Dell PowerVault DL4000 Backup To Disk Appliance
Guide d'utilisation - Pour les licences de capacité

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessure corporelle ou de mort.

2013 - 10

Rev. A02

Table des matières

1

Présentation d'AppAssure 5

Ce chapitre décrit les fonctions, la fonctionnalité et l'architecture d'AppAssure 5.

À propos d'AppAssure 5

AppAssure 5 définit une nouvelle norme pour la 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 infonuagiques.

AppAssure 5 combine la sauvegarde et la réplication en un seul produit de protection des données unifié et intégré. AppAssure 5 assure également la reconnaissance des applications pour garantir la fiabilité de la restauration des données d'application à partir de vos sauvegardes. AppAssure 5 repose sur True Scale™, nouvelle architecture en attente de brevet qui offre les performances de sauvegarde les plus rapides, avec des objectifs de temps de restauration (RTO) et de point de restauration (RPO) pratiquement égaux à zéro.

AppAssure 5 combine plusieurs technologies de pointe uniques et innovantes :

- Live Recovery
- Recovery Assure
- 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 et à des fonctions intégrées de déduplication, compression, chiffrement et réplication sur toute infrastructure dans un nuage privé ou public, AppAssure 5 peut rapidement traiter des pétaoctets de données. Les applications et données des serveurs peuvent être restaurées en quelques minutes à des fins de rétention des données (DR) et de conformité.

AppAssure 5 prend en charge les environnements à plusieurs hyperviseurs, y compris ceux qui fonctionnent sous VMware vSphere et Microsoft Hyper-V (qui constituent des clouds privés et publics). AppAssure 5 vous apporte des avances technologiques, tout en réduisant sensiblement les coûts de gestion informatique et de stockage.

Technologies AppAssure 5 Core

Live Recovery

AppAssure 5 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 AppAssure 5 enregistre des instantanés simultanés de plusieurs VM ou serveurs, offrant une protection quasi-instantanée des données et des systèmes. Vous pourrez reprendre l'utilisation du serveur directement depuis le fichier de sauvegarde sans attendre une restauration complète au 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 et RPO actuels toujours plus rigoureux.

Recovery Assure

AppAssure Recovery Assure 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 et 2012. Recovery Assure 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, ce qui 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 5, vous pouvez restaurer ou exporter de physique à cloud ou de virtuel à cloud.

Déduplication globale réelle

AppAssure 5 offre une fonction de déduplication réellement globale qui réduit de façon significative 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 AppAssure 5 True Scale

AppAssure 5 repose sur l'architecture AppAssure True Scale. Il 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. Il offre des RTO et RPO de quelques minutes sans nuire aux performances. Il comprend un gestionnaire d'objets et de volumes, qui intègre déduplication globale, compression, cryptage, réplication et 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 5 True Scale. Le magasin d'objets évolutif stocke des instantanés au niveau du bloc qui sont capturés 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 de données prend tout en charge simultanément avec des E/S asynchrones qui offrent un haut débit avec une latence minimale et optimise 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 AppAssure 5

AppAssure 5 est un produit de sauvegarde et 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 d'AppAssure 5 inclut la planification de la topologie de stockage du réseau, la planification de l'infrastructure de restauration du matériel du core et de restauration après sinistre ainsi que la planification de la sécurité.

L'architecture de déploiement d'AppAssure 5 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 dénommées agents. Le composant hors site est activé à l'aide de la réplication, pour fournir des fonctionnalités de restauration complète sur le site DR. AppAssure 5 Core utilise des images de base et des instantanés incrémentiels pour compiler les points de restauration des agents protégés.

De plus, AppAssure 5 reconnaît les applications car il 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. AppAssure 5 peut également tronquer les journaux des serveurs Microsoft Exchange et SQL Server protégés.

Le diagramme suivant illustre un déploiement AppAssure 5 simple. Dans ce diagramme, les agents AppAssure sont installés sur des machines comme le serveur de fichiers, le serveur d'e-mail, le serveur de base de données ou des machines virtuelles, et ils se connectent à un seul core AppAssure qui les protège et joue également le rôle de référentiel central. Le portail de licences AppAssure 5 gère les abonnements aux licences, les groupes et les utilisateurs des agents 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 agents et des cores en fonction des licences dont vous disposez pour votre environnement.

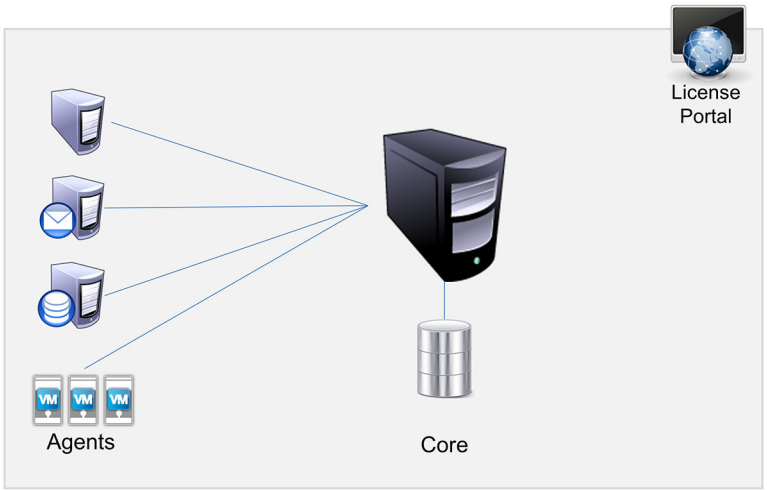

Figure 2. Architecture de déploiement AppAssure 5 de base

Vous pouvez également déployer plusieurs cores AppAssure comme le montre le diagramme suivant. Une console centrale gère plusieurs cores.

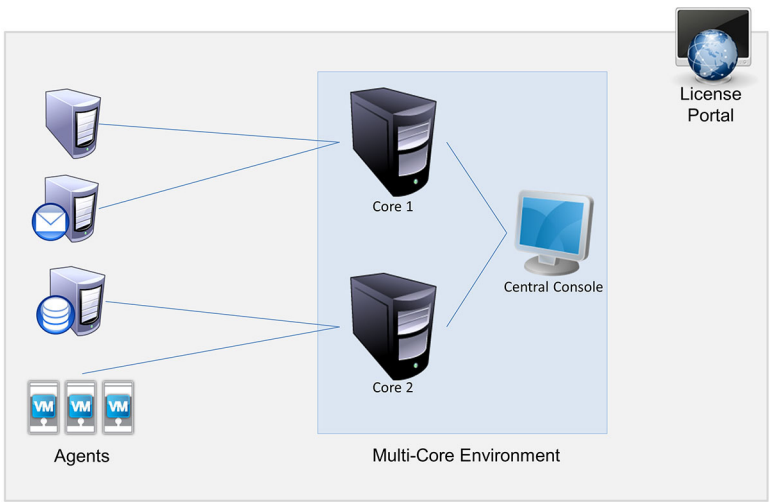

Figure 3. Architecture de déploiement AppAssure 5 avec plusieurs cores

AppAssure 5 Smart Agent

L'AppAssure 5 Smart Agent s'installe sur les ordinateurs protégés par l'AppAssure 5 Core. Le Smart Agent fait le suivi des blocs modifiés sur le volume de disque puis prend un instantané de l'image des blocs modifiés à un intervalle de protection prédéfini. Les instantanés incrémentiels au niveau du bloc évitent à l'utilisateur d'avoir à copier de façon répétée les mêmes données depuis l'ordinateur protégé vers le Core. Le Smart Agent reconnaît les applications et reste

dormant lorsque vous ne l'utilisez pas, son pourcentage d'utilisation de l'unité centrale étant pratiquement de zéro (0) pour cent et son utilisation de la mémoire de 20 Mo. Lorsque le Smart Agent est actif, il utilise jusqu'à 2 à 4 pour cent de l'UC et moins de 150 Mo de mémoire, ce qui couvre le transfert des instantanés au Core. Ces valeurs sont bien inférieures à celles des programmes logiciels hérités qui utilisent beaucoup plus de l'UC et de la mémoire, même lorsqu'ils sont dormants.

L'AppAssure 5 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 journalise ensemble 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'instantanéest est prêt, il est rapidement transféré à l'AppAssure 5 Core à l'aide de connexions à base de socket intelligentes multithreads. Pour conserver la bande passante de l'UC et la mémoire sur les ordinateurs protégés, le smart agent ne chiffre pas et ne déduplique pas les données à la source et les ordinateurs et agents sont associés à un core à des fins de protection.

AppAssure 5 Core

L'AppAssure 5 Core est le composant central de l'architecture de déploiement AppAssure 5. Le core stocke et gère toutes les sauvegardes de l'ordinateur et fournit des services de core pour la sauvegarde, la restauration et la rétention, la réplication, l'archivage et la gestion. Le core est un ordinateur autonome adressable sur un réseau qui exécute une variante 64 bits du système d'exploitation Microsoft Windows. AppAssure 5 effectue la compression inline à base cible, le chiffrement et la déduplication des données reçues de l'agent. Le core stocke ensuite les sauvegardes d'instantanés dans un référentiel, qui peut résider sur diverses technologies de stockage telles que SAN (Storage Area Network), DAS (Direct Attached Storage) ou NAS (Network 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 API REST. 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 (mis en paire) à un autre core pour la réplication.

Processus d'instantané

Le processus de protection AppAssure commence par le transfert d'une image de base depuis une machine d'agent vers le core (seul moment où le système doit transporter une copie complète de la machine sur le réseau, dans des conditions de fonctionnement normal), suivi par des instantanés incrémentiels pendant tout le reste de la durée de vie du système. L'agent AppAssure 5 pour Windows utilise le service de copie fantôme de volume Microsoft (Volume Shadow Copy Service, VSS) pour geler les données d'application et les figer sur le disque, afin de capturer une sauvegarde cohérente avec le système d'exploitation et avec les applications. Lorsqu'un instantané est créé, le service d'écriture VSS du serveur cible interdit l'écriture de contenu sur le disque. Pendant ce processus de suspension de l'écriture du contenu sur le disque, toutes les E/S de disque sont mises en file d'attente ; elles reprennent uniquement quand l'instantané est terminé, alors que les opérations déjà en cours sont terminées et que tous les fichiers ouverts sont fermés. Le processus de création d'une copie fantôme 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 Server 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 endommagées sur disque pour placer la base de données dans un état de transaction cohérent. Attention, notez bien 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 AppAssure 5 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 est créé au niveau du volume.

Réplication - Site de restauration après sinistre ou fournisseur de services

Le processus de réplication dans AppAssure exige une relation source-cible associés entre deux cores. Le core source copie les points de restauration des agents protégés, puis les transmet de façon synchrone et continue à un core cible dans un site de restauration 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, AppAssure 5 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 ordinateurs basculés. Suite à la restauration du site principal, le core répliqué peut restaurer automatiquement des données à partir des instances restaurées sur les agents du site principal.

Restauration

La restauration peut être réalisée au site local ou au site à distance répliqué. Une fois le déploiement en état stable avec une protection locale et une réplication optionnelle, l'AppAssure 5 Core vous permet de réaliser une restauration à l'aide de Recovery Assure, Universal Recovery ou Live Recovery.

Fonctionnalités produit d'AppAssure 5

Grâce à AppAssure 5, vous pouvez gérer toutes les facettes de la protection et de la restauration des données critiques en utilisant les fonctions et fonctionnalités suivantes.

- Référentiel
- Déduplication globale réelle
- Chiffrement
- Réplication
- RaaS (Restauration en tant que service)
- Rétention et archivage
- Virtualisation et nuage
- Alertes et gestion des événements
- Portail de licences AppAssure 5
- Console Web
- API de gestion des services
- Marquage blanc

Référentiel

Le référentiel utilise le DVM (Deduplication Volume Manager, 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 stockages 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 AppAssure 5 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 AppAssure exécute des sauvegardes incrémentielles des machines, au niveau du bloc, à perpétuité. 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

AppAssure 5 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 qu'AppAssure exécute des sauvegardes incrémentielles des machines au niveau du bloc, sans date de fin. Cette approche incrémentielle en continu, alliée à la déduplication des données vous aide à réduire de façon significative la quantité totale de données validées sur le disque ; le taux de réduction peut atteindre 80:1.

Cryptage

AppAssure 5 fournit un cryptage intégré qui protège les sauvegardes et les données en attente de tout accès ou utilisation non autorisé, ce qui garantit la confidentialité des données. AppAssure 5 fournit un cryptage puissant ; ainsi, les sauvegardes des machines protégées sont inaccessibles. Seul l'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 (Deduplication Volume Manager, Gestionnaire de volume de déduplication) 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, AppAssure 5 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 un processus de copies de points de restauration et de transmission de ceux-ci vers un deuxième emplacement dans le but d'une restauration en cas d'urgence. Le processus exige une relation en paire source-cible entre deux cores. La réplication est gérée pour chaque machine protégée ; ce qui veut dire que les instantanés de sauvegarde d'une machine protégée sont répliqués vers un core de réplique cible. Lorsque la réplication est définie, le core source transmet de manière asynchrone et continue les données d'instantané incrémentielles vers le core cible. Vous pouvez configurer cette réplication sortante vers le centre de données de votre société ou le site distant de restauration en cas d'urgence (c'est-à-dire un core cible « auto-géré ») ou vers un MSP (Managed Service Provider - Fournisseur de services gérés) offrant des services de sauvegarde hors site et de restauration en cas d'urgence. Lorsque vous procédez à une réplication vers un MSP, vous pouvez utiliser des flux de travail intégrés qui vous permettent de demander des connexions et de recevoir des notifications signalant des problèmes automatiquement.

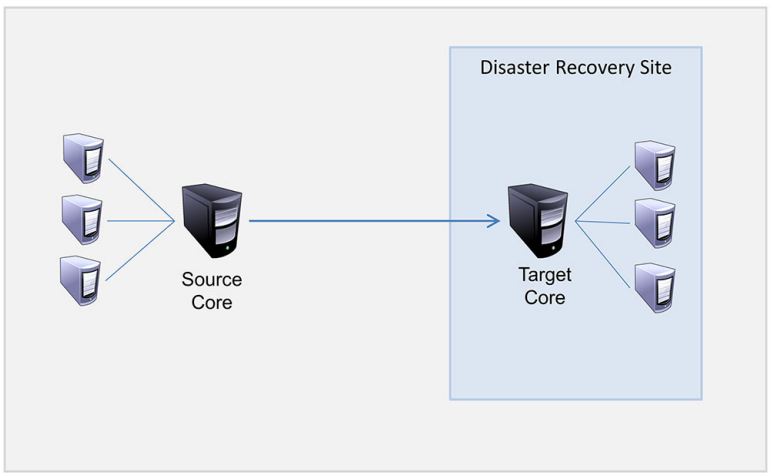

Figure 5. Architecture de réplication de base

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 la création de données de départ, à savoir le transfert initial d'images de base dédupliquées et d'instantanés incrémentiels d'agents protégés ; cela peut représenter des centaines ou des milliers de gigaoctets de données. Les données de départ de la réplication peuvent être créées sur le core cible à l'aide de supports externes. En général, cela s'avère utile pour les ensembles de données volumineux ou les sites avec liaisons lentes. Les données d'une archive de départ sont compressées, cryptées et dédupliquées. Si la taille totale de l'archive est supérieure à l'espace disponible sur le support amovible, l'archive peut être fractionnée sur plusieurs périphériques, selon l'espace disponible sur le support. Pendant le processus de création des données de départ, les points de

restauration incrémentiels sont répliqués sur le site cible. Une fois que le core cible a fini de consommer l'archive de départ, les points de restauration incrémentiels répliqués se synchronisent automatiquement.

RaaS (Restauration en tant que service)

Les MSP (Managed Service Providers - Fournisseurs de services gérés) peuvent tirer profit d'AppAssure 5 en tant que plateforme de RaaS (Restauration en tant que service). RaaS permet une restauration complète 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 ordinateurs protégés 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 5 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

Dans AppAssure 5, les stratégies de sauvegarde et de rétention sont flexibles 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 dans 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 en argent. 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.

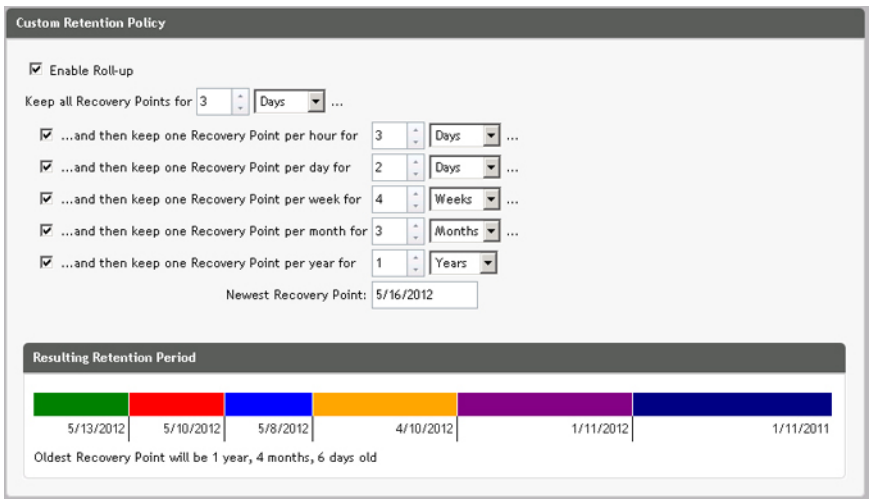

Figure 6. Stratégie de rétention personnalisée

Dans AppAssure 5, 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 approchent la fin de leur période de rétention, ils 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.

AppAssure 5 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, AppAssure 5 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, chiffrées et dédupliquées. Si la totalité de l'archive est supérieure à l'espace disponible du support amovible, l'archive s'étend sur plusieurs périphériques en fonction de l'espace disponible du support. L'archive peut aussi être verrouillé 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 chiffrement.

Virtualisation et cloud

L'AppAssure 5 Core est prêt pour le cloud, vous permettant de tirer profit de la capacité de calcul du cloud pour la restauration.

AppAssure 5 peut exporter toute machine protégée ou répliquée vers des versions de VMware ou Hyper-V sous licence. Les exportations peuvent se faire de façon ponctuelle ou 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 mis sous tension en un seul clic. Les exportations prises en charge sont :

- VMware Workstation ou Server dans un dossier
- Exportation directe vers un hôte ESXi Vsphere ou VMware, Microsoft Server 2008 R2 Hyper-V et Microsoft Server 2012 Hyper-V

Alertes et gestion des événements

En plus de HTTP REST API, AppAssure 5 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 Windows et 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'un environnement Windows uniquement, seul le Journal d'événements Windows est utilisé.

Portail de licences AppAssure 5

Le Portail de licences AppAssure 5 offre des outils de gestion de droits de licence faciles à utiliser. Vous pourrez 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

AppAssure 5 comprend une nouvelle console centrale sur le Web qui gère les cores AppAssure 5 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. L'AppAssure 5 Central Management Console (CMC - Console de gestion centrale) 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

AppAssure 5 est livré avec une API de gestion des services et fournit un accès programmé à toutes les fonctionnalités disponibles au moyen de la console AppAssure 5 Central Management. 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 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. AppAssure 5 est aussi livré avec un client SDK pour l'écriture de scripts PowerShell.

Marquage blanc

Le marquage d'AppAssure 5 peut également être modifié et il peut porter un marquage blanc pour certains partenaires OEM et partenaires d'entreprises dans le cadre du programme de fournisseurs de services Platine. Ce programme permet aux partenaires de marquer AppAssure 5 de leurs nom, logo et couleurs personnalisés et de livrer le produit ou service portant leur marque et présentant un aspect particulier à leur clientèle.

En tant que partenaire AppAssure, vous pouvez personnaliser le logiciel pour satisfaire aux exigences de votre entreprise. Pour explorer davantage la manière de marquer AppAssure 5 afin de répondre aux besoins de votre entreprise, contactez le service AppAssure Sales à l'adresse **sales@appassure.com** pour plus d'informations.

2

Gestion des licences AppAssure 5

Ce chapitre explique comment accéder aux licences de produit et les gérer depuis le portail de licences AppAssure 5.

À propos du portail de licences AppAssure 5

Le portail de licences AppAssure 5 vous permet de télécharger des logiciels et de gérer les abonnements aux licences. Depuis le portail de licences, vous pouvez ajouter des agents AppAssure 5, gérer les groupes, suivre les activités des groupes, inscrire des machines, créer des comptes, inviter des utilisateurs et générer des rapports.

À propos de la navigation dans le portail de licences

La première fois que vous vous connectez au portail de licences, un assistant vous guidera au cours de toutes les étapes de déploiement d'AppAssure 5. Lors des connexions qui suivront, si vous avez spécifié que vous ne vouliez pas voir l'Assistant, la page **Accueil Portail de licences** s'affiche sur le tableau de bord.

Dans le coin supérieur droit des pages du Portail de Licences, cliquez sur les liens de navigation pour accéder aux fonctions décrites dans le tableau suivant.

Lien de navigation	Description
Accueil	Fournit un lien vers la page d'Accueil du Portail de licences et vers le tableau de bord qui présente les informations d'état concernant les ordinateurs protégés dans votre environnement, fournit l'accès aux groupes et fournit l'accès aux rapports sur les licences et les ordinateurs.
Nom d'utilisateur	Affiche les prénom et nom de l'utilisateur connecté au portail de licences; fournit également un lien d'accès aux Paramètres personnels pour modifier les informations sur l'utilisateur ainsi que les références de connexion, telles que l'adresse électronique et le nom d'utilisateur. Depuis ce lien, vous pouvez accéder à l'Assistant Configuration du Portail de licences.
Contact	Affiche une boîte de dialogue qui contient les coordonnées de contact de Dell AppAssure.
Aide	Permet d'accéder à la documentation AppAssure 5.
Déconnexion	Vous déconnecte de la session sur le portail de licences et supprime la session du serveur.

À propos du License Portal Server

Le License Portal Server (serveur de Portail de licences) est un portail Web qui réside à un emplacement d'hébergement géré et offre support et disponibilité 24 heures sur 24.

Le License Portal Server contrôle l'accès aux téléchargements de produits et vous permet de suivre les déploiements, d'afficher les rapports et de gérer les clés de licences.

Le flux général du portail est le suivant :

- Vous vous inscrivez sur le portail de licences et créez un compte.
- Au cours de l'inscription, le portail de licences crée automatiquement un groupe racine par défaut pour le compte et lui attribue un nom.
- Lorsque vous vous connectez au portail de licences, ce dernier vous représente sous forme d'un compte pour cette session.
- Une arborescence de navigation contenant vos groupes s'affiche sur la droite de la page d'accueil du portail de licences. Vous pouvez utiliser les groupes pour afficher tous les cores et les agents lorsque vous vous connectez au portail de licences.

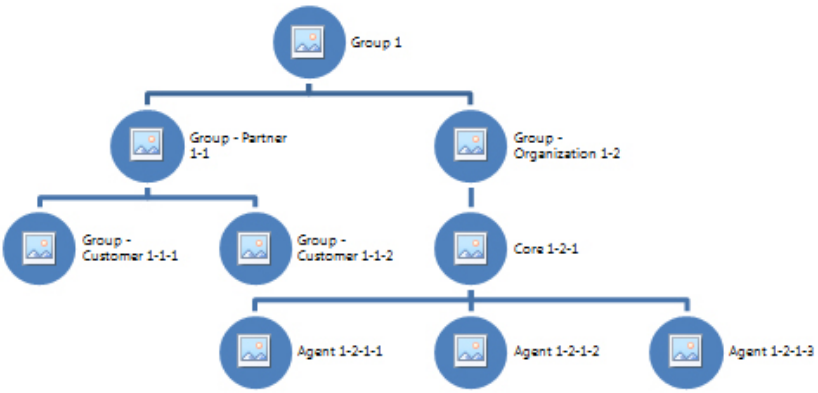

Figure 7. Portail de licences AppAssure 5 : compte et exemple de création de groupe

- Un fournisseur de services gérés peut créer des groupes distincts pour chacun de ses clients, puis créer des sous-groupes pour mieux séparer les agents et les cores.
- Pour la gestion des clients, vous pouvez générer des rapports pour chaque compte afin d'afficher différentes statistiques.

À propos des comptes

Lorsqu'ils sont connectés, les utilisateurs sont désignés comme des comptes dans le portail de licences. Les comptes représentent le groupe principal de l'utilisateur et les utilisateurs ont des droits d'accès aux groupes. Les sous-groupes héritent des droits d'accès correspondants d'un utilisateur.

Dans le portail de licences AppAssure 5, les droits d'utilisateur sont les suivants :

Admin	Contrôle complet pour la création, la modification et la suppression d'utilisateurs, de groupes, de cores et d'agents.
Lecture seule	Droits d'accès en lecture sur toutes les informations du portail de licences, notamment les groupes, les cores, les agents, les licences, etc.
Afficher uniquement les groupes	Affiche uniquement les informations sur les groupes. Toutes les informations sur le client sont limitées et sont ainsi inaccessibles.

Enregistrement de votre appliance sur le Portail de licences

Vous devez enregistrer votre appliance sur le Portail de licences Dell AppAssure.

Enregistrement de votre appliance sur le Portail de licences existant

Pour inscrire votre appliance si vous possédez un compte sur le portail de licences :

1. Sur votre navigateur Web, entrez **https://appliance.licenseportal.com/**.
   La page **Bienvenue sur le portail de licences Dell AppAssure** s'affiche.
2. Dans le champ **Adresse e-mail**, entrez l'adresse e-mail que vous avez utilisée pour créer un compte sur le portail de licences.
3. Dans le champ **Numéro de service**, entrez le numéro de service de votre appliance.
4. Pour ajouter des numéros de service supplémentaires, cliquez sur **Vous avez d'autres appliances ? Cliquez ici**.
5. Cliquez sur **Vérifier**.
   L'écran Connexion apparaît.
6. Entrez le nom d'utilisateur et le mot de passe de votre compte de Portail de licences, puis cliquez sur **Suivant**.
   La clé de licence s'affiche, avec les instructions nécessaires pour l'appliquer à la console AppAssure 5 Core.
7. Cliquez sur **Terminer**.

Enregistrement de votre appliance lorsque vous ne disposez pas d'un compte de Portail de licences

Vous devez enregistrer votre appliance sur le Portail de licences Dell AppAssure.

Pour enregistrer votre appliance si vous ne disposez pas d'un compte de Portail de licences:

1. Sur votre navigateur Web, entrez **https://appliance.licenseportal.com/**.
   La page **Bienvenue sur le portail de licences Dell AppAssure** s'affiche.
2. Dans le champ **Adresse e-mail**, entrez l'adresse e-mail que vous avez utilisée pour créer un compte sur le portail de licences.
3. Dans le champ **Numéro de service**, entrez le numéro de service de votre appliance.
4. Pour ajouter des numéros de service supplémentaires, cliquez sur **Vous avez d'autres appliances ? Cliquez ici**.
5. Cliquez sur **Vérifier**.
   Si l'adresse e-mail que vous avez entrée n'est pas inscrite sur le portail de licences, vous êtes invité à créer un compte sur le portail de licences à l'aide de l'adresse e-mail fournie.
   L'écran d'informations du compte s'affiche.
6. Créez un compte sur le portail de licences à l'aide de l'adresse e-mail entrée plus tôt.
   Pour plus d'informations sur la création d'un compte sur le portail de licences, voir Enregistrement pour un compte de Portail de licences.
   Une fois le compte de Portail de licences créé, un message d'activation est envoyé à votre adresse électronique.
7. Cliquez sur le lien situé dans le message d'activation.
   La boîte de dialogue Modifier le mot de passe apparaît.
8. Dans le champ **Mot de passe**, entrez un mot de passe pertinent.
9. Sous **Saisir le mot de passe à nouveau**, saisissez le mot de passe que vous venez de saisir dans **Mot de passe**.
10. Cliquez sur **Activer le compte**.
    La clé de licence s'affiche, avec les instructions nécessaires pour l'appliquer à la console AppAssure 5 Core.
11. Cliquez sur **Terminer**.

Enregistrement pour un compte de Portail de licences

Si vous n'avez pas actuellement de compte de Portail de licences, enregistrez-vous pour un compte d'accès au Portail de licences AppAssure 5.

Un compte d'utilisateur initial créé dans le portail de licences est créé en tant qu'utilisateur par défaut possédant des droits d'administrateur. Ce compte est également associé au groupe racine, ce qui signifie qu'il peut posséder des sous-groupes mais pas de « groupe parent ».

Le nouveau compte possède une licence d'évaluation. Par conséquent, tous les comptes, sous-groupes et agents ajoutés à ce compte possèdent également des licences d'évaluation jusqu'à ce qu'une licence complète soit activée. Seuls les utilisateurs dotés du rôle d'administrateur peuvent changer le type de licence d'un compte et activer la fonction qui permet l'ajout d'agents autres que les versions d'évaluation.

Pour s'enregistrer pour un compte de portail de licences :

1. Sur l'écran de connexion au **Portail de licences**, cliquez sur le lien pour vous enregistrer et créer un compte.
   La page **Inscription** s'affiche.
2. Entrez les détails d'inscription du compte comme indiqué dans le tableau suivant :

Champ	Description
Prénom	Entrez le prénom de l'utilisateur. **REMARQUE :** Cette entrée est obligatoire.
Nom	Entrez le nom de famille de l'utilisateur. **REMARQUE :** Cette entrée est obligatoire.
Adresse e-mail	Entrez une adresse e-mail unique pour l'utilisateur. **REMARQUE :** L'adresse e-mail doit être unique et ne peut pas avoir été utilisée préalablement pour une inscription sur le portail de licences. Cette entrée est obligatoire.
Société	Entrez le nom de la société avec laquelle l'utilisateur est associé. **REMARQUE :** Cette entrée est obligatoire.
Téléphone	Entrez le numéro de téléphone de ce compte d'utilisateur. Il servira à enregistrer les coordonnées de l'utilisateur.
Adresse :	Entrez une adresse pour le compte d'utilisateur.
Pays	Sélectionnez un pays. **REMARQUE :** Si vous choisissez les États-Unis, vous devez préciser un état.
État	Sélectionnez un état pour le compte d'utilisateur si vous avez sélectionné les États-Unis comme pays.
(Ville)	Entrez une ville pour le compte d'utilisateur.
Code postal	Entrez un code postal pour le compte d'utilisateur.

3. Pour recevoir des offres promotionnelles et des mises à jour, cochez la case **Me tenir informé(e) des offres spéciales**.

4. Cliquez sur **Enregistrer**.

   Un message s'affiche ; il confirme l'inscription et vous demande de vérifier vos e-mails pour consulter les instructions d'activation de votre compte.

Connexion au portail de licences AppAssure 5

Si vous avez déjà un compte dans le portail de licences AppAssure 5, il vous suffit d'entrer votre ID utilisateur (par exemple, votre adresse e-mail et votre mot de passe) pour vous connecter. L'option **Garder ma session active** vous permet d'enregistrer vos détails pour que vous puissiez vous connecter facilement au portail de licences lorsque vous y retournez. Vos références de connexion sont conservées pendant un maximum de 24 heures.

Si vous oubliez vos références de connexion, vous pouvez réinitialiser votre mot de passe en cliquant sur le lien **Vous avez oublié votre mot de passe ?**. Vous recevrez un nouveau mot de passe à l'adresse e-mail associée à votre compte.

REMARQUE : Si vous n'êtes pas inscrit sur le portail de licences, vous devez le faire pour obtenir une clé de licence et télécharger le logiciel. Pour plus d'informations sur l'inscription de votre appliance, voir Enregistrement de votre appliance sur le Portail de licences.

Pour vous connecter au portail de licences AppAssure 5 :

1. Naviguez jusqu'au portail de licences à l'adresse **https://licenseportal.com**.

   L'écran **Accueil** s'affiche.
2. Entrez votre ID utilisateur dans la zone de texte **ID utilisateur**.
3. Dans la zone de texte **Mot de passe**, entrez le mot de passe défini lors du processus d'inscription.

   REMARQUE : Si vous avez oublié votre mot de passe, cliquez sur **Vous avez oublié votre mot de passe ?** Vous recevrez un nouveau mot de passe à l'adresse e-mail fournie lors de la création du compte.
4. Cliquez sur **Garder ma session active** pour être automatiquement connecté à votre compte lors de vos futures sessions.

   REMARQUE : Les détails utilisateur sont conservés pendant 24 heures.
5. Cliquez sur **Ouvrir une session**.

Utilisation de l'Assistant Portail de licences

Vous pouvez utiliser l'Assistant Portail de licences pour installer les nouveaux cores, ajouter des groupes et des sous-groupes et inviter des utilisateurs.

1. Sur la page d'**Accueil** de l'**Assistant Configuration**, cliquez sur **Installer de nouveaux cores**.

   La page **Navigation dans le Portail de licences** qui s'affiche décrit la facon de naviguer dans le portail de licences.
2. Cliquez sur **Suivant**.

   La page **Groupes** s'affiche.
3. Pour ajouter un nouveau groupe, cliquez sur **Ajouter un groupe** pour ajouter un sous-groupe à votre organisation.

   Le terme organisation désigne la société que vous avez saisie lorsque vous avez enregistré votre compte. Les sous-groupes représentent les partenaires, d'autres sociétés et d'autres services de votre société.
4. Dans la page **Ajout d'un sous-groupe**, entrez un **nom de groupe** et une **description** pour le sous-groupe.

   REMARQUE : Le **Nom de groupe** est requis.
5. Cliquez sur **Add** (Ajouter).
6. Dans la page **Ajouter un groupe**, cliquez sur **Suivant**.

   La page **Utilisateurs** s'affiche.

7. Si vous souhaitez inviter et ajouter des utilisateurs à vos groupes, sélectionnez le groupe ou sous-groupe auquel l'utilisateur doit être ajouté, puis cliquez sur **Inviter l'utilisateur**.

   REMARQUE : Un utilisateur « invité » reçoit une notification par e-mail qui inclut des informations de connexion, notamment un nom d'utilisateur, un mot de passe et un lien vers le **Portail de licences**.

8. Dans la page **Invitation d'un utilisateur**, entrez le **prénom**, le **nom** et l'**ID utilisateur** (c'est-à-dire l'adresse e-mail) de l'utilisateur.

9. Sous **Droits d'utilisateur**, sélectionnez le type de droits dont cet utilisateur a besoin.

   Vous pouvez sélectionner l'une des options suivantes :

Admin	Contrôle complet pour la création, la modification et la suppression d'utilisateurs, de groupes, de cores et d'agents.
Lecture seule	Droits d'accès en lecture sur toutes les informations du portail de licences (à l'exception de la liste des utilisateurs et de la clé de licence).
Afficher uniquement les groupes	Droits d'accès en lecture uniquement aux informations sur les groupes. Toutes les informations des clients sont restreintes et donc inaccessibles.

10. Cliquez sur **Add** (Ajouter).

11. Dans la page **Utilisateurs**, cliquez sur **Suivant**.

12. Dans la page **Téléchargements**, sélectionnez le groupe pour lequel installer et ajouter le logiciel AppAssure 5, puis cliquez sur **Télécharger**.

    REMARQUE : Vous devez disposer de droits d'administration pour télécharger et ajouter des logiciels.

    La page est actualisée avec la liste des téléchargements disponibles.

13. En regard du progiciel à télécharger, cliquez sur **Télécharger**.

    REMARQUE : Vous pouvez télécharger une version du progiciel d'installation de Core afin de l'installer sur votre machine locale ou préférer un programme d'installation Web que vous exécutez directement depuis le Web. Le progiciel d'installation télécharge le fichier exécutable en une seule tâche, alors que le programme d'installation Web diffuse en continu un téléchargement de la version la plus récente d'AppAssure 5 Core, et vous permet de suspendre et de reprendre le processus selon vos besoins. Pour l'agent, vous pouvez choisir le type de machine Windows voulu (x64 ou x86). Des programmes d'installation d'agent sont également disponibles pour plusieurs versions de Linux.

14. Une fois que vous avez téléchargé les programmes d'installation nécessaires, cliquez sur **Terminer**.

    REMARQUE : Par défaut, le logiciel que vous téléchargez est valide pendant 14 jours. Si vous êtes un nouveau client, votre licence est automatiquement activée par Dell AppAssure. Après avoir téléchargé le programme d'installation avec succès, vous recevez un e-mail contenant votre clé de licence.

15. Dans la page **Téléchargements**, cliquez sur **Suivant**.

    La **page Ressources et support** s'affiche. Cette page vous permet de consulter des informations concernant la façon de prendre contact avec le support Dell AppAssure (ou avec le propriétaire ou l'administrateur du groupe). Elle contient aussi des informations expliquant comment obtenir de l'aide pour l'utilisation d'AppAssure 5.

16. Si vous ne voulez plus afficher cet Assistant, sélectionnez **Ne pas afficher cet Assistant à la prochaine connexion**.

    Si vous sélectionnez cette option, la page **Accueil du Portail de licences** s'affiche à la prochaine connexion.

17. Cliquez sur **Terminer** pour fermer l'Assistant.

Ajout d'un core au portail de licences

L'AppAssure 5 Core, installé sur un serveur dédié, stocke et gère les sauvegardes de toutes les machines protégées dans votre environnement.

REMARQUE : Seuls les utilisateurs possédant des droits d'administrateur peuvent télécharger un core.

Pour ajouter un AppAssure Core au Portail de licences :

1. Sur la page d'**Accueil du portail de licences d'AppAssure 5**, sélectionnez un groupe, puis cliquez sur **Télécharger AppAssure 5**.
   La boîte de dialogue **Télécharger AppAssure 5** s'ouvre.
2. Choisissez **Télécharger le programme d'installation** ou **Télécharger le programme d'installation Web**.

   REMARQUE : Le programme d'installation télécharge le fichier exécutable en une seule tâche, alors que le programme d'installation Web diffuse en continu la version la plus récente version d'AppAssure 5 Core et vous permet de suspendre ou de reprendre le processus, selon vos besoins. Une clé de licence est générée automatiquement et vous est transmise pour que vous la saisissiez afin d'activer l'abonnement. La clé de licence s'affiche dans l'e-mail de confirmation que vous recevez après avoir choisi votre option de téléchargement.
3. Pour installer le logiciel, cliquez sur **Exécuter** dans les boîtes de dialogue qui suivent.

   REMARQUE : Une fois l'installation automatique du fichier exécutable du Core terminée, l'écran d'**Accueil** s'affiche.

Ajout d'un agent à l'aide du portail de licences

REMARQUE : Vous devez disposer de droits d'administration pour télécharger et ajouter des agents.

Pour ajouter un agent :

1. Dans l'écran d'**Accueil du portail de licences d'AppAssure 5**, sélectionnez un groupe, puis cliquez sur **Télécharger un agent**.
   La boîte de dialogue **Télécharger un agent** s'affiche.
2. Cliquez sur **Télécharger**, en regard de la version du programme d'installation à télécharger.
   Choisissez parmi les options suivantes :
   - Programme d'installation Windows 32 bits
   - Programme d'installation Windows 64 bits
   - Programme d'installation Red Hat Enterprise Linux 6.3 32 bits
   - Programme d'installation Red Hat Enterprise Linux 6.3 64 bits
   - Programme d'installation CentOS 6.3, 6.4 32 bits
   - Programme d'installation CentOS 6.3, 6.4 64 bits
   - Programme d'installation Ubuntu 12.04 LTS, 13.04 32 bits
   - Programme d'installation Ubuntu 12.04 LTS, 13.04 64 bits
   - Programme d'installation SUSE Linux Enterprise Server 11 SP2 32 bits
   - Programme d'installation SUSE Linux Enterprise Server 11 SP2, SP3 64 bits
   - Microsoft Hyper-V Server 2012

REMARQUE : Nous prenons en charge ces distributions Linux et avons effectué des tests sous la plupart des versions de noyau publiées.

REMARQUE : Les agents installés sur Microsoft Hyper-V Server 2012 fonctionnent en mode d'édition Core de Windows Server 2012.

Le fichier **Agent** se télécharge.

3. Cliquez sur **Exécuter** dans la boîte de dialogue **Programme d'installation**.

REMARQUE : Pour en savoir plus sur l'ajout d'agents à l'aide de l'ordinateur Core, voir Déploiement d'un agent (Installation Pousser) dans le *Guide d'utilisation de Dell PowerVault DL4000* sur **dell.com/support/manuals**.

Configuration des paramètres personnels

Vous pouvez personnaliser vos paramètres personnels selon les exigences de votre entreprise et vos préférences personnelles depuis la section **Paramètres personnels** de l'écran **Profil de compte**. Par exemple, vous pouvez gérer votre adresse e-mail, votre nom, etc.

Pour configurer les paramètres personnels :

1. Sur la page d'**Accueil du Portail de licences AppAssure 5**, cliquez sur votre nom d'utilisateur, puis cliquez sur les **Paramètres personnels** .

   La page **Profil de compte** s'affiche et l'onglet **Paramètres personnels** s'ouvre.
2. Pour modifier votre **ID d'utilisateur**, cliquez sur **Modifier** en regard de votre ID d'utilisateur.
3. Dans le champ **Prénom**, modifiez votre prénom, si nécessaire.
4. Dans le champ **Nom de famille**, modifiez votre nom de famille, si nécessaire.
5. Dans le menu **Langue**, sélectionnez la langue par défaut pour ce compte.
6. (Facultatif) Dans la zone de texte **Commentaires**, vous pouvez saisir une description pour le compte.
7. (Facultatif) Sélectionnez **Mettre à jour l'onglet Cores toutes les : x minutes** pour spécifier une fréquence de mise à jour des informations d'un groupe.

   REMARQUE : Si vous sélectionnez l'option **Mettre à jour l'onglet Core toutes les : x minutes**, vous devez préciser le nombre de minutes nécessaires pour la mise à jour des informations de l'onglet Core.
8. (Facultatif) Sélectionnez **Me tenir informé des offres spéciales** afin de recevoir nos promotions par e-mail.
9. (Facultatif) Sélectionnez **Invite au groupe lors de l'addition d'un core** afin qu'une invite s'affiche, demandant à l'utilisateur d'attribuer un groupe au Core nouvellement ajouté.
10. Cliquez sur **Enregistrer**.

Configuration des paramètres de notification par e-mail

La page **Profil du compte** vous permet de modifier les paramètres de notification par e-mail d'un compte d'utilisateur, notamment le moment où vous souhaitez être averti par e-mail lorsqu'un événement particulier se produit.

Pour configurer les paramètres privés de sécurité :

1. Dans la page d'**Accueil du portail de licences AppAssure 5**, cliquez sur votre nom d'utilisateur, puis cliquez sur **Paramètres privés**.

   La page **Profil du compte** s'affiche.
2. Cliquez sur l'onglet **Notifications par e-mail**.
3. Pour que votre compte reçoive une notification lorsqu'un événement se produit, sélectionnez les options de sécurité voulues.

Vous pouvez choisir parmi les options suivantes :

- **L'adresse e-mail de mon compte a changé**
- **Mon mot de passe a été modifié**
- **Échec de la tentative de connexion au compte**
- **J'ai pu me connecter à mon compte avec succès**
- **Un core a été ajouté**
- **Un core a été supprimé**
- **Un core a été téléchargé**
- **Une machine a été ajoutée**
- **Une machine a été supprimée**
- **Un utilisateur a été ajouté**
- **Un utilisateur a été supprimé**
- **Un groupe a été ajouté**
- **Un groupe a été supprimé**
- **J'ai été nommé propriétaire du groupe**

4. Cliquez sur **Enregistrer**.

Modification de votre mot de passe de Portail de licences AppAssure

Vous pouvez modifier le mot de passe de votre compte en utilisant l'onglet **Modifier le mot de passe** dans la page **Profil du compte** .

Pour modifier votre mot de passe :

1. Sur la page **Accueil du Portail de licences AppAssure 5**, cliquez sur votre nom d'utilisateur, puis sur **Paramètres personnels**.

   La page **Profil du compte** s'affiche.

2. Cliquez sur l'onglet **Modifier le mot de passe**.
3. Dans la zone de texte **Mot de passe actuel**, entrez le mot de passe actuellement associé à votre compte.
4. Dans la zone de texte **Nouveau mot de passe**, entrez le nouveau mot de passe à associer à votre compte.

   REMARQUE : Les mots de passe contiennent au moins huit caractères. Pour obtenir une sécurité optimale, il vous est conseillé d'utiliser une combinaison de caractères majuscules et minuscules en conjonction avec des symboles numériques et uniques.

5. Dans la zone de texte **Confirmer le nouveau mot de passe**, entrez une nouvelle fois le nouveau mot de passe de votre compte.

   Selon les caractères que vous utilisez dans le mot de passe, la force de ce dernier est reconnue comme :

   - **Très faible**
   - **Faible**
   - **Normal**
   - **Élevée**
   - **Très élevée**

6. Cliquez sur **Change Password (Modifier le mot de passe)**.

Invitation d'utilisateurs et définition des droits de sécurité des utilisateurs

Vous pouvez utiliser le portail de licences pour inviter des utilisateurs dans un groupe ou sous-groupe et pour définir des droits de sécurité pour ces utilisateurs.

REMARQUE : Vous devez détenir des droits d'administrateur pour inviter, supprimer ou modifier un utilisateur.

En tant qu'administrateur, vous pouvez effectuer les actions suivantes pour un utilisateur :

Définir des droits	Si vous définissez des privilèges plus faibles, tous les sous-groupes sont affectés.
Révoquer des droits	La sélection de cette option supprime l'utilisateur du groupe. S'il s'agit d'un groupe racine, le compte d'utilisateur est supprimé du système.

Pour inviter des utilisateurs et définir les droits de sécurité des utilisateurs :

1. À la page d'**Accueil du Portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Développez la zone **Utilisateurs**, puis cliquez sur **Inviter un nouvel utilisateur**.
   La boîte de dialogue **Inviter un nouvel utilisateur** s'affiche.
3. Dans la boîte de dialogue **Inviter un nouvel utilisateur**, saisissez les informations suivantes :

Champ	Description
Prénom	Sert à identifier l'utilisateur. Saisissez le prénom de l'utilisateur. **REMARQUE :** Cette entrée est obligatoire.
Nom	Sert à identifier l'utilisateur. Saisissez le nom de l'utilisateur. **REMARQUE :** Cette entrée est obligatoire.
Réf. utilisateur	Sert à identifier l'utilisateur. Saisissez une adresse e-mail unique pour l'utilisateur. **REMARQUE :** L'adresse e-mail doit être unique et ne peut pas avoir été utilisée préalablement pour une inscription sur le portail de licences. Cette entrée est obligatoire.
Droits d'utilisateur	Sert à définir le niveau de droits de contrôle d'accès au contenu du portail de licences. Sélectionnez les droits appropriés à attribuer à l'utilisateur. Vous avez le choix entre : – **Admin** : fournit un accès complet au contenu du portail, y compris la capacité de créer, modifier et supprimer des utilisateurs, groupes, cores et agents. – **Lecture seule** : fournit un accès d'affichage uniquement au contenu du portail. – **Afficher uniquement les groupes** : limite l'accès à l'affichage de la liste des sous-groupes.

4. Cliquez sur **Add** (Ajouter).
   Dans la zone **Utilisateurs**, les informations suivantes s'affichent : l'utilisateur, les privilèges attribués, l'adresse e-mail de l'utilisateur et l'heure la plus récente de la connexion de cet utilisateur au portail de licences.

Modification des privilèges de sécurité de l'utilisateur

REMARQUE : Les droits d'accès de l'utilisateur sont hérités par leur sous-groupe.

Pour modifier les privilèges de sécurité de l'utilisateur :

1. À la page d'**Accueil du Portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Développez la zone **Utilisateurs**.
3. Cliquez sur **Actions** en regard du nom de l'utilisateur dont vous souhaitez modifier les privilèges, puis cliquez sur **Privilèges**.
   La boîte de dialogue **Sécurité utilisateur** apparaît.
4. Sélectionnez les droits d'utilisateur appropriés pour cet utilisateur.
   Vous pouvez choisir parmi les options suivantes :

Admin	Fournit un accès complet au contenu du portail, notamment la création, la modification et la suppression d'utilisateurs, de groupes, de cores et d'agents.
Lecture seule	Autorise l'accès en lecture seule au contenu du portail (à l'exception de la liste des utilisateurs et de la clé de licence).
Afficher uniquement les groupes	Limite l'accès à l'affichage d'une liste des sous-groupes. Ne permet pas d'afficher la liste des utilisateurs. Toutes les informations sur les clients sont restreintes et inaccessibles.

   REMARQUE : Les droits d'accès des utilisateurs sont hérités par leurs sous-groupes, à l'exception de **ViewGroupsOnly**, car ce type de privilège ne donne pas accès aux sous-groupes.
5. Cliquez sur **Enregistrer**.
   Le nouveau niveau de privilèges attribué s'affiche dans la colonne **Type de privilège**.

Révocation des droits d'utilisateur

Pour révoquer les droits de l'utilisateur :

1. À la page d'**Accueil du portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Développez la zone **Utilisateurs**.
3. En regard des privilèges à modifier, cliquez sur **Actions**, puis sélectionnez **Révoquer tous les privilèges**.
   Un message de confirmation s'affiche. Vous devez confirmer que vous souhaitez révoquer les privilèges de groupe.
4. Après avoir vérifié que l'utilisateur identifié est bien celui dont vous voulez révoquer les privilèges, cliquez sur **OK**.

Affichage d'utilisateurs

Les utilisateurs sont associés à des groupes et vous les affichez dans l'onglet **Utilisateur** de la page **Vue de groupe** du portail de licences.

REMARQUE : Pour afficher les utilisateurs d'un groupe, l'utilisateur connecté doit détenir des privilèges d'administrateur sur ce groupe d'utilisateurs.

Pour afficher des utilisateurs :

1. À la page d'**Accueil du Portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Développez la zone **Utilisateurs**.

Vous pouvez afficher les détails suivants des utilisateurs d'un groupe :

- **Adresse e-mail**
- **Nom**
- **Date de la dernière connexion**
- **Type de privilège**
- **Actions**

REMARQUE : Cette liste est spécifique au groupe sélectionné. L'utilisateur actuellement connecté n'est pas affiché.

À propos des groupes

Les groupes représentent les partenaires, sociétés et sous-groupes de sociétés. Ils contiennent les informations et la structure suivantes :

- Informations sur l'organisation.
- Liens vers l'option de téléchargement du programme d'installation, qui permet de télécharger l'AppAssure 5 Core et les agents.
- Nombre illimité de cores.
- Autres groupes, sans aucune limite de profondeur.
- Les groupes doivent contenir au moins un utilisateur doté de droits d'accès. Lorsque l'utilisateur se connecte, le portail de licences affiche le compte en tant que groupe racine.
- Les groupes peuvent contenir de nombreux utilisateurs possédant des droits d'accès.

Gestion des groupes

Vous pouvez facilement afficher et gérer des groupes et sous-groupes depuis la page d'**Accueil du Portail de licences**. Vous pouvez ajouter des sous-groupes et afficher tous les sous-groupes du groupe actuel. Vous pouvez également modifier et supprimer des groupes.

REMARQUE : Seuls les utilisateurs possédant des droits d'administration peuvent gérer les groupes et les sous-groupes.

Ajout d'un groupe ou d'un sous-groupe

REMARQUE : Seuls les utilisateurs possédant des droits d'administration peuvent ajouter des groupes et des sous-groupes.

Pour ajouter un groupe ou un sous-groupe :

1. À la page d'**Accueil du Portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Pour ajouter un groupe au groupe racine, cliquez sur **Ajouter un groupe** dans la zone **Groupes** de la page. Pour ajouter un groupe à un sous-groupe, sélectionnez ce dernier, puis cliquez sur **Ajouter un groupe**.

   La boîte de dialogue **Ajouter un groupe** s'affiche.
3. Dans la zone de texte **Nom de groupe**, entrez un nom pour le groupe ou le sous-groupe.

   REMARQUE : Le **Nom de groupe** est requis.
4. Dans la zone de texte **Description**, entrez une description pour le groupe.
5. Cliquez sur **Add** (Ajouter).

Suppression d'un sous-groupe

REMARQUE : Seuls les utilisateurs possédant des droits d'administration peuvent ajouter des groupes et des sous-groupes.

Pour supprimer un sous-groupe :

1. À la page d'**Accueil du Portail de licences**, sélectionnez un groupe dans la zone de navigation de gauche.
2. Dans la zone **Groupes** de la page, dans le menu **Actions** en regard du sous-groupe à supprimer, cliquez sur **Supprimer**.
3. Dans la boîte de dialogue de **Confirmation**, cliquez sur **OK**.

Modification des informations sur le groupe

Pour modifier les informations sur un groupe :

1. Dans la page d'**Accueil du Portail de licences AppAssure 5** de la zone de navigation de gauche, sélectionnez le groupe racine ou un sous-groupe.
2. Dans la page **Groupes**, effectuez l'une des actions suivantes :
   - Pour modifier les informations sur le groupe racine, cliquez sur **Paramètres** sous le nom de groupe racine.
   - Pour modifier les informations d'un sous-groupe, cliquez sur **Actions** en regard du nom de ce sous-groupe, puis sélectionnez **Paramètres**.

   La boîte de dialogue **Paramètres** s'ouvre et affiche l'onglet **Infos sur le groupe**.
3. Entrez les informations concernant le groupe comme suit :

Champ	Description
Nom du groupe	Entrez un nom pour le groupe. Ce nom sert à identifier le groupe. **REMARQUE :** Il s'agit d'une zone de texte obligatoire.
Propriétaire	Sélectionnez un utilisateur de la liste déroulante. L'utilisateur sélectionné représente l'administrateur du groupe, qui contrôle l'abonnement et l'accès utilisateur. **REMARQUE :** Seul un utilisateur propriétaire peut sélectionner un autre propriétaire. Pour les autres types d'utilisateur, ce champ est désactivé.
Sous-domaine	Vous pouvez entrer le sous-domaine pour un accès de portail d'un groupe racine. Le sous-domaine représente la première partie de l'URL qui dirige les utilisateurs vers le portail de licences. **REMARQUE :** Ce champ s'affiche uniquement pour un groupe racine. Notez également que le nom du sous-domaine ne doit comporter que des lettres et des chiffres, sans espace.
Description	Entrez une description pour le groupe.

4. Cliquez sur **Enregistrer**.

Modification des paramètres de personnalisation du groupe racine

Pour modifier les paramètres de personnalisation du groupe racine :

1. Dans la page d'**Accueil du Portail de licences AppAssure 5** de la zone de navigation de gauche, sélectionnez le groupe racine.
2. Dans la page **Groupes**, cliquez sur **Paramètres** sous le nom de groupe racine.
   La boîte de dialogue **Paramètres** s'ouvre et affiche l'onglet **Infos sur le groupe**.
3. Cliquez sur l'onglet **Repersonnalisation**.
4. Entrez les informations de marque comme suit :

Champ	Description
Sélectionner une image	Naviguez pour localiser et sélectionner l'image (portant l'extension .png, .jpg. ou .gif) à utiliser pour personnaliser la marque sur le portail de licences avec le logo de votre société.
Sélectionner une icône	Naviguez pour localiser et sélectionner l'icône (portant l'extension de fichier .ico) à utiliser pour personnaliser la marque sur le portail de licences avec l'icône de votre société.
Nous contacter	Sélectionnez l'ensemble de coordonnées à utiliser pour votre portail de licences. Vous pouvez sélectionner l'une des options suivantes : – **Contacts AppAssure** : utilise les coordonnées Dell AppAssure par défaut. – **Identiques aux informations de société** : utilise les coordonnées saisies dans l'onglet **Informations de société**. – **Contacts personnalisés** : vous permet d'entrer des informations de contact personnalisées.

   REMARQUE : Vous pouvez cliquer sur **Réinitialiser la repersonnalisation** pour remettre les paramètres aux paramètres AppAssure par défaut.
5. Cliquez sur **Enregistrer**.

Ajout des informations de société et de facturation à un groupe

Pour ajouter des informations de société et de facturation à un groupe :

1. Dans la page d'**Accueil du Portail de licences AppAssure 5** de la zone de navigation de gauche, sélectionnez le groupe racine ou un sous-groupe.
2. Dans la page **Groupes**, effectuez l'une des actions suivantes :
   – Pour modifier les informations sur le groupe racine, cliquez sur **Paramètres** sous le nom de groupe racine.
   – Pour modifier les informations d'un sous-groupe, cliquez sur **Actions** en regard du nom de ce sous-groupe, puis sélectionnez **Paramètres**.

   La boîte de dialogue **Paramètres** s'ouvre et affiche l'onglet **Infos sur le groupe**.
3. Sélectionnez l'onglet **Infos sur la société**.
4. Dans l'onglet **Infos sur la société**, entrez les informations concernant la société, comme suit :

Zone de texte	Description
Nom de la société	Sert à identifier la société. Entrez le nom de la société.
Contact de la société	Sert à établir un point de contact avec la société. Entrez le nom du contact de la société.
Numéro de téléphone de la société	Sert à spécifier les coordonnées pour le point de contact de la société. Entrez le numéro de téléphone du contact de la société.
E-mail de la société	Sert à spécifier les coordonnées du contact de la société. Entrez l'adresse e-mail de cette personne.
Pays de la société	Sert à identifier le pays dans lequel se trouve la société. Sélectionnez le pays dans lequel se trouve la société.
État de la société (États-Unis)	Sert à spécifier l'État dans lequel se trouve la société, si elle est située aux États-Unis d'Amérique. Sélectionnez l'État dans lequel se trouve la société.
Ville de la société	Sert à spécifier la ville où se trouve la société. Entrez la ville où se trouve la société.
Adresse de la société	Sert à spécifier l'adresse physique de la société. Entrez l'adresse physique de la société.
Code postal de la société (si aux États-Unis)	Sert à spécifier l'adresse postale correspondant à l'adresse physique de la société. Entrez le code postal correspondant à l'adresse physique de la société.

5. Si les informations de facturation sont identiques aux informations sur la société, cochez la case **Les informations de facturation sont identiques aux informations de société**.

   Les informations de société sont automatiquement entrées dans les zones de texte de **Facturation** suivantes.

6. Si les informations de facturation sont différentes des informations de la société, entrez-les comme indiqué ci-dessous :

Zone de texte	Description
Nom de facturation	Entrez le nom de la personne responsable. Le nom est utilisé pour identifier la personne responsable des paiements des prestations de service.
Contact de facturation	Entrez le nom de la personne responsable du paiement. Il sert à établir un point de contact responsable du paiement.
Numéro de téléphone de facturation	Entrez le numéro de téléphone de la personne responsable. Il sert à spécifier les coordonnées de la personne responsable.
Adresse électronique de facturation	Entrez l'adresse e-mail de la personne responsable. Elle sert à spécifier les coordonnées de la personne responsable.
Pays de facturation	Sélectionnez le pays où se trouve la personne responsable. Cette information est utilisée pour identifier le pays où se trouve la personne responsable.
État de facturation (États-Unis)	Sélectionnez l'État où se trouve la personne responsable. Cette information est utilisée pour spécifier l'État où se trouve la personne responsable, si elle se trouve aux États-Unis d'Amérique.
Ville de facturation	Entrez la ville où se trouve la personne responsable. Cette information est utilisée pour spécifier la ville où se trouve la personne responsable.
Adresse de facturation	Entrez l'adresse physique de la personne responsable. Cette information sert à spécifier l'adresse physique de l'endroit où se trouve la personne responsable.

Zone de texte	Description
Code postal de facturation (si aux États-Unis)	Entrez le code postal de l'adresse physique de la personne responsable. Cette information sert à spécifier le code postal de l'adresse physique de la personne responsable.

7. Cliquez sur **Enregistrer**.

Gestion des licences

Le serveur de portails sert à gérer les licences et l'expiration de licences machine par machine. Il existe trois types de licences :

Évaluation La licence est valable 14 jours. Il s'agit de la licence par défaut disponible sur le portail de licences AppAssure 5.

REMARQUE : La licence d'évaluation peut être prolongée une seule fois par l'administrateur du groupe, pour passer de 14 à 28 jours.

Abonnement La licence est valide pour une durée limitée (30 jours, par exemple).

Enterprise Licence permanente qui représente le nombre de licences disponibles pouvant être utilisées lors de l'ajout de nouveaux agents.

REMARQUE : Vous ne pouvez associer un compte qu'avec une licence par abonnement ou une licence d'entreprise. La valeur par défaut (licence par abonnement) est définie par l'utilisateur lors de la création du compte. Seuls les administrateurs peuvent changer le type de licence des sous-groupes pour lesquels le groupe racine possède uniquement des licences d'évaluation.

Le type de licence peut être défini pour un groupe et tous ses sous-groupes à l'aide de l'option **Appliquer à tous les sous-groupes**. Dans ce cas, par exemple, si le type de licence défini pour le groupe est Abonnement, tous les sous-groupes de ce groupe reçoivent également une licence par abonnement.

REMARQUE : Si le compte de l'utilisateur inscrit est migré de la licence d'évaluation à une licence d'abonnement, cet utilisateur ne peut pas s'inscrire pour une autre licence d'évaluation.

Lorsqu'une licence d'évaluation expire, la machine sur laquelle elle était activée est automatiquement désactivée dans le portail de licences et son état devient **Expiré**.

REMARQUE : Lorsqu'une licence expire, la licence d'agent expire également et l'agent cesse de prendre des instantanés.

Pour en savoir plus sur les licences AppAssure 5, voir Gestion des licences AppAssure 5.

Affichage de votre clé de licence

Pour afficher votre clé de licence à l'aide du portail de licences :

1. Sur la page d'**Accueil du portail de licences d'AppAssure 5**, sélectionnez un groupe.
2. Cliquez sur **Clé de licence**.
   La boîte de dialogue **Clé de licence** affiche la clé de licence associée au core pour votre groupe.

Modification du type de licence d'un sous-groupe

Seuls les utilisateurs possédant des droits d'administrateur peuvent changer les types de licence d'un sous-groupe depuis le groupe racine.

Pour modifier le type de licence d'un sous-groupe :

1. Dans la page d'accueil du portail de licences, sélectionnez le groupe, puis ouvrez le menu déroulant et cliquez sur **Licences**.
2. Dans la boîte de dialogue **Licences**, en regard de l'option **Type de licence**, cliquez sur **Modifier**.
3. Dans la boîte de dialogue **Modifier le type de licence**, sélectionnez le type voulu (par exemple, licence par abonnement, licence d'entreprise ou licence d'évaluation).
4. (Facultatif) Pour appliquer cette licence à tous les sous-groupes apparentés, sélectionnez **Appliquer à tous les sous-groupes**.

   Vous pouvez appliquer une date d'expiration à une licence par abonnement : désélectionnez la case à cocher **N'expire jamais** sous **Date d'expiration**, choisissez une date d'expiration, puis cliquez sur **Enregistrer**.

   Vous pouvez également prolonger la période de validité d'une licence d'évaluation en choisissant une autre date d'expiration pour cette licence sous **Date de prolongation**, puis en cliquant sur **Enregistrer**.

   REMARQUE : Vous pouvez étendre la période d'évaluation pour l'ensemble du groupe si aucune machine d'agent du groupe n'a encore été étendue.

   REMARQUE : Lorsqu'une licence expire, la licence d'agent expire également et l'agent cesse de prendre des instantanés.

À propos de la facturation des licences

Les licences d'abonnement se paient mensuellement et donc comprennent tous les agents activés, inscrits et désactivés. Collectivement, tous les agents du mois de facturation sont pris en compte pour la totalité des licences d'abonnement de cette période. Les agents qui ont été désactivés au cours du mois de facturation précédent ne sont pas inclus dans le calcul.

Les utilisateurs ne paient que les licences utilisées. Par exemple, si la capacité du groupe est de 20 To et que seuls 10 To sont utilisés, le groupe sera facturé seulement pour les 10 To utilisés. Les factures sont générées le premier jour de chaque mois pour le mois précédent.

Les licences d'entreprise sont comptabilisées de la même manière mais, comme elles sont permanentes, la facturation mensuelle n'a pas lieu.

À propos de la suppression de licences

Vous pouvez choisir de supprimer une licence en désactivant ou désinstallant l'application AppAssure 5. Que vous choisissiez de supprimer ou de désinstaller l'application AppAssure 5, la suppression elle-même se produit au début du mois suivant.

Configuration des paramètres de portail de licences

REMARQUE : L'onglet **Avancé** n'est visible que pour les utilisateurs possédant des droits d'administrateur.

Pour configurer les paramètres avancés :

1. Dans la page d'**Accueil** du **portail de licences AppAssure 5**, sélectionnez un groupe, puis cliquez sur **Paramètres** dans la liste déroulante.

La boîte de dialogue **Paramètres** s'affiche.

2. Cliquez sur l'onglet **Avancé** dans la zone **Paramètres d'interrogation de service**, puis saisissez les informations décrites ci-dessous :

Zone de texte	Description
Intervalle d'interrogation	Entrez une valeur pour l'intervalle d'interrogation. La valeur par défaut de l'intervalle d'interrogation est de 60 minutes. L'intervalle d'interrogation détermine la fréquence avec laquelle le logiciel communique avec le portail. La valeur est en minutes.
Période de grâce	Entrez une valeur pour la période de grâce. Le nombre maximal que vous pouvez entrer est 15 jours. Le délai de grâce détermine la durée pendant laquelle le logiciel fonctionne sans communiquer avec le service de portail.

3. Cliquez sur **Enregistrer**.

Gestion des ordinateurs

L'affichage des ordinateurs enregistrés est un contrôle d'arborescence qui affiche les cores et les agents AppAssure 5 installés. Cet affichage vous permet de voir et gérer les licences ordinateur par ordinateur, ajouter un core ou ajouter un agent.

Pour gérer les ordinateurs enregistrés

1. Sur la page d'**Accueil** dans le **Portail de licences AppAssure 5**, sélectionnez un groupe, puis effectuez un défilement pour afficher et développer la zone **Ordinateurs enregistrés** de la page.

   Une liste d'agents est imbriquée dans les cores AppAssure respectifs. Les informations suivantes sont énumérées pour tous les ordinateurs enregistrés :

   - **Condition**
   - **Nom d'ordinateur**
   - **Version (d'AppAssure)**
   - **SE (Système d'exploitation)**
   - **Type de licence**
   - **Licence**
   - **Actions (menu déroulant)**

2. Vous pouvez sélectionner des actions parmi celles décrites dans le tableau suivant pour gérer l'agent.

Option	Description
Activer	Réactive un agent désactivé.
Désactiver	Un agent désactivé continue à être facturé pour le mois courant. Il n'est pas facturé pour le mois suivant.
Mise à niveau	Met à niveau la version d'AppAssure installée sur l'agent, s'il n'exécute pas la dernière version disponible.
Bloquer	Bloque l'agent. Un agent bloqué continue à être facturé pour le mois courant. Il n'est pas facturé pour le mois suivant. Un agent bloqué ne peut pas être réactivé sur un ordinateur client.

Option	Description
Débloquer et activer	Rend l'agent visible et l'active.
Débloquer et désactiver	Rend l'agent visible mais le désactive.

REMARQUE : Les utilisateurs dotés de privilèges d'administrateur peuvent rétrograder ou étendre chaque machine une seule fois. Les rétrogradations s'appliquent aux agents autres que ceux avec une licence d'évaluation et l'extension s'applique aux licences d'évaluation.

À propos des rapports du Portail de licences

Le Portail de licences AppAssure 5 vous permet de générer des rapports au sujet de l'activité du Portail de licences. Vous pouvez accéder aux rapports concernant n'importe quel groupe depuis la page d'Accueil dans le Portail de licences AppAssure 5. Vous pouvez exporter les rapports dans n'importe lequel des formats suivants :

- XLS
- XLSX
- PDF
- RTFMHT
- txt
- CSV
- Image

De nombreux rapports prennent en charge les analyses en cascade (drill down). Vous pouvez cliquer sur les liens d'un rapport pour que le sous-rapport correspondant s'affiche. Par exemple, lorsque vous cliquez sur un nom de groupe, le rapport du groupe sélectionné s'affiche. Le portail de licences produit des rapports pour les catégories de rapports suivantes :

- Résumé
- Utilisateur
- Groupe
- Ordinateur
- Licence

Catégorie Résumé

Le rapport de tableau de bord suivant est disponible dans la catégorie Résumé.

Rapport de tableau de bord

Ce rapport affiche le nombre total de machines d'un groupe et de tous ses sous-groupes. Il comprend les informations suivantes :

- Le nombre de licences actives sur une période donnée.
- L'espace total protégé sur une période donnée.
- Diagramme à secteurs qui indique le taux de machines portant chaque état, par rapport au nombre total de machines.

Le rapport de tableau de bord contient également les options d'analyse en cascade (drill down) suivantes :

- Nombre total de machines
- Ordinateurs actifs
- Ordinateurs inactifs
- Ordinateurs bloqués

Catégorie Utilisateur

La catégorie Utilisateurs inclut les rapports suivants.

Rapport Liste d'utilisateurs

Affiche tous les utilisateurs, y compris ceux qui ont été ajoutés et supprimés.

Rapport Utilisateurs ajoutés

Ce rapport affiche la liste des utilisateurs qui ont été ajoutés au cours d'une période de temps donnée. Vous pouvez l'utiliser pour afficher le groupe et tous les sous-groupes.

Rapport Utilisateurs supprimés

Affiche la liste des utilisateurs supprimés au cours de la période spécifiée.

Catégorie Groupes

Les rapports suivants sont disponibles dans la catégorie Groupe :

- Liste de rapports de Groupes
- Rapport de Groupes ajoutés
- Rapport de Groupes supprimés

Liste de rapports de Groupes

Ce rapport affiche tous les sous-groupes d'un groupe sélectionné (de tout niveau). Il contient les informations de recherches approfondies suivantes :

- Nom du groupe
- Chemin du groupe, qui mène à la page **Groupe**

Rapport de Groupes ajoutés

Ce rapport affiche la liste de groupes ajoutés au groupe ou tout sous-groupe pendant un intervalle de temps spécifié. Il contient les informations détaillées suivantes :

- Nom du groupe
- Chemin du groupe, qui mène à la page **Groupe**

Rapport de Groupes supprimés

Ce rapport affiche la liste des groupes supprimés dans le groupe actuel ou ses sous-groupes pendant un intervalle de temps spécifié.

Catégorie Machines

Les rapports suivants sont disponibles dans la catégorie Machines (Ordinateurs) :

- Rapport Liste de machines
- Rapport Liste de cores

- Rapport machines ajoutées
- Rapport machines supprimées

Rapport Liste de machines

Ce rapport affiche la liste des machines d'un groupe sélectionné, y compris tous les sous groupes. Il contient les informations détaillées suivantes :

- Nom de la machine
- Groupe
- Chemin du groupe, qui mène à la page **Groupe**

Rapport Liste de cores

Ce rapport affiche la liste des cores d'un groupe sélectionné, y compris tous les sous-groupes. Il contient les informations détaillées suivantes :

- Nom du groupe
- Chemin du groupe, qui mène à la page **Groupe**

Rapport Machines ajoutées

Ce rapport affiche la liste des machines ajoutées sur une période donnée. Elle comprend le groupe et tous les sous groupes, ainsi que les informations détaillées suivantes :

- Nom de la machine
- Nom du groupe
- Chemin du groupe, qui mène à la page **Groupe**

Rapport Machines supprimées

Ce rapport affiche la liste des machines supprimées sur une période donnée. Elle comprend le groupe et tous les sous-groupes, ainsi que les informations détaillées suivantes :

- Nom du groupe
- Chemin du groupe, qui mène à la page **Groupe**

Catégorie Licences

Les rapports suivants sont disponibles dans la catégorie Licences.

- Rapport de Licences activées
- Rapport de Licences actives
- Rapport de Licences inactives
- Rapport de Licences d'évaluation

Rapport de Licences activées

Ce rapport affiche la liste des ordinateurs qui ont été activés au cours d'une période donnée. Il contient les informations détaillées suivantes :

- Nom de l'ordinateur
- Groupe
- Chemin d'accès du groupe

Rapport de Licences actives

Ce rapport affiche la liste des licences actives d'un groupe et de ses sous-groupes. Il contient les informations détaillées suivantes :

- Nom de l'ordinateur
- Groupe
- Chemin d'accès du groupe

Rapport de Licences inactives

Ce rapport affiche la liste des ordinateurs inactifs d'un groupe et de ses sous-groupes. Il contient les informations détaillées suivantes :

- Nom de l'ordinateur
- Groupe
- Chemin d'accès du groupe

Rapport de Licences d'évaluation

Ce rapport affiche la liste des licences d'évaluation d'un groupe et de ses sous-groupes. Il contient les informations détaillées suivantes :

- Nom de l'ordinateur
- Groupe
- Chemin d'accès du groupe

Recherche approfondie

Les paragraphes suivants décrivent les options d'analyse en cascade (drill down) disponibles dans les rapports.

Nombre total de machines

Affiche le nombre de machines du groupe sélectionné, notamment de tous les sous-groupes. Vous pouvez effectuer une recherche approfondie pour afficher les informations suivantes :

- Nom de la machine
- Groupe
- Chemin d'accès du groupe
- État actuel
- Nom de société
- Espace actuellement protégé

Machines actives

Affiche le nombre de machines actives du groupe sélectionné et notamment de tous les sous-groupes. Vous pouvez effectuer une recherche approfondie pour afficher les informations suivantes :

- Nom de la machine
- Groupe
- Chemin d'accès du groupe
- État actuel
- Date d'activation
- Nombre de jours actif
- Espace actuellement protégé

Machines inactives

Affiche le nombre de machines inactives du groupe sélectionné et notamment de tous les sous-groupes. Vous pouvez effectuer une recherche approfondie pour afficher les informations suivantes :

- Nom de la machine
- Groupe
- Chemin d'accès du groupe
- État actuel
- Nom de société
- Date de désactivation
- Nombre de jours inactif
- Espace actuellement protégé

Machines bloquées

Affiche le nombre de machines du groupe sélectionné et notamment de tous les sous-groupes, y compris les machines bloquées par AppAssure. Vous pouvez effectuer une recherche approfondie pour afficher les informations suivantes :

- Nom de la machine
- Groupe
- Chemin d'accès du groupe
- État actuel
- Nom de société
- Date de bloc
- Nombre de jours bloqué
- Espace actuellement protégé

Nom de la machine

Affiche les détails de la machine et ceux du core de cette machine.

Groupe/Nom du groupe

Affiche les détails du groupe.

(Chemin d'accès/ Chemin d'accès du groupe).

Redirige l'utilisateur vers le groupe dont le chemin a été sélectionné.

Génération d'un rapport

Pour générer un rapport :

1. Effectuez l'une des opérations suivantes :
   - Sélectionnez un rapport de la liste déroulante **Rapport**.
   - Dans la page d'**Accueil** du **Portail de licences**, sélectionnez une catégorie de la liste déroulante **Catégorie**.
   - Pour un rapport de groupe, naviguez jusqu'au groupe, puis descendez jusqu'à la zone **Rapports** de la page de groupe.
2. Sélectionnez l'une des options suivantes :
   - Pour exécuter un rapport unique, cliquez sur **OK**.
   - Pour exécuter automatiquement le rapport de façon récurrente, cliquez sur **S'abonner** et sélectionnez une option, comme **Quotidiennement**, **Hebdomadairement** ou **Mensuellement** ; puis cliquez sur **Ajouter**.

Gestion des abonnements aux rapports

Vous pouvez modifier la fréquence de vos abonnements aux rapports existants afin que les rapports électroniques vous soient envoyés tous les jours, toutes les semaines ou tous les mois. Vous pouvez également annuler votre abonnement à un rapport, selon vos besoins.

Pour gérer les abonnements :

1. Sur la page d'**Accueil du Portail de licences AppAssure 5**, cliquez sur votre nom d'utilisateur, puis cliquez sur les **Paramètres personnels** .
2. Sur la page **Profil de compte**, cliquez sur l'onglet **Abonnements**.
3. Pour modifier la fréquence de votre abonnement aux rapports, effectuez l'une des opérations suivantes :
   - Dans la colonne **Actions**, cliquez sur la liste déroulante des **Actions** correspondant aux abonnements de rapport disponibles, puis sélectionnez **Modifier l'abonnement**.
   - Dans la boîte de dialogue **Paramètres**, dans le menu déroulant, choisissez l'une des options suivantes de fréquence de rapports, puis cliquez sur **Enregistrer** :

Tous les jours	Le rapport sélectionné est envoyé tous les jours.
Toutes les semaines	Le rapport sélectionné est envoyé tous les vendredis.
Tous les mois	Le rapport sélectionné est envoyé à la fin de chaque mois.

4. Cliquez sur **Enregistrer**.
5. Pour annuler votre abonnement à un rapport, ouvrez la liste déroulante **Actions** correspondant au rapport dont vous voulez vous désabonner, cliquez sur **Annuler l'abonnement au rapport**, puis sur **Oui**.

3

Travailler avec l'AppAssure 5 Core

Accès à la console AppAssure 5 Core

Assurez-vous de mettre à jour les sites de confiance de la façon discutée dans la rubrique Mise à jour des sites de confiance dans Internet Explorer, puis configurez vos navigateurs de la façon discutée dans la rubrique Configuration de navigateurs pour accéder à distance à l'AppAssure 5 Core Console. Après avoir mis à jour les sites de confiance dans Internet Explorer et configuré vos navigateurs, effectuez l'une des tâches suivantes pour accéder à l'AppAssure 5 Core Console:

- Connectez-vous localement à votre serveur AppAssure 5 Core, puis sélectionnez l'icône **Core Console**.
- Ou, entrez l'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 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 de navigateurs pour accéder à distance à l'AppAssure 5 Core Console

Pour pouvoir accéder avec succès à la console AppAssure 5 Core depuis une machine distante, vous devez modifier les paramètres de votre navigateur. Les procédures suivantes détaille la manière de modifier les paramètres de navigateur Internet Explorer, Google Chrome et Mozilla Firefox.

REMARQUE : Pour modifier les paramètres de navigateur, vous devez être connecté à la machine avec des privilèges d'administrateur.

REMARQUE : Comme Chrome utilise les paramètres Internet Explorer, vous devez apporter les modifications à Chrome à l'aide d'Internet Explorer.

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

1. Dans l'écran **Options Internet**, sélectionnez l'onglet **Sécurité**.
2. Cliquez sur **Sites de confiance** et cliquez sur **Sites**.
3. 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 Appliance hébergeant AppAssure 5 Core*> à la zone **Sites de confiance**.
4. Cliquez sur **Fermer**, sélectionnez **Sites de confiance**, puis cliquez sur **Personnaliser le niveau**.
5. Faites défiler l'affichage jusqu'à **Divers → Affiche un contenu mixte** et sélectionnez **Activer**.
6. 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**.
7. Cliquez sur **OK**, puis sélectionnez l'onglet **Avancé**.
8. Faites défiler la liste jusqu'à **Multimédia**, puis sélectionnez **Lire les animations dans les pages Web**.
9. Faites défiler l'écran jusqu'à **Sécurité**, sélectionnez **Activer l'authentification Windows intégrée**, puis cliquez sur **OK**.

Pour modifier les paramètres de navigateur 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 5 Core ; par exemple, *AdresseIP,nom-hôte*.
4. Redémarrez Firefox.

Schéma de configuration de l'AppAssure 5 Core

Avant d'utiliser AppAssure 5, vous devez configurer l'AppAssure 5 Core. La configuration comprend des tâches telles que la création et la configuration du référentiel pour stocker des instantanés, définir des clés de chiffrement pour sécuriser les données protégées, et configurer des alertes et notifications. Après avoir terminé la configuration de l'AppAssure 5 Core, vous pourrez protéger des agents et effectuer une restauration.

Pour configurer l'AppAssure 5 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 l'appliance DL4000 Backup To Disk, 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 Dell DL4000* sur **dell.com/support/manuals** .

Gestion des licences

AppAssure 5 vous permet de gérer les licences AppAssure 5 directement depuis AppAssure 5 Core Console. Depuis la console, vous pouvez modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au Portail de licences AppAssure 5 depuis la page de Gestion des licences dans la Core Console.

La page de gestion des licences inclut les informations suivantes :

- Type de licence
- État 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

Pour plus d'informations sur les licences AppAssure 5, voir le Chapitre 2, Gestion des licences AppAssure 5.

Modifier une clé de licence

Pour modifier une clé de licence :

1. Accédez à la console AppAssure 5 Core, puis sélectionnez l'onglet **Configuration**.
2. Cliquez sur **Licences**.
   La page **Gestion des licences** s'affiche.
3. Depuis les détails de la licence, cliquez sur **Modifier**.
   La boîte de dialogue **Modifier la clé de licence** apparaît.
4. Dans la boîte de dialogue **Modifier la clé de licence**, entrez la nouvelle clé de licence, puis cliquez sur **OK**.

Contacter le serveur de Portail de licences

La console AppAssure 5 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 la console AppAssure 5 Core, puis sélectionnez l'onglet **Configuration**.
2. Cliquez sur **Licences**.
   La page **Gestion des licences** s'affiche.
3. À partir de l'option **Licence Server**, cliquez sur **Contacter maintenant**.

Gestion des paramètres de l'AppAssure 5 Core

Les paramètres de l'AppAssure 5 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 DL4000 Backup to Disk. 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 AppAssure 5 Core Console, puis cliquez sur l'onglet **Configuration** et cliquez sur **Paramètres**.
2. Dans la zone **Généralités**, cliquez sur **Modifier**.
   La boîte de dialogue **Nom d'affichage** s'affiche.
3. Dans le champ **Nom**, entrez un nouveau nom d'affichage pour le core.
4. Cliquez sur **OK**.

Régler l'option Heure de tâche nocturne

Pour régler l'heure de tâche nocturne :

1. Naviguez jusqu'à AppAssure 5 Core Console, puis sélectionnez l'onglet **Configuration** et cliquez sur **Paramètres**.
2. Dans la zone **Tâches nocturnes**, cliquez sur **Modifier**.
   La boîte de dialogue **Tâches nocturnes** s'affiche.
3. Dans le champ **Heure de début**, entrez une nouvelle heure de début.
4. 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 AppAssure 5 Core Console, cliquez sur l'onglet **Configuration**, puis sur **Paramètres**.
2. Dans la zone **File d'attente de transfert**, cliquez sur **Modifier**.
   La boîte de dialogue **File d'attente de transfert** s'affiche.
3. 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.
4. Dans le champ **Nombre maximal de nouvelles tentatives**, entrez une valeur pour mettre à jour le nombre de nouvelles tentatives.
5. 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 AppAssure 5 Core Console, puis cliquez sur l'onglet **Configuration** et cliquez sur **Paramètres**.
2. 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.
3. Dans le champ **Délai d'attente de connexion**, entrez le délai imparti, en nombre de minutes et de secondes.
4. Dans le champ **Délai d'attente de lecture/écriture**, entrez le délai imparti (en minutes et secondes) pour un événement de lecture/écriture.
5. Cliquez sur **OK**.

Configuration des paramètres de cache de déduplication

Pour configurer les paramètres de cache de déduplication :

1. Naviguez jusqu'à AppAssure 5 Core Console, puis cliquez sur l'onglet **Configuration** et sur **Paramètres**.
2. Dans la zone de **Configuration du cache de déduplication**, cliquez sur **Modifier**.
   La boîte de dialogue **Configuration du cache de déduplication** s'affiche.
3. Dans le champ **Emplacement du cache principal**, entrez une valeur mise à jour pour modifier l'emplacement du cache principal.
4. Dans le champ **Emplacement du cache secondaire**, entrez une valeur mise à jour pour modifier l'emplacement du cache principal.
5. Dans le champ **Emplacement du cache de métadonnées**, entrez une valeur mise à jour pour modifier l'emplacement du cache de métadonnées.
6. Cliquez sur **OK**.

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

Modification des paramètres du moteur AppAssure 5

Pour modifier les paramètres du moteur AppAssure 5 :

1. Naviguez jusqu'à AppAssure 5 Core Console, puis cliquez sur l'onglet **Configuration** et sur **Paramètres**.
2. Dans la zone **Configuration du moteur de relecture**, cliquez sur **Modifier**.
   La boîte de dialogue **Configuration du moteur de relecture** s'affiche.
3. Dans la boîte de dialogue **Configuration du moteur de relecture**, spécifiez l'adresse IP. Choisissez l'une des options suivantes :
   - 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**.
4. Entrez les informations concernant la configuration comme suit :

Zone de texte	Description
Port	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 pour le moteur AppAssure.

Zone de texte	Description
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.
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.
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.

5. Sélectionnez **Aucun délai**.
6. 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 l'AppAssure 5 Core Console, sélectionnez l'onglet **Configuration** puis **Paramètres**.
2. 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.
3. 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.
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.

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

Á 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, AppAssure 5 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 AppAssure 5 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 console AppAssure 5 Core
- Création d'un référentiel
- Affichage des détails concernant un référentiel
- Modification des paramètres de référentiel
- Ajout d'un emplacement de stockage à un référentiel existant
- Vérification d'un référentiel
- Suppression d'un référentiel
- Restauration d'un référentiel

REMARQUE : Si vous utilisez l'appliance DL4000 Backup To Disk, il est recommandé d'utiliser l'onglet **Appliance** pour configurer les référentiels. Pour plus d'informations sur la création d'un référentiel sur l'appliance DL4000 Backup To Disk, voir Provisionnement du stockage.

Avant d'utiliser AppAssure 5, vous devez configurer un ou plusieurs référentiels sur le serveur core AppAssure 5. 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 l'AppAssure 5 Core Console.

Création d'un référentiel

REMARQUE : Si vous utilisez l'appliance DL4000 Backup To Disk, il vous est recommandé d'utiliser l'onglet **Appliance** pour configurer les référentiels. Pour plus d'informations sur la création d'un référentiel sur l'appliance DL4000 Backup To Disk, voir Provisionnement du stockage. Vous pouvez appliquer cette procédure si vous souhaitez configurer manuellement le stockage.

Pour créer un référentiel

1. Dans l'AppAssure 5 Core Console, cliquez sur l'onglet **Configuration**.
   La page **Référentiels** s'affiche.
2. Dans le menu déroulant **Actions**, sélectionnez **Ajouter un nouveau référentiel**.
   La boîte de dialogue **Ajouter un nouveau référentiel** s'affiche.
3. 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.

4. 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 AppAssure 5 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.
5. 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 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.
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.

- 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.
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.

6. 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.

Zone de texte	Description
	REMARQUE : Pour qu'AppAssure 5 valide le système d'exploitation, vous devez installer Windows Management Instrumentation (WMI) sur l'emplacement de stockage prévu.
Stratégie de mise en cache d'écriture	La stratégie de mise en cache d'écriture contrôle 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 **Désactivé**, AppAssure 5 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.

7. Cliquez sur **Enregistrer**.
   L'écran **Référentiels** s'affiche pour inclure le nouvel emplacement de stockage qui vient d'être ajouté.
8. Répétez les Étapes 4 à 7 pour ajouter plus d'emplacements de stockage au référentiel.
9. 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. Dans la console AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
   La page **Référentiels** s'affiche.
2. Cliquez sur **>** en regard de la colonne **État** du référentiel dont vous voulez afficher les détails.
3. 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. Dans l'AppAssure 5 Core Console, cliquez sur l'onglet **Configuration**.
   La page **Référentiels** s'affiche.
2. Cliquez sur **>** en regard de la colonne **État** du référentiel que vous souhaitez modifier.
3. En regard de l'option **Actions**, cliquez 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 me s'appliquent qu'aux sauvegardes effectuées après ces modifications. 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 l'agent.
Activation de la compression	Pour désactiver la compression, décochez cette case. Pour activer la compression, cochez cette case.

Champ	Description
	REMARQUE : Les modifications apportées à ce paramètre me s'appliquent qu'aux sauvegardes effectuées après ces modifications. 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 l'agent.

5. Cliquez sur **Enregistrer**.

Extension d'un référentiel existant

Si vous ajoutez un autre DAS MD1200 à l'appliance DL4000, vous pouvez utiliser le stockage disponible pour étendre un référentiel existant.

Pour étendre un référentiel existant :

1. Après avoir installé le DAS MD1200, ouvrez la console AppAssure Core 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'une spécification de fichier 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 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.

Zone de texte	Description
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 qu'AppAssure 5 valide 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 – 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 **Désactivé**, AppAssure 5 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

AppAssure 5 permet d'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 **Vérifier**.
3. Dans la boîte de dialogue **Supprimer un référentiel**, cliquez sur **Supprimer.**

   PRÉCAUTION : Lorsqu'un référentiel est supprimé, les données contenues dans le référentiel sont mises au rebut et ne peuvent être récupérées.

Remontage des volumes

Pour remonter les volumes :

1. Dans la console AppAssure 5 Core, cliquez sur l'onglet **Appliance**, puis sur **Tâches**.
2. Cliquez sur **Remonter les volumes**.
   Les volumes sont remontés.

Résolution de volumes étrangers

Si vous avez éteint ou déconnecté un MD1200 provisionné, puis que vous le rallumez ultérieurement, un événement s'affiche sur AppAssure 5 Core Console et vous signale que le MD1200 est connecté. Toutefois, aucune tâche n'apparaît dans l'onglet **Appliance** de l'écran **Tâches** pour vous permettre d'effectuer la restauration. L'écran **Enceintes** indique que le MD1200 porte un état « étranger ». De plus, AppAssure 5 signale les référentiels des disques virtuels étrangers comme étant hors ligne.

Pour résoudre les volumes étrangers :

1. Dans la console AppAssure 5 Core, 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 AppAssure 5 ne parvient pas à importer un référentiel, AppAssure 5 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'état **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 ; 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. Dans la console AppAssure 5 Core, cliquez sur l'onglet **Configuration**, puis sur **Référentiels**.

   L'écran **Référentiels** affiche le référentiel en échec avec un indicateur d'état rouge.
2. Développez le référentiel en échec en cliquant sur **>** en regard de l'option **État**.
3. Dans la section **Actions**, cliquez sur **Vérifiez**, puis sur **Oui** pour confirmer que vous souhaitez exécuter la vérification.

   AppAssure restaurer le référentiel.

Gestion de la sécurité

AppAssure 5 Core peut crypter des données d'instantané d'agent dans le référentiel. Au lieu de crypter l'ensemble du référentiel, AppAssure 5 vous permet d'indiquer une clé de cryptage au cours de la protection d'un agent dans un référentiel, ce qui permet la réutilisation des clés pour différents agents. 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 chiffrement pour assurer la confidentialité
- Le chiffrement n'a aucun effet sur les performances.
- Vous pouvez ajouter, retirer, importer, exporter, modifier et supprimer des clés de chiffrement configurées sur l'AppAssure 5 Core.
- Le nombre de clés de chiffrement que vous pouvez créer est illimité.

Ajout d'une clé de chiffrement

Pour ajouter une clé de chiffrement :

1. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer** de l'onglet **Configuration**, sélectionnez **Sécurité**.
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.

Zone de texte	Description
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. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Sécurité**.

   L'écran **Clés de chiffrement** s'affiche.
3. Cliquez sur le symbole de chevron droit **>** en regard du nom de la clé de cryptage à modifier, puis 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. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Sécurité**.
3. Cliquez sur le symbole de chevron droit **>** en regard du nom de la clé de cryptage à modifier, puis cliquez sur **Modifier la phrase d'authentification**.

   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 chiffrement

Pour importer une clé de cryptage :

1. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **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. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **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. Dans AppAssure 5 Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Sécurité**.
3. Cliquez sur le symbole de chevron droit **>** en regard du nom de la clé de cryptage 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.

Comprendre la réplication

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.

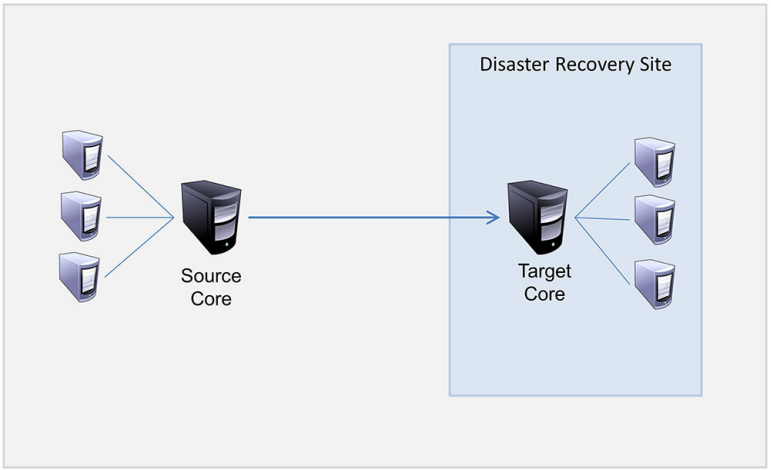

Figure 8. Diagramme de l'architecture de réplication de base

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

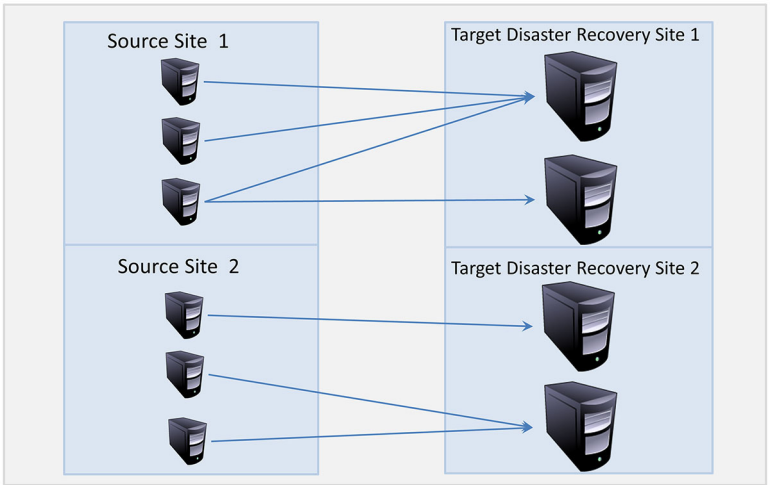

Figure 9. Diagramme de l'architecture de réplication multipoint

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 d'agents protégés, ce qui peut ajouter jusqu'à des centaines ou des milliers de gigaoctets de données. La réplication initiale peut être amorcée sous le noyau cible à l'aide de supports externes pour transférer les données initiales au noyau cible. En général, cela est utile pour les gros ensembles de données ou les sites dont les liens sont lents.

REMARQUE : Bien qu'il est 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 Mb/s, le transfert peut prendre plus de 40 jours à s'accomplir.

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 noyau 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 noyau 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 noyau source à l'emplacement du noyau cible à distance.
- La deuxième partie est la consommation, qui se produit lorsqu'un noyau cible reçoit le lecteur transporté et copie les données répliquées sur le référentiel. Le noyau cible consomme ensuite les points de restauration et les utilise pour former des agents répliqués.

REMARQUE : Tandis que la réplication d'instantanés incrémentiels peut se produire entre le noyau source et noyau cible avant la fin de l'amorçage, les instantanés répliqués transmis de la source au noyau 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 et de la restauration dans AppAssure 5

En cas de panne de courant entraînant des pannes du core source et de l'agent, AppAssure 5 prend en charge le basculement et la restauration dans des environnements répliqués. Le terme basculement désigne le passage à un AppAssure Core cible redondant ou de secours après panne du système ou arrêt anormal d'un core source et de ses agents associés. 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 l'agent (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 d'agents. Il importante de prendre en compte le nombre d'agents protégés par core source et le nombre que vous planifiez de répliquer vers la cible. AppAssure 5 vous permet d'effectuer la réplication sur la 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.

Tableau 1. Vitesse de modification maximale 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 5, vous devez configurer les cores source et cible pour la réplication. Après avoir configuré la réplication, vous pouvez répliquer les données d'agent, surveiller et gérer la réplication, et effectuer des restaurations.

L'exécution d'une réplication dans AppAssure 5 implique l'exécution des tâches suivantes :

- Configuration de la réplication autogérée. Pour plus d'informations sur la réplication d'un core cible autogéré, voir Réplication vers un core autogéré.
- Configuration de la réplication tierce. Pour plus d'informations sur la réplication d'un core cible tiers, voir Réplication vers un core géré par un tiers.
- Réplication d'un nouvel agent rattaché au core source. Pour plus d'informations sur la réplication d'un agent, voir Réplication d'un nouvel agent.
- Réplication d'un agent existant. Pour plus d'informations sur la configuration d'un agent pour la réplication, voir Réplication de données d'agent d'une machine.
- Définition de la priorité de réplication d'un agent. Pour plus d'informations sur la définition des priorités de réplication des agents, voir Définir 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.
- Gestion des paramètres de réplication si nécessaire. Pour plus d'informations sur la gestion des paramètres de réplication, voir Paramètres de gestion de réplication.
- Restauration des données répliquées en cas de sinistre ou de perte de données. Pour plus d'informations sur la restauration des données répliquées, voir Restauration de 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 5 Core sur toutes les machines source et cible. Si vous configurez AppAssure 5 pour une réplication multipoint à point, vous devez réaliser cette tâche sur tous les cores source et sur le core cible unique.

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 AppAssure 5 Core, cliquez sur l'onglet **Réplication**.
2. Dans le menu déroulant **Actions**, sélectionnez **Ajouter un core distant**.
   La boîte de dialogue **Sélectionner un type de réplication** s'affiche.
3. Sélectionnez **Je possède mon propre core distant vers lequel je souhaite répliquer**, puis entrez les informations telles que 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 5 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.

4. Cliquez sur **Continuer**.
5. Dans la boîte de dialogue **Ajouter un core distant**, sélectionnez l'une des options suivantes :

Option	Description
Remplacer un core répliqué existant	Remplace un core existant sur l'hôte distant par le core sélectionné dans la liste déroulante.
Créer un nouveau core répliqué sur <nom d'hôte>	Crée un core portant le nom affiché dans le champ sur la machine de core cible distante. **REMARQUE :** Il s'agit de la sélection par défaut. Le nom de core s'affiche automatiquement dans la zone de texte.

6. Sélectionnez les agents à répliquer, puis sélectionnez un référentiel pour chaque agent.
7. Si vous prévoyez d'effectuer un processus d'amorçage pour le transfert de la base de données, cochez la case en regard de l'option **Utiliser un lecteur d'amorçage pour effectuer un transfert initial.**
8. Cliquez sur **Démarrer la réplication**.
   - Si vous avez sélectionné l'option **Utiliser un lecteur de départ pour effectuer le transfert initial**, la boîte de dialogue **Copier dans le lecteur de départ** apparaît.
   - Si vous n'avez pas choisi d'utiliser un lecteur d'amorçage, la tâche est terminée.
9. Dans la boîte de dialogue **Copier vers le lecteur de départ**, saisissez les informations comme indiqué ci-dessous :

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.

Zone de texte	Description
	REMARQUE : Ceci est obligatoire si le lecteur d'amorçage est situé sur un partage réseau.
Taille maximale	Sélectionnez l'une des options suivantes : – La cible entière. – Une partie de l'espace disponible du lecteur. Ensuite, pour désigner une partie du lecteur, saisissez la quantité d'espace désirée dans la zone de texte et sélectionnez les dimensions.
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.
Agents	Sélectionnez les agents que vous souhaitez répliquer à l'aide du lecteur d'amorçage.

REMARQUE : Comme le programme doit copier d'importantes quantités de données vers le périphérique de stockage mobile, une connexion eSATA, USB 3.0 ou autre connexion haut débit sur ce périphérique de stockage mobile est recommandée.

10. Cliquez sur **Démarrer** pour écrire le lecteur de départ dans le chemin sélectionné.

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 procédure 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 la console AppAssure 5 Core sur le core cible, cliquez sur l'onglet **Réplication**.
3. Sous **Réplication entrante**, sélectionnez le core source correct à l'aide du menu déroulant, puis cliquez sur **Consommer**.
4. Saisissez les informations suivantes :

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.

5. 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 auto-géré.

6. 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 de départ en attente de la console AppAssure 5 Core 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 la console AppAssure 5 Core 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 à la réplication dans le cloud. Vous devez installer AppAssure 5 Core sur toutes les machines de core source. Si vous configurez AppAssure 5 pour une réplication multipoint à point, vous devez réaliser cette tâche sur tous les cores 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 5 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. Depuis le core source, naviguez jusqu'à l'AppAssure 5 Core, puis cliquez sur 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 agents à répliquer.
   b) Sélectionnez un référentiel pour chaque agent.
   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 de départ**, entrez les informations du lecteur de départ 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.
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 :

Zone de texte	Description
	– **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 fois que l'utilisateur a terminé la procédure Réplication vers un core géré par un tiers, 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 la console AppAssure 5 Core 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 distant**.
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. Vérifiez le **nom du core**, l'**adresse e-mail** du client et son **ID de client**, et modifiez les informations si nécessaire.
     2. 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 plus d'informations sur la vérification des demandes de réplication, voir Passage en revue d'une demande de réplication.

Pour ignorer une demande de réplication :

1. Dans la console AppAssure 5 Core sur le core cible, 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 :

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 date de création et la plage de dates.	Dans le menu déroulant, cliquez sur **Abandonner** pour abandonner ou annuler le processus de création des données de départ.
Réplication sortante	Affiche tous les cores cible sur lesquels le core source effectue une réplication. Il inclut le nom de core cible, l'état d'existence, le nombre des machines d'agent 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 choisir un hôte de la liste déroulante, sélectionner des agents

Section	Description	Actions disponibles
		répliqués pour la réplication et créer un lecteur d'amorçage pour le transfert initial du nouvel agent.
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 d'amorçage, 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 d'agents autorisés à répliquer vers le core cible à la fois.
Nombre maximal d'émissions parallèles	Indiquez le nombre de connexions réseau autorisées pour un seul agent afin de répliquer les données de cette machine à la fois.

4. Cliquez sur **Enregistrer**.

Suspension d'une réplication

Vous pouvez supprimer une réplication et retirer des machines protégées d'une réplication de plusieurs façons.

- Supprimer un agent de la réplication sur le core source

- Supprimer un agent du core cible
- Supprimer un core cible de la réplication
- 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.

Retrait d'un agent de la réplication sur le core source

Pour retirer un agent de la réplication sur le core source :

1. Depuis le core source, ouvrez la console AppAssure 5 Core, puis cliquez sur l'onglet **Réplication**.
2. Développez la section **Réplication sortante**.
3. Dans le menu déroulant de l'agent que vous souhaitez retirer de la réplication, cliquez sur **Supprimer.**
4. Dans la boîte de dialogue **Réplication sortante**, cliquez sur **Oui** pour confirmer la suppression.

Suppression d'un agent du core cible

Pour supprimer un agent du core cible

1. Depuis le core source, ouvrez l'AppAssure 5 Core Console, puis cliquez sur l'onglet **Réplication**.
2. Développez la section **Réplication entrante**.
3. Dans le menu déroulant de l'agent que vous souhaitez retirer de la réplication, cliquez sur **Supprimer**, puis sélectionnez l'une des options suivantes.

Option	Description
Relation seulement	Retire l'agent de la réplication mais conserve les points de restauration répliqués.
Avec point de restauration	Retire l'agent de la réplication et supprime tous les points de restauration reçus depuis cet ordinateur.

Suppression d'un core cible de la réplication

Pour supprimer un core cible de la réplication :

1. Depuis le core source, ouvrez la console AppAssure 5 Core, 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.

Suppression d'un core source de la réplication

REMARQUE : Le retrait d'un core source entraîne le retrait de tous les agents répliqués protégés par ce core.

Pour supprimer un core source de la réplication

1. Depuis le core source, ouvrez l'AppAssure 5 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 5 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 5, le basculement et la retauration 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 AppAssure 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 AppAssure 5 Core pour la source, puis installez un AppAssure 5 Core pour la cible.
   Pour en savoir plus, voir le *Guide de déploiement Dell DL4000* à l'adresse **dell.com/support/manuals**.
2. Installez un agent AppAssure 5 Agent à être protégé par le core source.
   Pour en savoir plus, voir le *Guide de déploiement Dell DL4000* à l'adresse **dell.com/support/manuals**.
3. Créez un référentiel sur le core source et une logithèque sur le core cible.
   Pour plus d'informations, voir Création d'un référentiel.
4. Ajoutez l'agent à protéger sous le core source.
   Pour plus d'informations, voir Protection d'une machine.

5. Configurez la réplication du core source vers le core cible, puis répliquez l'agent protégé avec tous les points de restauration.

   Suivez les instructions dans la section Configuration de la réplication d'un core auto-géré pour ajouter le core cible vers lequel vous allez effectuer la réplication.

Exécution d'un basculement vers le core cible

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 5 pour transférer la protection à votre 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. Naviguez jusqu'à la console AppAssure 5 Core 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 Effectuer une restauration.

Effectuer une restauration

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

Pour effectuer la restauration automatique :

1. Naviguez jusqu'à la console AppAssure 5 Core 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.

   Pour plus d'informations sur la création d'archives, voir Création d'une archive.

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.

   Pour plus d'informations, voir Importation d'une archive.
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.

    Pour plus d'informations, voir Stratégie d'exécution d'une restauration sans système d'exploitation (BMR) d'une machine Windows.

    REMARQUE : Lorsque vous lancez la restauration comme le décrit la section Lancement d'une restauration à partir de l'AppAssure 5 Core, 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.

    Pour plus d'informations, voir Configuration des paramètres de la machine.
18. Naviguez jusqu'à la console Core sur le core cible, puis supprimez l'agent de l'onglet **Réplication**.

    Pour plus d'informations, voir Suspension d'une 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.

    Pour plus d'informations, voir Configuration de la réplication d'un core auto-géré.

Gestion des événements

La gestion des événements facilite la surveillance de l'intégrité et de l'utilisation de l'AppAssure 5 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-mail, la réduction des répétitions et la rétention des événements. L'option Groupes de notification dans AppAssure 5 vous permet de gérer les groupes de notification groups, 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
- 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 l'AppAssure 5 Core Console, 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 :** – **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 du Dell PowerVault DL4000* sur **dell.com/support/manuals**.

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

1. Depuis l'AppAssure 5 Core Console, 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. 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. Dans AppAssure 5 Core, cliquez sur 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. Dans AppAssure 5 Core, cliquez sur 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

L'AppAssure 5 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 Recovery Assure 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 5 vous permet d'afficher les informations concernant l'AppAssure 5 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'à l'AppAssure 5 Core, puis sélectionnez l'onglet **Outils**.
2. Depuis l'option **Outils**, sélectionnez **Infos système**.

Téléchargement des programmes d'installation

AppAssure 5 vous permet d'installer des programmes d'installation depuis l'AppAssure 5 Core. Téléchargez 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 Téléchargement et installation du programme d'installation de l'agent. Pour savoir comment déployer le programme d'installation de l'agent, voir le *Guide de déploiement de Dell DL4000* à l'adresse **dell.com/support/manuals**. Pour accéder au programme d'installation du Local Mount Utility, voir À propos de Local Mount Utility et pour en savoir plus sur le Local Mount Utility, voir 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 5 Agent sur les ordinateurs destinés à être protégés par l'AppAssure 5 Core. Si vous déterminez que vous avez un ordinateur qui exige le programme d'installation de l'agent, vous pouvez télécharger ce programme depuis l'onglet **Outils** dans l'AppAssure 5 Core.

REMARQUE : Le téléchargement du Core est effectué depuis le portail de licences. Pour télécharger le programme d'installation de l'AppAssure 5 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 d'AppAssure 5 Agent sur n'importe quelle machine qui sera protégée par l'AppAssure 5 Core.

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

1. Téléchargez le fichier de programme d'installation d'AppAssure 5 Agent depuis le portail de licences AppAssure 5 ou depuis l'AppAssure 5 Core.

   Par exemple : **Agent-X64-5.3.xxxxx.exe**

2. Cliquez **Enregistrer le fichier**.

   Pour en savoir plus sur l'installation des agents, voir le *Guide de déploiement Dell DL4000* à l'adresse **dell.com/support/manuals**.

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 AppAssure 5 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 un AppAssure 5 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 la console AppAssure 5 Core. 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 AppAssure 5 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 console AppAssure 5 Core, 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.

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 où le point de restauration est stocké. Comme le décrit la section Ajout d'un core à l'utilitaire 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 :

Zone de texte	Description
	– 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.

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.

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 AppAssure 5 Core et les options d'agent

En effectuant un clic droit sur le core ou l'agent AppAssure 5 dans l'écran LMU principal, vous pouvez utiliser certaines options, notamment :

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

Options d'accès Hôtelocal

Pour accéder aux options d'hôte local (Localhost), effectuez un clic droit sur le core ou l'agent AppAssure 5, puis sélectionnez **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 AppAssure 5, 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.

Options d'accès à l'agent

Pour accéder aux options d'agent, effectuez un clic droit sur le core ou l'agent AppAssure 5, 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 de stratégie de rétention.

À propos de l'archivage

Les stratégies de rétention définissent les périodes de stockage des sauvegardes sur support à court terme (rapide et cher). Parfois, certaines contraintes techniques et d'entreprise nécessitent une prolongation de la rétention de ces sauvegardes, 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 5 sert à prendre en charge la rétention étendue des données de conformité et de non-conformité ; elle sert aussi à créer des données de départ de réplication sur un core 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.
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 :

Zone de texte	Description
	– 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**.

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 AppAssure 5 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 et 2012. 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 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. Dans la console Core, cliquez sur l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Capacité d'attachement**.
   La fenêtre **Paramètres de capacité d'attachement** apparaît.
3. Pour réaliser les vérifications de capacité d'attachement pour les bases de données SQL protégées, sélectionnez l'instance SQL Server locale.
   Choisissez parmi les options suivantes :
   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
4. Sélectionnez le type de référence.
   Choisissez parmi les options suivantes :
   - **Windows**
   - **SQL**
5. 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.

6. 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.
7. Cliquez sur **Appliquer**.

Vous pouvez maintenant exécuter les vérifications de capacité d'attachement sur les bases de données SQL Server protégées.

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 d'AppAssure 5 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. Cliquez sur **Paramètres SQL Server**.

   La boîte de dialogue **Paramètres SQL Server** s'affiche.
3. Sélectionnez ou supprimez les paramètres SQL Server suivants en fonction des besoins de votre organisation :

   - **Activer la vérification de capacité d'attachement nocturne**
   - **Activer la troncature nocturne des journaux**
4. Cliquez sur **OK**.

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

   REMARQUE : Ces étapes doivent être réalisées pour chacune des machines protégées sous le core. Pour plus d'informations sur le forçage de la troncature des journaux, voir Forcer la troncature des journaux.

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

Lorsque vous utilisez AppAssure 5 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 5 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 d'AppAssure 5 Core, 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 gauche d'AppAssure 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 des instructions sur la façon d'afficher l'état des vérifications de capacité d'attachement, voir Affichage d'événements et d'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 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 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 d'événements et d'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. Naviguez jusqu'à la console AppAssure 5 Core, puis sélectionnez l'onglet **Machines**.
2. Dans l'onglet **Ordinateurs**, 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 de 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 en savoir plus sur l'affichage des points de restauration, voir Affichage de points de restauration.

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

Tableau 2. 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.

Tableau 3. Couleurs d'état des points de restauration des bases de données Exchange

Couleur d'état	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.

Couleur d'état	Description
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.

4

Gestion de l'appliance DL4000 Backup To Disk

La console AppAssure 5 Core 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 DL4000 Backup To Disk

Vous pouvez surveiller l'état des sous-systèmes d'appliance DL4000 Backup To Disk à l'aide de l'onglet **Appliance**, page **État global**. Cette page affiche un voyant d'état près de chaque sous-système, ainsi qu'une description de l'état, qui spécifie 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/manuals**. 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. Pour plus d'informations sur le provisionnement du stockage, voir Provisionnement du stockage.

Affichage de l'état des contrôleurs de l'appliance DL4000 Backup To Disk

Vous pouvez utiliser l'onglet **Appliance** → lien **Contrôleurs** pour afficher l'état des contrôleurs installés. La page Contrôleurs affiche les éléments suivants :

- Condition
- Nom du contrôleur
- État actuel
- Nombre de connecteurs
- Taille du cache en mégaoctets (Mo)
- Version du micrologiciel
- Version du pilote

Si l'état du contrôleur n'est pas vert ou si le statut indiqué n'est pas OK, vous pouvez utiliser le lien **État global** afin de lancer l'application OpenManage Server Administrator pour dépanner les éventuels avertissements ou erreurs. Pour plus d'informations sur l'accès à l'application OpenManage Server Administrator, voir Surveillance de l'état de l'appliance DL4000 Backup To Disk.

Affichage de l'état des enceintes

Vous pouvez afficher des détails concernant les enceintes DL4000 Backup To Disk Appliance, en cliquant sur l'onglet **Appliance** et en sélectionnant **Enceintes**. L'écran Enceintes affiche les informations suivantes :

- État de l'enceinte
- Nom de l'enceinte
- Numéro de service de l'enceinte
- Statut de l'enceinte
- Nombre de lecteurs installés dans l'enceinte
- Capacité totale de l'enceinte
- Nom du contrôleur
- Version du micrologiciel de l'enceinte
- Position dans la chaîne d'enceintes

Vous pouvez effectuer une analyse en cascade (drill down) pour consulter les détails des disques physiques : cliquez sur **>** en regard de l'option **État**. La section **Disques physiques** répertorie chacun des disques physiques, son état, son nom, son statut, sa capacité en gigaoctets (Go) et son type de bus.

Pour une analyse en cascade (drill down) plus poussée concernant les détails des disques physiques, cliquez sur **>** en regard de l'option **État**. La section **Détails** du disque physique affiche les informations suivantes :

- **Numéro/ID fournisseur)**
- **Numéro/ID de produit**
- **Numéro de série**
- **Numéro de pièce**
- **Version du micrologiciel**
- **Échec prévu**
- **Disque de rechange**

Affichage de l'état des disques virtuels

Vous pouvez afficher des détails concernant les disques virtuels DL4000 Backup To Disk Appliance, en cliquant sur l'onglet **Appliance** et en sélectionnant **Disques virtuels**. L'écran Disques virtuels affiche les informations suivantes :

- État des disques virtuels
- Nom de chaque disque virtuel
- Statut de chaque disque virtuel
- Nom du contrôleur où réside le disque virtuel
- Nom de l'enceinte contenant le disque virtuel
- Niveau de RAID du disque virtuel
- Capacité totale de chaque disque virtuel

Vous pouvez effectuer une analyse en cascade (drill down) pour consulter les détails des disques physiques : cliquez sur **>** en regard de l'option **État**. La section **Disques physiques** indique le nom du volume Windows et la taille de l'élément de division en bandes. La section **Disques physiques** répertorie aussi chacun des disques physiques, son état, son nom, son statut, sa capacité en gigaoctets (Go) et son type de bus.

Pour une analyse en cascade (drill down) plus poussée concernant les détails des disques physiques, cliquez sur **>** en regard de l'option **État**. La section **Détails** du disque physique affiche les informations suivantes :

- **Numéro/ID fournisseur)**

- **Numéro/ID de produit**
- **Numéro de série**
- **Numéro de pièce**
- **Version du micrologiciel**
- **Échec prévu**
- **Disque de rechange**

Provisionnement du stockage

L'appliance configure le stockage interne DL4000 disponible et tout boîtier de stockage externe attaché pour :

- Référentiels AppAssure
- Mode Veille virtuelle des machines protégées

REMARQUE : Seuls les MD1200 dotés de lecteurs de 1, 2, 3 ou 4 To (capacité élevée) connectés au contrôleur H810 sont pris en charge. Le programme prend en charge un seul MD1200 pour l'appliance d'édition Standard et deux MD1200 pour l'appliance d'éditon High Capacity (Capacité élevée).

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 le DL4000.

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**.

   L'écran **Tâches** affiche la capacité de stockage interne disponible pour l'appliance. Cette capacité est utilisée pour créer un nouveau référentiel AppAssure.

   PRÉCAUTION : Avant de passer à l'étape 2 de cette procédure, ouvrez la fenêtre Provisionnement du stockage en cliquant sur Provisionner dans la colonne Action, en regard du stockage à provisionner. Dans la section Action de tâche de provisionnement, vérifiez que vous avez bien coché la case en regard de Faire ceci pour une seule tâche de provisionnement si plusieurs tâches sont provisionnées simultanément, sauf si vous souhaitez créer une réserve sur la première enceinte (dans ce cas, vous laissez cette option sélectionnée). Dans la section Réserve de stockage facultative, cochez la case en regard de l'option Allouer une portion du stockage provsionné aux machines virtuelles de secours et autres, puis indiquez le pourcentage du stockage à allouer. Sinon, le pourcentage de stockage indiqué dans le champ Réserve de stockage facultative correspond à l'ensemble des disques rattachés.
2. Cliquez sur **Provisionner tout**.

REMARQUE : Par exemple, si vous avez choisi d'allouer 30 % du stockage aux VM de secours, la commande **Provisionner tout** provisionne le stockage interne à raison de 70 % pour le référentiel et 30 % pour les VM de secours. Si vous avez désélectionné l'option **Faire ceci pour une seule tâche de provisionnement si plusieurs tâches sont provisionnées simultanément**, alors tout le stockage externe est provisionné, à 100 %, pour le référentiel, qui est ajouté comme espace de stockage supplémentaire pour le référentiel que vous créez dans le stockage interne.

Provisionnement du stockage sélectionné

Pour provisionner le stockage sélectionné :

1. Dans l'onglet **Appliance**, cliquez sur **Tâches**.

   L'écran **Tâches** affiche la capacité de stockage interne et de stockage externe disponible pour l'appliance, indique si elle est disponible pour le provisionnement ou déjà provisionnée, et précise s'il existe une condition interdisant le provisionnement automatique du stockage. Cette capacité est utilisée pour créer un référentiel AppAssure 5.

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**, vous pouvez sélectionner l'option qui permet d'allouer une portion du stockage aux machines virtuelles de secours, puis spécifier le pourcentage de stockage à allouer à ces VM.

4. Vous pouvez choisir de désélectionner la case à cocher **Faire ceci pour une seule tâche de provisionnement si plusieurs tâches sont provisionnées simultanément** (cochée par défaut).

   Si vous désélectionnez cette option, le pourcentage de stockage sélectionné est appliqué uniquement au périphérique de stockage sélectionné. Si vous activez l'option, le pourcentage est appliqué au stockage sélectionné à la fois pour les enceintes de stockage interne et pour le stockage externe.

5. Cliquez sur **Provisionner**.

   Le provisionnement de disque comment et l'état de création du référentiel AppAssure s'affiche dans la zone **État** de l'écran **Tâches**. Le champ **Description de l'état** affiche **Provisionné**.

6. 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 la console AppAssure 5 Core, 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 la console AppAssure 5 Core (onglet **Appliance**, écran **Tâches**) comme étant disponible pour provisionnement.

Résolution des tâches ayant échoué

AppAssure 5 fait un rapport des tâches de vérification, de provisionnement et de restauration qui échouent, en créant un événement dans la page Accueil de la console AppAssure 5 Core, 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 l'appliance DL4000 Backup To Disk

Avant de lancer le processus de mise à niveau, veillez à arrêter les services AppAssure Core.

Pour mettre à niveau l'appliance DL4000 Backup to Disk :

1. Téléchargez **Recovery and Update Utility** (RUU, Utilitaire de restauration et de mise à jour) depuis le site **dell.com/support** sur l'appliance DL4000 Backup to Disk.
2. Copiez l'utilitaire sur le bureau de l'appliance et extrayez les fichiers.
3. Double-cliquez sur l'icône **Lancer RUU**.
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.

   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 AppAssure 5 Core démarre.

Réparation de l'appliance DL4000 Backup To Disk

Avant de lancer le processus de réparation, veillez à arrêter les services AppAssure Core.

Pour réparer l'appliance DL4000 Backup to Disk :

1. Téléchargez **Recovery and Update Utility** (RUU, Utilitaire de restauration et de mise à jour) depuis le site **dell.com/support** sur l'appliance DL4000 Backup to Disk.
2. Copiez l'utilitaire sur le bureau de l'appliance et extrayez les fichiers.

3. Double-cliquez sur l'icône **Lancer RUU**.
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**.

    La console AppAssure 5 Core démarre.

5

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

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

Pour protéger vos données avec AppAssure 5, vous devez ajouter les postes de travail et les serveurs à protéger à la console AppAssure 5 Core ; par exemple, ajoutez votre serveur Exchange, votre serveur SQL ou votre serveur Linux.

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

Dans la console AppAssure 5, vous pouvez identifier la machine où un agent AppAssure 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 console AppAssure 5 Core 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 la console AppAssure 5 Core, cliquez sur l'onglet **machines/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. Nom de cette machine tel qu'il doit s'afficher dans la console AppAssure 5 Core. 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.

Zone de texte	Description
Port	Entrez un numéro de port pour la machine. Le core utilise ce port pour communiquer avec cette machine.
Référentiel	Sélectionnez le référentiel pour les points de restauration. Affiche sur AppAssure 5 Core le référentiel dans lequel les données de cette 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 chiffrement	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'une machine

L'AppAssure 5 Core Console offre une vue d'ensemble de 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 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. Cliquez sur l'onglet **Outils**, puis cliquez sur **Informations système**.

   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

   Les informations détaillées sur les volumes de cette machine comprennent :
   - Processeurs
   - Type de processeurs
   - Cartes réseau
   - Les adresses IP associées à cette machine

Configuration de groupes de notification pour les événements système

Dans AppAssure 5, 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 les 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)** – **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 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. Naviguez jusqu'à la console AppAssure 5 Core, 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.

Zone de texte	Description
	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** **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.

Zone de texte	Description
	– **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 Processus de modification des paramètres de 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**

Zone de texte	Description
...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**
...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 sur la licence actuelle correspondant au logiciel agent AppAssure installé sur une machine.

Pour afficher les informations de licence

1. Dans la console Core, cliquez sur l'onglet **Machines**.
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 5, vous pouvez modifier les horaires de protection de 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

Dans AppAssure 5, vous pouvez modifier les paramètres pour gérer les processus de transfert de données d'une machine protégée. Les paramètres de transfert décrits à cette section sont définis au niveau de l'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 AppAssure. 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 Dell AppAssure.

Il existe trois types de transfert dans AppAssure 5 :

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.

Dans AppAssure 5, le transfert de données implique la transmission d'un volume de données sur un réseau, des machines d'agent AppAssure 5 vers le core. En cas de réplication, le transfert se produit également du core d'origine (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.

Zone de texte	Description
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 – 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'a pas été réalisée dans ce délai, le programme effectue une nouvelle tentative.
Expiration du délai d'attente d'écriture réseau	Spécifie (en minutes et secondes) la durée maximale d'attente d'établissement d'une connexion d'écriture. Si l'écriture réseau n'a pas été réalisée dans ce délai, le programme effectue une nouvelle tentative.

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, il peut être utile de consulter les journaux pour effectuer le dépannage.

Pour afficher les journaux de machine

1. Dans la console Core, cliquez sur l'onglet **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 AppAssure 5 Agent sur la machine pour pouvoir la protéger. Vous pouvez choisir d'installer l'agent à l'avance, avant de réaliser la présente procédure, ou de le déployer pendant que vous définissez la protection dans la boîte de dialogue **Connexion**. Pour connaître les étapes spécifiques d'installation du logiciel d'agent pendant le processus de protection de la machine, voir Déploiement du logiciel de l'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 d'agent, redémarrez la machine sur laquelle vous avez installé le logiciel AppAssure 5 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 AppAssure 5 Core communique avec l'agent de 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 d'agent n'est pas encore installé sur la machine choisie, suivez la procédure 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	Ce champ de texte affiche le nom d'hôte ou l'adresse IP que vous avez indiquée dans la boîte de dialogue **Connexion**. (Facultatif) Entrez un nouveau nom pour la machine, qui sera affiché dans la console AppAssure 5 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 l'AppAssure 5 Core dans lequel les données de cette machine 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 chiffrement d'un référentiel se définissent dans l'onglet **Configuration** de l'AppAssure 5 Core Console.
Suspendre initialement la protection	Une fois que vous avez ajouté une machine à la liste de protection, AppAssure 5 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,

Champ	Description
	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. Pour plus d'informations sur la modification de la planification de protection du volume sélectionné, voir 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) commence immédiatement à se transférer vers le référentiel sur le core AppAssure 5, 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'ouvre.

2. Cliquez sur **Oui** pour déployer à distance le logiciel d'agent sur l'ordinateur.

   La boîte de dialogue **Déployer l'agent** s'ouvre.

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 par l'intermédiaire duquel l'AppAssure 5 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** : précise pour l'ordinateur un nom qui s'affiche sur l'AppAssure 5 Core Console. Ce nom peut être identique au nom d'hôte.
   - **Protéger l'ordinateur après l'installation** : si vous sélectionnez cette option, AppAssure 5 peut prendre un instantané de base des données après que vous ajoutez un ordinateur à protéger. Cette option est sélectionnée par défaut. Si vous la désélectionnez, vous devez forcer une prise d'instantané manuelle lorsque vous êtes prêt à démarrer la protection des données. Pour en savoir plus sur le forçage manuel d'un instantané, voir Forcer un instantané dans le *Guide d'utilisation de PowerVault DL4000* sur **dell.com/support/manuals**.
   - **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 : Les paramètres de chiffrement d'un référentiel se définissent dans l'onglet **Configuration** de l'AppAssure 5 Core Console.

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 Protection d'une machine pour plus d'informations sur l'accès à cette boîte de dialogue), sous **Groupes de volumes**, sélectionnez le volume à protéger, puis cliquez sur **Modifier**.
   La boîte de dialogue **Planification de protection** s'ouvre.

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'Exchange Server

Pour protéger les données d'un serveur Microsoft Exchange, vous devez configurer des paramètres supplémentaires dans l'AppAssure 5 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 la console AppAssure 5 Core.

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 5 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 5 vous permet de déployer le AppAssure 5 Agent Installer pour la protection de machines individuelles Windows. Complétez les étapes de la procédure suivante pour lancer le programme d'installation en mode Pousser vers un agent. Pour déployer simultanément des agents vers plusieurs machines, voir 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 pour spécifier si le core devra démarrer lorsque le déploiement et l'installation du programme d'installation d'AppAssure 5 Agent seront terminés.

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 une protection à un agent AppAssure 5 sur un core source, AppAssure 5 vous offre l'option de répliquer le nouvel agent vers un core cible existant.

Pour plus d'informations sur la réplication, voir Comprendre la réplication.

Pour répliquer un nouvel agent :

1. Naviguez vers l'AppAssure 5 Core Console, puis sélectionnez l'onglet **Machines** (Ordinateurs).
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 l'AppAssure 5 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 un nom pour la machine ; ce nom s'affichera dans l'AppAssure 5 Core Console.
Référentiel	Sélectionnez le référentiel sur l'AppAssure 5 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 chiffrement d'un référentiel se définissent dans l'onglet **Configuration** de l'AppAssure 5 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, pour la suspendre jusqu'au moment suivant où AppAssure 5 prend 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 les 15 minutes. Pour des informations sur les planifications personnalisées, voir Création d'horaires personnalisés pour les volumes.
Suspendre initialement la protection	Cochez cette case si vous souhaitez suspendre la protection; par exemple, pour empêcher AppAssure 5 de prendre une image de base jusqu'après les heures de forte utilisation.

6. Cliquez sur **Protéger**.

Gestion des ordinateurs

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. Naviguez jusqu'à la console AppAssure 5 Core, 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 qui lie deux cores (cible et source) sur un même site ou sur deux sites liés par une connexion réseau 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 vers le 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 plus d'informations sur la réplication, voir Comprendre la réplication.

Pour répliquer des données d'agent sur une machine :

1. Dans l'AppAssure 5 Core Console, cliquez sur l'onglet **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 la console AppAssure 5 Core, accédez à l'ordinateur protégé pour lequel vous souhaitez établir 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 l'AppAssure 5 Core Console, cliquez sur l'onglet **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 la console AppAssure Core, 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 **Récapitulatif** apparaît.

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 ordinateurs

Cette rubrique décrit les tâches que les administrateurs devront effectuer pour déployer le logiciel AppAssure 5 Agent simultanément sur plusieurs ordinateurs.

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

1. Déployer AppAssure 5 sur plusieurs ordinateurs.
   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 Suivi 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 Bulk Deploy (Déploiement en masse) d'AppAssure 5. Vous pouvez effectuer des déploiement en masse vers :

- 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 5 utilise la version Web du programme d'installation de l'agent AppAssure 5 pour déployer les composants d'installation. Si aucun accès à Internet n'est disponible, vous pouvez installer le programme d'installation de l'AppAssure 5 Agent 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 Installation en mode Push du programme d'installation de l'agent depuis la machine de core. Vous pouvez télécharger les mises à jour du core et de l'agent depuis le portail de licences. Pour plus d'informations sur ce portail, voir À propos du portail de licences AppAssure 5.

Installation en mode Push du programme d'installation de l'agent depuis la machine de 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 de core. L'appliance DL4000 Backup to Disk 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 AppAssure 5. Pour plus d'informations sur le portail de licences, voir À propos du portail de licences AppAssure 5

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

1. Sur la machine core, copiez le fichier d'installation de l'agent **Agent-X64–5.x.x.xxxxx.exe** vers le répertoire **C:\Program Files\apprecovery\core\installers**.
2. Dans la console AppAssure 5 Core, cliquez sur l'onglet **Configuration**, puis 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 AppAssure 5 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 5, 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	Le numéro du port sur lequel l'AppAssure 5 Core communique avec l'agent sur l'ordinateur.
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 AppAssure 5 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**.
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 5 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 5 peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure 5 est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure 5 ne peut pas se connecter à la machine. Cela peut être parce-que les références de connexion sont incorrectes, la machine est hors tension, le pare-feu bloque

Zone de texte	Description
	le trafic, ou autre. Pour corriger le problème, cliquez sur **Modifier les paramètres** dans la barre d'outils ou sur 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 5, 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 5 ne peut pas détecter le nom d'hôte de la machine virtuelle sur laquelle effectuer le déploiement. Au lieu du nom d'hôte, AppAssure 5 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 AppAssure 5 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 5, 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, voir Déploiement sur des machines d'un domaine Active Directory.
6. Vérifiez qu'AppAssure 5 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 5 peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure 5 est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure 5 ne peut pas se connecter à la machine. Cela peut être parce-que les références de connexion sont incorrectes, la machine est hors tension, le pare-feu bloque

Zone de texte	Description
	le trafic, ou autre. Pour corriger le problème, cliquez sur **Modifier les paramètres** dans la barre d'outils ou sur 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 console AppAssure 5 Core, 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 un 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, voir Déploiement sur des machines d'un domaine Active Directory.
4. Vérifiez qu'AppAssure 5 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**.

   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 5 peut se connecter à la machine et est prêt pour le déploiement.
Icône jaune	AppAssure 5 est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure 5 ne peut pas se connecter à la machine. Cela peut être parce-que les références de connexion sont incorrectes, la machine est hors tension, le pare-feu bloque le trafic, ou autre. Pour corriger le problème, cliquez sur **Modifier les paramètres** dans la barre d'outils ou sur 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 ordinateurs

Vous pouvez afficher l'avancement du déploiement du logiciel de l'agent AppAssure 5 vers les ordinateurs.

Pour surveiller le déploiement de plusieurs ordinateurs :

1. Depuis la console AppAssure 5 Core, 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 AppAssure 5 Agent vers les machines Windows, vous devez les protéger pour protéger vos données. Si vous avez sélectionné **Protéger l'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 la console AppAssure 5 Core, 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 en savoir plus sur l'exécution de chaque option, voir 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 de port que le core AppAssure 5 utilise pour communiquer avec l'agent sur la machine.
Référentiel	Sélectionnez le référentiel sur l'AppAssure 5 Core dans lequel les données de ces 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 Modification des horaires 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 5 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 5 est en mesure de se connecter à la machine et est prêt à être protégé.
Icône jaune	AppAssure 5 est en mesure de se connecter à la machine ; toutefois, l'agent est déjà associé à une machine core.
Icône rouge	AppAssure 5 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**.

Suivi de la protection de plusieurs machines

Suivez l'avancement de l'application des stratégies et des horaires aux ordinateurs par AppAssure 5.

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 une collection d'instantanés de volumes de disque distincts, capturés et stockés dans le référentiel. Les instantanés capturent et stockent l'état d'un volume de disque à un point dans le temps précis, alors que l'application qui génère les données est toujours en cours d'exécution. Dans AppAssure 5, vous pouvez forcer la prise d'instantané, suspendre temporairement les instantanés, afficher la liste des points de restauration actuellement stockés dans le référentiel et en supprimer certains si nécessaire. Les points de restauration servent à restaurer des machines protégées ou à monter des données sur un système de fichiers local.

AppAssure 5 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 5 utilise un pilote de filtre de volume à niveau faible, qui s'attache aux volumes montés puis suit toutes les modifications au niveau du bloc pour le prochain instantané prévu. Microsoft Volume Shadow Services (VSS) est utilisé pour faciliter la prise d'instantanés conformes à l'échec 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 particulier

Pour afficher un point de restauration particulier :

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 **>** en regard d'un point de restauration dans la liste pour développer la vue.

   Vous y trouverez des informations plus détaillées concernant le contenu des points de restauration de la machine sélectionnée et vous pourrez accéder à toute une variété d'opérations pouvant être exécutée sur le point de restauration, comme l'indique 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 pour 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, voir 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 d'une restauration à partir de l'AppAssure 5 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 AppAssure 5 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 la console AppAssure 5 Core, 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 la console AppAssure 5 Core, cliquez sur 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 la console AppAssure 5 Core, cliquez sur 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 un ordinateur 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. À l'invite, entrez l'adresse IP ou 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 <numéro_ligne_ordinateur>`

   REMARQUE : Vous pouvez aussi saisir le numéro d'identification de l'ordinateur dans cette commande au lieu du numéro d'objet de 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 <numéro_identification_de_point_de_restauration_de_volume> <chemin>`

   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 <numéro_de_ligne_ordinateur> <numéro_de_ligne_de_point_de_restauration> <lettre_de_volume> <chemin>`. 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 <chemin au volume>`. Dans cette commande, `<chemin au 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'un ordinateur donné à partir du référentiel. Lorsque vous supprimez des points de restauration dans AppAssure 5, 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 5 Core, sélectionnez l'ordinateur 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. Pour plus d'informations sur le forçage d'une image de base, voir Forcer un instantané.

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 la console AppAssure 5 Core, 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 la console AppAssure 5 Core, 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 l'AppAssure 5 Core Console, 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

À l'aide d'AppAssure, 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 target), vous pouvez uniquement exporter les données depuis le core cible une fois que la réplication initiale est terminée. Pour plus de détails, voir Réplication de données d'agent d'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 ReFS (Resilient File System, système de fichiers résilient). Pour plus de détails, consultez le manuel « *Dell DL4000 Deployment Guide* » (Guide de déploiement Dell DL4000), à l'adresse **dell.com/support/manuals**.

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

AppAssure 5 prend en charge l'exportation ponctuelle et l'exportation en continu (pour prendre en charge les disques virtuels de secours) des informations de sauvegarde Windows vers une machine virtuelle. L'exportation de vos données vers une machine de secours virtuelle pour procure une copie haute disponibilité des données. Si une machine protégée tombe en panne, vous pouvez effectuer l'amorçage sur la machine virtuelle, puis réaliser une restauration.

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

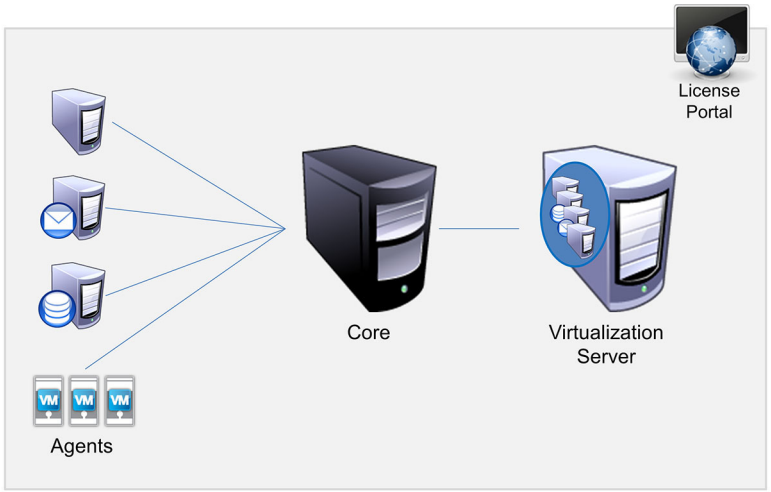

Figure 10. Exportation de données vers une machine virtuelle

Vous créez un disque virtuel de secours en exportant en continu les données protégées depuis votre machine Windows vers une machine virtuelle (VMware, ESXi et Hyper-V). 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.

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

Limites de support des volumes dynamiques et de base

AppAssure 4.x et 5.x prennent tous les deux en charge la création d'instantanés de tous les volumes dynamiques et de base. AppAssure 4.x et 5.x prennent aussi en charge l'exportation des volumes dynamiques simples résidant sur un seul disque physique. Comme leur nom l'indique, les volumes dynamiques simples ne sont pas divisés en bandes, mis en miroir ni fractionnés. Les volumes dynamiques non simples comportent des géométries de disque arbitraires impossibles à interpréter entièrement, ce qui empêche AppAssure de les exporter. AppAssure 5 permet d'exporter des volumes dynamiques complexes ou non simples.

Les volumes dynamiques non simples comportent des géométries de disque arbitraires impossibles à interpréter entièrement, ce qui empêche AppAssure de les exporter. Ni Replay 4.x, AppAssure 5.x ne permettent 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 Windows vers une machine virtuelle

Dans AppAssure 5, vous pouvez exporter des données à partir de vos machines Windows vers une machine virtuelle (VMware, ESXi et Hyper-V) 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 machine.

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

1. Dans l'AppAssure 5 Core Console, 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

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

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

Dans AppAssure 5, vous pouvez choisir d'exporter les données à l'aide de l'exportation ESXi en effectuant une exportation ponctuelle ou continue.

Effectuer 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** .

Effectuer 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 l'ordinateur hôte.
Port	Saisissez le port pour l'ordinateur hôte. Le port par défaut est 443.
Nom d'utilisateur	Entrez les références de connexion de l'ordinateur hôte.
Mot de passe	Entrez les références de connexion de l'ordinateur 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	Entrez un nom pour la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire. Vous avez le choix entre : – Utiliser la même quantité de RAM que l'ordinateur source – Utiliser une quantité spécifique de RAM, puis spécifier le montant en Mo
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.
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 5, vous pouvez choisir d'exporter des 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 l'exportation VMware Workstation correspondant au type d'exportation approprié.

Effectuer une exportation VMware Workstation ponctuelle

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 uniques pour effectuer une exportation VMware Workstation

Pour définir des paramètres ponctuels pour effectuer une exportation VMware Workstation

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 :** Le nom par défaut est le nom de la machine source.
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 VMware Workstation continue (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 :** Le nom par défaut est le nom de la machine source.
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 autorisée est de 512 Mo, et le maximum dépend de la capacité et des limites de la machine hôte.

6. Cliquez sur **Effectuer une exportation ad-hoc initiale** pour tester l'exportation des données.
7. Cliquez sur **Enregistrer**.

Exportation de données à l'aide de l'exportation Hyper-V

Dans AppAssure 5, vous pouvez choisir d'exporter des 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 correspondant au type d'exportation approprié.

Effectuer une exportation Hyper-V unique

Pour effectuer une exportation Hyper-V 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 Hyper-V - Sélectionner un point de restauration** s'affiche.
3. Sélectionnez un point de restauration pour exporter, puis cliquez sur **Suivant.**
   La boîte de dialogue **Hyper-V** s'ouvre.

Définition de paramètres uniques pour effectuer une exportation Hyper-V

Pour définir des paramètres uniques 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 de l'hôte Hyper-V	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.
Emplacement de la machine VM	Entrez le chemin d'accès de la machine virtuelle. Par exemple, **D:\export**. Cette valeur sert à identifier l'emplacement de la machine virtuelle. **REMARQUE :** Indiquez l'emplacement de la machine virtuelle pour les serveurs Hyper-V locaux et distants. Le chemin d'accès doit être un chemin d'accès local valide pour le serveur Hyper-V. Les répertoires non existants sont créés automatiquement. Ne tentez pas de les créer manuellement. L'exportation vers des dossiers partagés, par exemple, **\\data\share** n'est pas autorisée.

3. À l'onglet **Exporter les volumes**, sélectionnez les volumes à exporter ; par exemple, **C:**.
4. Sélectionnez l'onglet **Options**, puis entrez le nom de la machine virtuelle dans la zone de texte **Nom de machine virtuelle**.
   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.

5. Effectuez l'une des opérations 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 de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo.
6. Cliquez sur **Exporter**.

Exécution d'une exportation Hyper-V continue (disque de secours virtuel)

Pour effectuer une exportation Hyper-V ponctuelle

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 **Hyper-V** s'ouvre.
3. Cliquez sur l'option **Utiliser la machine locale** pour effectuer l'exportation Hyper-V vers une machine locale auquel le rôle Hyper-V est attribué.
4. 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 de l'hôte Hyper-V	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.
Emplacement de la machine VM	Entrez le chemin d'accès à la machine virtuelle. Par exemple, **D:\export**. Ce nom sert à identifier l'emplacement de la machine virtuelle. **REMARQUE :** Indiquez l'emplacement de la machine virtuelle pour les serveurs Hyper-V locaux et distants. Vous devez indiquer un chemin d'accès local valide pour le serveur Hyper-V. Les répertoires qui n'existent pas sont créés automatiquement. Ne tentez pas de les créer manuellement. L'exportation vers des dossiers partagés (par exemple, **\\data\share**) n'est pas autorisée.

5. Dans l'onglet **Exporter les volumes**, sélectionnez les volumes à exporter ; par exemple, **C:**.
6. Sélectionnez l'onglet **Options**, puis entrez le nom de la machine virtuelle dans la zone de texte Nom de machine virtuelle.
   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
7. Effectuez l'une des opérations 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 de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo.

8. Cliquez sur **Effectuer une exportation ad-hoc initiale** pour tester l'exportation des données.
9. Cliquez sur **Enregistrer**.

Exécution d'une restauration (rollback)

Dans AppAssure 5, une restauration consiste à restaurer les volumes sur un ordinateur depuis des points de restauration.

REMARQUE : La fonctionnalité de restauration (rollback) est également prise en charge sur vos machines Linux protégées, avec l'utilitaire de ligne de commande `aamount`. Pour en savoir plus, voir Exécution d'une restauration (rollback) pour une machine Linux avec la ligne de commande.

Pour effectuer une restauration (rollback) :

1. Dans la console AppAssure 5 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 5 Core, sélectionnez la machine à restaurer (rollback) 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 5, 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 l'AppAssure 5 Core Console. Pour en savoir plus, voir Exécution d'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 récemment montés pour 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 sans système d'exploitation après un amorçage sur un disque Live CD. Pour plus d'informations, voir Exécution d'une restauration sans système d'exploitation 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 sans système d'exploitation pour des 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 5 permet d'effectuer une BMR (Bare Metal Restore - Restauration sans système d'exploitation) de vos ordinateurs Windows, que la 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, connecter l'instance de console de restauration, adresser des volumes, initialiser la restauration, puis surveiller le processus. Suite à la restauration sans système d'exploitation, vous pouvez poursuivre la tâche de chargement du système d'exploitation et des applications logicielles sur le serveur restauré, ainsi que vos paramètres et 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 vos ordinateurs Linux protégés à l'aide de l'utilitaire `aamount`. Pour en savoir plus, voir Exécution d'une restauration sans système d'exploitation pour une machine Linux.

Prérequis d'exécution d'une restauration sans système d'exploitation 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 :

- Les sauvegardes du serveur et AppAssure 5 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 sans système d'exploitation (BMR) d'un ordinateur Windows

Pour effectuer une BMR d'un ordinateur Windows :

1. Créez un CD d'amorçage. Voir 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 5 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 sans système d'exploitation (BMR) d'une machine Windows, vous devez créer un CD amorçable/une image ISO dans la console AppAssure 5, et y stocker l'interface de console AppAssure Universal Recovery. La console AppAssure 5 Universal Recovery est un environnement qui permet de restaurer le lecteur système ou l'ensemble du serveur, directement depuis AppAssure 5 Core.

L'image ISO que vous créez est conçue sur mesure pour 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 autres pilotes sur le CD d'amorçage. Pour plus d'informations sur l'injection de ces pilotes dans le CD d'amorçage, voir Insertion de pilotes dans 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 la console AppAssure 5 Core 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 d'agent AppAssure 5

   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 de l'AppAssure 5 Core

Pour lancer une restauration à partir de l'AppAssure 5 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. Naviguez jusqu'au serveur du core, puis ouvrez l'AppAssure 5 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 Chargement d'un CD d'amorçage.
8. Cliquez sur **Charger les volumes** pour charger les volumes cibles sur le nouvel ordinateur.

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, voir Lancement d'une restauration à partir de l'AppAssure 5 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

N'oubliez pas : si vous avez restauré 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. Pour plus d'informations, voir Injection de pilotes sur votre 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 sans système d'exploitation pour une machine Linux

Dans AppAssure 5, vous pouvez effectuer la restauration sans système d'exploitation (BMR) d'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 opération de 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. Utilisez le numéro de ligne de l'agent/machine (de la sortie lm), suivi du numéro de ligne du point de restauration et de la lettre du volume, suivis 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 l'AppAssure 5 Core Console, cliquez sur le lien hypertexte de l'ordinateur dont vous souhaitez afficher les événements.
   - Dans la zone **Navigation** gauche de l'AppAssure 5 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.

6

Protection des clusters de serveurs

À propos de la protection des clusters de serveurs dans AppAssure 5

Dans AppAssure 5, la protection de clusters de serveurs est associée aux agents AppAssure installés sur des nœuds de clusters individuels (c'est-à-dire des machines individuelles dans le cluster) et AppAssure 5 Core (qui protège ces agents), tout comme s'il s'agissait d'une seule machine composite.

Vous pouvez facilement configurer un core AppAssure 5 afin de protéger et de gérer un cluster. Dans la console Core, 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, AppAssure 5 doit être installé sur l'agent AppAssure 5 sur chaque machine ou nœud dans le cluster. AppAssure 5 prend en charge les versions d'applications et configurations de cluster énumérées dans le tableau suivant.

Application	Version d'application et configuration de cluster associé	Cluster de basculement Windows
Microsoft Exchange	2007 Single Copy Cluster (SCC) 2007 Cluster Continuous Replication (CCR)	2003, 2008, 2008 R2
	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 le protéger dans AppAssure 5. Lorsque vous ajoutez un cluster à protéger, vous devez spécifier le nom d'hôte ou l'adresse IP du cluster, l'application du cluster ou un des nœuds de cluster ou de machine qui contient l'AppAssure 5 Agent.

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 Á 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 lequel l'AppAssure 5 Core communiquera avec l'agent sur la machine.
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, voir 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	Le numéro du port sur lequel l'AppAssure 5 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**.

Zone de texte	Description
Mot de passe	Le mot de passe utilisé pour vous connecter à cette machine

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 l'AppAssure 5 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 chiffrement d'un référentiel se définissent dans l'onglet **Configuration** de l'AppAssure 5 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, voir Affichage et modification des paramètres de configuration
3. Pour configurer des groupes de notification pour les événements système, voir Configuration de groupes de notification pour les événements système
4. Pour personnaliser les paramètres de stratégie de rétention, voir Personnalisation des paramètres de stratégie de rétention
5. Pour modifier l'horaire de protection, voir Modification des horaires de protection.

6. Pour modifier les paramètres de transfert, voir 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 du 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 l'AppAssure 5 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.
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** – **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 de stratégie de rétention, en commençant par l'étape 4.

Modification des horaires de protection du cluster

Dans AppAssure 5, 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 tel que décrit dans Modification des horaires de protection, en commençant par l'étape 2.

Modification des paramètres de transfert de cluster

Dans AppAssure 5, 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 transfert dans AppAssure 5 :

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 alertes d'un ordinateur ou un core 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 des informations de résumé

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 le récapitulatif et l'état des informations d'un ordinateur ou d'un nœud particulier dans le cluster, voir 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 ponctuelle des dossiers et fichiers des volumes partagés d'un cluster, stockés dans le référentiel. Les points de restauration servent à restaurer des machines protégées ou à monter un système de fichiers local. Dans AppAssure 5, vous pouvez afficher les listes de points de restauration du référentiel. Effectuez les étapes de la procédure suivante pour afficher 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 de machines individuels dans un cluster, voir Affichage de 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 en savoir plus sur les opérations que vous pouvez effectuer sur les points de restauration, voir Affichage d'un point de restauration particulier
4. Sélectionnez un point de restauration à monter.

   Pour savoir comment monter un point de restauration, voir Montage d'un point de restauration pour une machine Windows, en commençant par l'étape 2.
5. Sélectionnez un point de restauration à monter.

   Pour savoir comment monter un point de restauration, voir Montage d'un point de restauration pour une machine Windows.
6. Pour supprimer des points de restauration, voir Suppression de points de restauration.

Gestion des instantanés d'un cluster

Vous pouvez gérer des instantanés dans AppAssure 5 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, voir Forcer un instantané. Pour savoir comment suspendre et reprendre des instantanés des instantanés d'ordinateurs individuels d'un cluster, voir Suspension et reprise d'instantanés.

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 (rollback) à l'aide de la procédure AppAssure standard de la machine, comme l'indiquent les sections Exécution d'une restauration (rollback) et Exécution d'une restauration (rollback) pour une machine Linux avec 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 (rollback) à l'aide de la procédure AppAssure standard de la machine, comme l'indiquent les sections Exécution d'une restauration (rollback) et Exécution d'une restauration (rollback) pour une machine Linux avec 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 obtenir plus d'informations et des instructions de réplication de données, voir 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 de la protection des nœuds de cluster

Effectuez les étapes des procédures suivantes pour retirer les nœuds de cluster de la protection. Si vous souhaitez uniquement supprimer un nœud du cluster, voir Conversion d'un nœud de cluster protégé en agent. Pour supprimer un nœud de cluster de la protection.

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 5 de votre cluster et vos nœuds individuels. Les rapports comprennent des informations d'activité AppAssure 5 sur le cluster, le nœud et les volumes partagés. Pour en savoir plus sur les rapports AppAssure 5, 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 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 avant le déploiement de l'AppAssure 5 Core ou de l'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.

7

Rapports

À propos des rapports

AppAssure 5 vous permet de générer et d'afficher les informations de conformité, d'erreurs et de résumé de plusieurs ordinateurs de core et d'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.

Icône	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.

Pour en savoir plus sur la génération d'un rapport, voir Génération d'un rapport pour un core ou un agent. Pour en savoir plus sur la génération d'un rapport de plusieurs cores dans la Central Management Console, voir Génération d'un rapport depuis la Central Management Console Pour en savoir plus sur la génération de rapports de clusters, voir Affichage d'un cluster ou d'un rapport de nœud.

À propos des rapports de conformité

Les rapports de conformité sont disponibles pour l'AppAssure 5 Core et l'AppAssure 5 Agent. Ils vous permettent de visualiser l'état des tâches effectuées par un core ou un agent sélectionné. Les tâches en échec 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

Pour en savoir plus sur la génération d'un rapport, voir Génération d'un rapport pour un core ou un agent.

À propos des rapports d'erreurs

Les rapports d'erreur sont des sous-ensembles des Rapports de conformité et sont disponibles aux AppAssure 5 Cores et aux AppAssure 5 Agents. Les Rapports d'erreur incluent uniquement les tâches en échec répertoriées 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
- Total

Pour en savoir plus sur la génération d'un rapport, voir Génération d'un rapport pour un core ou un agent.

À propos du rapport de résumé de core

Le **Rapport de résumé de core** inclut des informations sur les référentiels de l'AppAssure 5 Core sélectionné et sur les agents protégés par ce core. Les informations s'affichent sous forme de deux résumés dans un rapport.

Pour savoir comment générer un rapport de résumé de core, voir Génération d'un rapport pour un core ou un agent.

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. Naviguez jusqu'à l'AppAssure 5 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 d'exportation.
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. Pour en savoir plus sur la barre d'outils, voir À propos de la barre d'outils Rapports.

À propos des rapports de core de la Central Management Console

AppAssure 5 vous permet de générer et d'afficher les informations de conformité, d'erreur et de résumé de plusieurs AppAssure 5 Cores. Des informations détaillées sur les cores s'affichent en colonnes comprenant les catégories décrites dans les sections À propos des rapports de conformité, À propos des rapports d'erreurs et À propos du rapport de résumé de core.

Pour savoir comment générer un rapport concernant plusieurs cores, voir Génération d'un rapport depuis la Central Management Console.

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 d'erreurs**
3. Dans la zone de navigation de gauche, sélectionnez le ou les AppAssure 5 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. Pour en savoir plus sur la barre d'outils, voir À propos de la barre d'outils Rapports.

8

Exécution d'une restauration totale de la DL4000 Backup To Disk Appliance

Les lecteurs de données de l'appliance DL4000 Backup To Disk Appliance se trouvent dans les logements 2 à 9. Ils sont au format RAID 6, ce qui signifie qu'ils peuvent subir un maximum de deux échecs de lecteur sans perte de données. Le système d'exploitation réside sur les lecteurs 0 et 1, 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 0 et 1 sont des disques connus en bon état de fonctionnement.
2. Amorcez l'appliance DL4000 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**.
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) du système DL4000 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 Recovery and Update Utility

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 DL4000 Backup to Disk Appliance et extrayez les fichiers.
3. Double-cliquez sur **Lancer-RUU**.
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.

9

Modification manuelle du nom d'hôte

Il vous est recommandé de sélectionner un nom d'hôte au cours de la configuration initiale de DL4000 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 AppAssure 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 de certificats de serveur AppAssure

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 d'AppAssure Core avec le nouveau nom d'hôte

Pour lancer l'AppAssure 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 5 Core à l'aide de l'icône **AppAssure 5 Core**.

Modification du nom d'affichage dans AppAssure

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**.

10

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 5 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 5 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 et paramètres\Tous les utilisateurs \Données d'application**.

REMARQUE : Vous devez utiliser Windows PowerShell. Il doit être installé puis configuré avant l'utilisation et l'exécution de scripts AppAssure 5.

Conditions requises pour la création de scripts Powershell

Avant l'utilisation et l'exécution de PowerShell scripts for AppAssure 5, 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.

AgentProtectionStorageConfiguration (namespace Replay.Common.Contracts.Agents)

Méthode	Description
`public Guid RepositoryId { get; set; }`	Obtient ou définit l'ID du référentiel dans lequel seront stockés les points de restauration de cet agent.
`public string EncryptionKeyId { get; set; }`	Obtient ou définit l'ID de la clé de chiffrement pour les points de restauration de cet agent. Une chaîne vide signifie l'absence de chiffrement.

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 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 le `BlockHashesUri` et les propriétés `BlockDataUri` de l'objet `VolumeSnapshotInfo` pour chaque volume aligné.
`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.

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)

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 l'ordinateur 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.Sql)

Hérite ses valeurs du paramètre, `BackgroundJobRequest`.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Hérite ses valeurs du paramètre, `BackgroundJobRequest`.

TakeSnapshotResponse (namespace Replay.Agent.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.Core.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`, `Copy`, et `Full`.

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.

TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

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`, `Copy`, et `Full`.
`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
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtient ou définit la collection des informations sur l'instantané pour chaque volume inclus dans l'instantané

TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

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`, `Copy`, et `Full`.
`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.

VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

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.RecoveryPoints)

Hérite ses valeurs du paramètre, `System.Collections.ObjectModel.Collection<string>`.

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.
`public string UrlEncode()`	Obtient une version encodée par URL du nom pouvant passer facilement dans une URL.

Méthode	Description
	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 ses valeurs du paramètre, `System.Collections.ObjectModel.Collection<VolumeName>`.

Méthode	Description
`public override bool Equals(object obj)`	Détermine si cette instance et un objet spécifié, qui doit également être un objet `VolumeNameCollection` ont la même valeur. (Écrase `Object.Equals(Object)`.)
`public override int GetHashCode()`	Retourne le code hash de ce(tte) `VolumeNameCollection`. (Écrase `Object.GetHashCode()`.)

VolumeSnapshotInfo (namesapce 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 script

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

11

Obtenir de l'aide

Recherche de documentation

Il existe des liens directs vers la documentation d'AppAssure et de l'appliance DL4000 dans la console AppAssure 5 Core. Pour accéder aux liens vers la documentation, sélectionnez l'onglet **Appliance**, puis cliquez sur **État global**. Les liens vers la documentation se trouvent dans la section **Documentation**.

Recherche de mises à jour du logiciel

Il existe des liens directs vers les mises à jour du logiciel d'AppAssure et de l'appliance DL4000 dans la console AppAssure 5 Core. Pour accéder aux liens vers les mises à jour du logiciel, sélectionnez l'onglet **Appliance**, puis cliquez sur **État global**. Les liens vers les mises à jour se trouvent dans la section **Documentation**.

Contacter Dell

REMARQUE : Dell fournit plusieurs options de service et de support en ligne et par téléphone. Si vous ne possédez pas une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, acte de vente 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.

Pour prendre contact avec Dell pour des questions commerciales, de support technique ou de service clientèle :

1. Rendez-vous sur dell.com/contactdell.
2. Sélectionnez votre pays ou région depuis la carte du monde interactive.
   Les pays correspondant à la région sélectionnée s'affichent lorsque vous sélectionnez une région.
3. Sélectionnez la langue appropriée sous le pays de votre choix.
4. Sélectionnez votre secteur d'activités.
   La page de support principale pour le secteur d'activités sélectionné s'affichera.
5. Sélectionnez l'option appropriée en fonction de vos besoins.

Commentaires sur la documentation

Si vous avez des commentaires à faire sur ce document, écrivez à l'adresse documentation_feedback@dell.com. Sinon, cliquez sur le lien **Commentaires** sur n'importe laquelle des pages de documentation Dell, remplissez le formulaire et cliquez sur **Soumettre** pour envoyer vos commentaires.