web à la zone**, saisissez **https://[Nom d'affichage]** et utilisez le nouveau nom que vous avez fourni pour le nom d'affichage.
7. Cliquez sur **Add** (Ajouter).
8. Sous **Ajouter ce site Web à la zone**, entrez **about:blank**.
9. Cliquez sur **Add** (Ajouter).
10. Cliquez sur **Fermer**, puis sur **OK**.

9

Annexe A : Créature de scripts

À propos de la création de scripts PowerShell

Windows PowerShell est un environnement connecté à Microsoft .NET Framework conçu pour l'automatisation de l'administration. AppAssure comprend des SDK (Software development kits - Kits de développement de logiciel) client exhaustifs pour la création de scripts PowerShell qui permettent aux administrateurs d'automatiser l'administration et la gestion des ressources AppAssure 5 au moyen de l'exécution de commandes via des scripts.

Il permet aux utilisateurs administratifs d'exécuter des scripts PowerShell fournis par l'utilisateur à intervalles désignés. Par exemple, avant ou après un instantané, des vérifications de capacité d'attachement et montabilité, etc. Les administrateurs peuvent exécuter des scripts depuis l'AppAssure Core et l'agent. Les scripts acceptent des paramètres et la sortie d'un script est écrite sur les fichiers core et les fichiers journaux de l'agent.

REMARQUE : Pour les tâches nocturnes, vous devez conserver un fichier de script ainsi que le paramètre d'entrée JobType afin de faire la distinction entre les tâches nocturnes.

Les fichiers 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. Il doit être installé puis configuré avant l'utilisation et l'exécution de scripts AppAssure.

PowerShell Scripting : conditions requises

Avant l'utilisation et l'exécution de scripts PowerShell for AppAssure, vous devez installer Windows PowerShell 2.0.

REMARQUE : Veillez à placer le fichier **powershell.exe.config** dans le répertoire d'accueil PowerShell. Par exemple, **C: \WindowsPowerShell\powershell.exe**.

powershell.exe.config

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

Test de scripts

Si vous souhaitez tester les scripts que vous comptez exécuter, utilisez l'éditeur graphique PowerShell **powershell_is**. Vous devez aussi ajouter le fichier de configuration **powershell_ise.exe.config** au même dossier que le fichier de configuration **powershell.exe.config**.

REMARQUE : Le fichier de configuration **powershell_ise.exe.config** doit avoir le même contenu que celui du fichier **powershell.exe.config**.

PRÉCAUTION : Si le pré ou post-script PowerShell échoue, alors la tâche échouera aussi.

Paramètres d'entrée

Tous les paramètres d'entrée disponibles sont utilisés dans les échantillons de scripts. Ces paramètres sont décrits dans les tableaux suivants.

REMARQUE : Les fichiers de script doivent avoir le même nom que les fichiers d'échantillons de scripts.

Tableau 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Méthode	Description
`public uint MaxConcurrentStreams { get; set; }`	Obtient ou définit le nombre maximum de connexions TCP concurrentes que le core établira à l'agent pour le transfert de données.
`public uint MaxTransferQueueDepth { get; set; }`	Lorsqu'une plage de blocs est lue depuis un flux de transfert, cette place est placée dans une file d'attente de producteurs ou clients, où un fil client lit et l'écrit sur l'objet époque. Si le référentiel écrit plus lentement que le réseau lit, cette file d'attente se remplit. Le point auquel la file d'attente est pleine et où la lecture s'arrête est la profondeur maximale de file d'attente de transfert.
`public uint MaxConcurrentWrites { get; set; }`	Obtient ou définit le nombre maximal d'opérations d'écriture de blocs en attente sur une époque à tout moment. Si des blocs supplémentaires sont reçus lorsque ce nombre d'écritures de blocs sont en attente, ces blocs supplémentaires sont ignorés tant qu'une des écritures en cours n'est pas terminée.
`public ulong MaxSegmentSize { get; set; }`	Obtient ou définit le nombre maximal de blocs contigus à transférer en réponse à une unique requête. Selon les tests, des valeurs supérieures ou inférieures peuvent être optimales.
`public Priority Priority { get; set; }`	Obtient ou définit la priorité de requête de transfert.

Méthode	Description
`public int MaxRetries { get; set; }`	Obtient ou définit le nombre maximal de nouvelles tentatives de transfert après lesquelles il est présumé qu'il y a échec.
`public Guid ProviderId{ get; set; }`	Obtient ou définit le GUID du fournisseur VSS à utiliser pour les instantanés sur cet hôte. Habituellement, les administrateurs acceptent la valeur par défaut.
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	Obtient ou définit la collection d'ID de rédacteur VSS, qui est exclue de cet instantané. L'ID du rédacteur est déterminé par le nom du rédacteur. Ce nom, attribué à des fins de documentation uniquement, n'a pas besoin de correspondre exactement au nom du rédacteur.
`public ushort TransferDataServerPort { get; set; }`	Obtient ou définit la valeur contenant le port TCP sur lequel les connexions doivent être acceptées à partir du core pour le transfert réel de données de l'agent au core. L'agent tente d'écouter sur ce port, mais si celui-ci est en cours d'utilisation, l'agent peut utiliser un autre port. Le core utilise le numéro de port précisé dans les propriétés `BlockHashesUri` et `BlockDataUri` de l'objet `VolumeSnapshotInfo` pour chaque instantané de volume.
`public TimeSpan SnapshotTimeout { get; set; }`	Obtient ou définit le temps d'attente devant précéder l'abandon ou la temporisation d'une opération d'instantané VSS.
`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 des opérations d'écriture sur le réseau liées à ce transfert.

Tableau 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Méthode	Description
`public Guid AgentId { get; set; }`	Obtient ou définit l'ID de l'agent.
`public bool IsNightlyJob { get; set; }`	Obtient ou définit la valeur indiquant si la tâche en arrière-plan est une tâche nocturne.
`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.ChecksumChecks)

Hérite ses valeurs du paramètre `BackgroundJobRequest`.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Hérite ses valeurs du paramètre `BackgroundJobRequest`.

Méthode	Description
`public uint RamInMegabytes { get; set; }`	Obtient ou définit la taille de la mémoire pour la VM exportée. Définissez cette valeur sur zéro (0) pour utiliser la taille de la mémoire de la machine source.
`public VirtualMachineLocation Location { get; set; }`	Obtient ou définit l'emplacement de la cible de cette 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 à l'exportation de VM.
`public ExportJobPriority Priority { get; set; }`	Obtient ou définit la priorité de requête d'exportation.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Hérite ses valeurs du paramètre `BackgroundJobRequest`.

RollupJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Hérite ses valeurs du paramètre `BackgroundJobRequest`.

TakeSnapshotResponse (namespace Replay.Common.Contracts.Transfer)

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 sur l'instantané pour chaque volume inclus dans l'instantané

TransferJobRequest (namespace Replay.Common.Contracts.Transfer)

Hérite ses valeurs du paramètre `BackgroundJobRequest`.

Méthode	Description
`public VolumeNameCollection VolumeNames { get; set; }`	Obtient ou définit la collection des noms de volumes pour le transfert.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtient ou définit le type de copie pour le transfert. Les valeurs disponibles sont : `Inconnu`, `Copier` et `Saturé`.

Méthode	Description
`Public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtient ou définit la configuration du transfert.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtient ou définit la configuration du stockage.
`public string Key { get; set; }`	Génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier des requêtes de transfert.
`public bool ForceBaseImage { get; set; }`	Obtient ou définit la valeur indiquant si l'image de base a été forcée ou non.
`public bool IsLogTruncation { get; set; }`	Obtient ou définit la valeur indiquant si la tâche est une troncation de journal ou non.

Tableau 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.Transfer)

Méthode	Description
`public VolumeNameCollection VolumeNames { get; set; }`	Obtient ou définit la collection des noms de volumes pour le transfert.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtient ou définit le type de copie pour le transfert. Les valeurs disponibles sont : `Inconnu`, `Copier` et `Saturé`.
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtient ou définit la configuration du transfert.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtient ou définit la configuration du stockage.
`public string Key { get; set; }`	Génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier des requêtes de transfert.
`public bool ForceBaseImage { get; set; }`	Obtient ou définit la valeur indiquant si l'image de base a été forcée ou non.
`public bool IsLogTruncation { get; set; }`	Obtient ou définit la valeur indiquant si la tâche est une troncation de journal ou non.
`public uint LatestEpochSeenByCore { get; set; }`	Obtient ou définit la valeur de la dernière époque.
`public Guid SnapshotSetId { get; set; }`	Obtient ou définit le GUID attribué à cet instantané par VSS

Méthode	Description
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtient ou définit la collection des informations sur l'instantané pour chaque volume inclus dans l'instantané

Tableau 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.Transfer)

Méthode	Description
`public VolumeNameCollection VolumeNames { get; set; }`	Obtient ou définit la collection des noms de volumes pour le transfert.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtient ou définit le type de copie pour le transfert. Les valeurs disponibles sont : `Inconnu`, `Copier` et `Saturé`.
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtient ou définit la configuration du transfert.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtient ou définit la configuration du stockage.
`public string Key { get; set;}`	Génère une clé pseudo-aléatoire (mais non sécurisée cryptographiquement) pouvant être utilisée comme mot de passe unique pour authentifier des requêtes de transfert.
`public bool ForceBaseImage { get; set; }`	Obtient ou définit la valeur indiquant si l'image de base a été forcée ou non.
`public bool IsLogTruncation { get; set; }`	Obtient ou définit la valeur indiquant si la tâche est une troncation de journal ou non.
`public uint LatestEpochSeenByCore { get; set; }`	Obtient ou définit la valeur de la dernière époque.

Tableau 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Transfer)

Méthode	Description
`public string Description { get; set;}`	Obtient ou définit pour cet emplacement une description lisible par l'utilisateur.
`public string Method { get; set;}`	Obtient ou définit le nom de la VM.

VolumeImageIdsCollection (namespace Replay.Core.Contracts.Exchange.RecoveryPoints)

Hérite des valeurs du paramètre `System.Collections.ObjectModel.Collection<string>`.

Tableau 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

Méthode	Description
`public string GuidName { get; set;}`	Obtient ou définit l'ID du volume.
`public string DisplayName { get; set;}`	Obtient ou définit le nom de la VM.

Méthode	Description
`public string UrlEncode()`	Obtient une version encodée par URL du nom pouvant passer facilement 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'espace de chemin de fonctionner correctement dans un modèle d'URI. Étant donné qu'un nom de volume contient tant '\' que '?', vous devez remplacer les caractères spéciaux '\' et '?' 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>`.

Méthode	Description
`public override bool Equals(object obj)`	Détermine si cette instance et un objet spécifié, lequel doit également être un objet `volumeNameCollection`, ont la même valeur. (Remplace `Object.Equals(Object)`.)
`public override int GetHashCode()`	Retourne le code de hachage pour ce `VolumeNameCollection`. (Remplace `Object.GetHashCode()`.)

Tableau 11. VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer)

Méthode	Description
`public Uri BlockHashesUri { get; set;}`	Obtient ou définit l'URI sur laquelle les hachages MD5 des blocs de volumes peuvent être lus.
`public Uri BlockDataUri { get; set;}`	Obtient ou définit l'URI sur laquelle 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>`.

Pretransferscript.ps1

Le **PreTransferScript** s'exécute du côté de l'agent avant le transfert vers un instantané.

```
# 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

Le **PostTransferScript** s'exécute du côté de l'agent avant le transfert vers un instantané.

```
 # 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

Le **PreExportScript** s'exécute du côté du core avant toute tâche d'exportation.

```
# 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.StorageConfiguration
}
```

Postexportscript.ps1

Le **PostExportScript** s'exécute du côté du core avant toute tâche d'exportation.

REMARQUE : Il n'existe aucun paramètre d'entrée pour le **PostExportScript** lorsque celui-ci est exécuté une fois sur l'agent exporté suite au démarrage initial. L'agent normal contient ce script dans le dossier script, nommé PostExportScript.ps1.

```
# 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

Le **PreNightlyJobScript** est exécuté avant chaque tâche nocturne du côté du core. Il possède le paramètre **$JobClassName**, qui facilite le traitement de ces tâches enfant séparément.

```
 # 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 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                            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 'AgentId:' $RollupJobRequestObject.AgentId;
                    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 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                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

Le **PostNightlyJobScript** est exécuté après chaque tâche nocturne du côté du core. Il possède le paramètre **$JobClassName**, qui aide le traitement de ces tâches enfant séparément.

```
 # 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 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                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 'AgentId:' $RollupJobRequestObject.AgentId;
                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 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        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.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
```

```
        }
}
```

Modèles de scripts

Les modèles de script suivants sont fournis pour assister les utilisateurs administratifs dans l'exécution des scripts PowerShell.

Les modèles de scripts comprennent :

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

Obtention d'aide

Recherche de documentation et de mises à jour logicielles

Dans la console AppAssure Core, il existe des liens directs vers AppAssure, la documentation de l'appliance et les mises à jour logicielles. Pour accéder aux liens, cliquez sur l'onglet **Appliance**, puis cliquez sur **État global**. Les liens vers les mises à jour et la documentation se trouvent dans la section **Documentation**.

Contacter Dell

REMARQUE : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le borderau de colisage, la facture le catalogue des produits Dell.

Dell fournit plusieurs options de service et de support en ligne et par téléphone. Si vous ne disposez pas d'une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, facture ou catalogue de produits Dell. La disponibilité des produits varie selon le pays et le produit. Il se peut que certains services ne soient pas disponibles dans votre région.