Appliance Dell DL1000
Guide d'utilisation

Remarques, précautions et avertissements

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

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

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

2015 - 12

Rév. A01

Table des matières

1

Présentation du système Dell DL1000

Le système Dell DL1000 combine la sauvegarde et la réplication dans un produit de protection des données unifiées. Il assure la fiabilité des restaurations des données des applications à partir de vos sauvegardes pour protéger les machines virtuelles et physiques. Votre appliance est capable de gérer jusqu'à des téraoctets de données grâce à la déduplication globale, la compression, le cryptage et la réplication intégrés à une infrastructure privée ou publique du cloud. Les applications et données de serveur peuvent être restaurées en quelques minutes pour des raisons de conservation des données (DR) et de conformité.

Le système DL1000 prend en charge les environnements à plusieurs hyperviseurs sur les clouds privés et publics VMware vSphere et Microsoft Hyper-V.

Technologies principales du système Dell DL1000

Votre appliance combine les technologies suivantes :

- Live Recovery
- Universal Recovery
- Déduplication globale réelle
- Cryptage

Live Recovery

Live Recovery est une technologie de restauration instantanée pour les VM ou les serveurs. Elle donne un accès quasiment continu aux volumes de données sur les serveurs virtuels ou physiques.

La technologie de réplication et de sauvegarde du système DL1000 enregistre des instantanés simultanés de plusieurs VM ou serveurs protégeant quasiment instantanément les données et les systèmes. Vous pouvez recommencer à utiliser le serveur en montant le point de restauration sans avoir à attendre une restauration complète dans le stockage de production.

Universal Recovery

La fonction Universal Recovery offre une souplesse illimitée de restauration des ordinateurs. Vous pouvez restaurer vos sauvegardes depuis des systèmes physiques vers des machines virtuelles, depuis des machine virtuelles vers d'autres machines virtuelles, depuis des machines virtuelles vers des systèmes physiques ou depuis des systèmes physiques vers des systèmes physiques, puis effectuer des restaurations sans système d'exploitation (BMR) sur du matériel différent.

La technologie Universal Recovery accélère aussi les transferts multiplateformes entre les machines virtuelles ; par exemple, transfert de VMware vers Hyper-V ou d'Hyper-V vers VMware. Universal Recovery effectue des constructions dans la récupération au niveau des applications, des éléments et des objets

(fichiers individuels, dossiers, éléments, e-mails, éléments de calendrier, bases de données et applications).

Déduplication globale réelle

La déduplication globale élimine les données redondantes ou dupliquées en effectuant des sauvegardes incrémentielles au niveau bloc des machines.

La structure de disque standard 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 de serveur et de 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, 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 de l'ensemble de l'environnement.

Figure 1. Diagramme de la déduplication globale réelle

Cryptage

Le système DL1000 fournit une fonction de cryptage pour protéger les sauvegardes et les données au repos contre toute utilisation et tout accès non autorisés afin de garantir la confidentialité des données. Les données sont accessibles et peuvent être décryptées à l'aide de la clé de cryptage. Le cryptage est effectué en ligne sur les données d'instantané, à la vitesse de transmission de ligne sans affecter les performances.

Fonctions de protection des données du Dell DL1000

Core Dell DL1000

Le Core est le composant central de l'architecture de déploiement DL1000. Il stocke et gère les sauvegardes de machine et fournit des services pour la sauvegarde, la récupération, la conservation, la réplication, l'archivage et la gestion. Le Core est un ordinateur adressable sur le réseau exécutant une variante 64 bits des systèmes d'exploitation Microsoft Windows Server 2012 R2 Foundation et Standard. L'appliance exécute la compression, le cryptage et la déduplication intégrés basés sur la cible des

données reçues de l'agent. Le Core stocke alors les sauvegardes des instantanés dans le référentiel qui réside sur l'appliance. Les Cores sont appariés pour la réplication.

Le référentiel réside dans le stockage interne dans le core. Ce dernier est géré en accédant à l'URL **https://CORENAME:8006/apprecovery/admin** depuis un navigateur Web compatible Javascript.

Agent intelligent Dell DL1000

Le Smart Agent est installé sur la machine à Core protégé. Le Smart Agent fait le suivi des modifications apportées aux blocs du volume de disques, puis crée un instantané des blocs modifiés selon une fréquence de protection définie. L'approche permanente des instantanés incrémentiels au niveau du bloc évite d'avoir à copier de manière répétée les mêmes données de la machine protégée vers le Core.

Une fois configuré, l'agent utilise une technologie intelligente pour faire le suivi des blocs modifiés sur les volumes de disques protégés. Lorsque l'instantané est prêt, il est rapidement transféré vers le Core à l'aide de connexions à base de sockets, multithreads intelligentes.

Processus d'instantané

Le processus de protection de votre DL1000 démarre lorsqu'une image de base est transférée d'une machine protégée au Core ; c'est le seul moment où une copie complète de la machine doit être transportée sur le réseau lors d'une opération normale, suivie d'instantanés incrémentiels définitifs. Le DL1000 Agent pour Windows utilise le service de copie Microsoft Volume Shadow copy Service (VSS) pour geler ou suspendre les données d'application sur un disque pour capturer une sauvegarde compatible avec le système de fichiers et l'application. Lors de la création d'un instantané, l'enregistreur VSS situé sur le serveur cible empêche l'écriture du contenu sur le disque. Au cours du processus d'arrêt de l'écriture du contenu sur le disque, toutes les opérations d'E/S du disque sont mises en file d'attente et reprennent uniquement une fois l'instantané terminé, tandis que les opérations en cours se terminent et que tous les fichiers ouverts se ferment. Le processus de création d'une copie miroir n'affecte pas de manière significative les performances du système de production.

Le système DL1000 utilise Microsoft VSS, car il dispose du support intégré pour toutes les technologies internes Windows, notamment NTFS, Registre, Active Directory, 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 les plug-ins Enregistreur VSS pour recevoir une notification lorsqu'un instantané est préparé et lorsqu'elles doivent vider sur disque leurs pages de base de données utilisées pour placer la base de données dans un état de transaction cohérent. Les données capturées sont rapidement transférées et stockées sur le core.

Réplication : site de reprise après sinistre ou fournisseur de services

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

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

intégrés, qui vous permettent de demander des connexions et de recevoir des notifications automatiques de rétroinformation.

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

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

La réplication commence par l'amorçage : le transfert initial d'images de base dédupliquées et d'instantanés incrémentiels de machines protégées, ce qui peut ajouter jusqu'à des centaines ou des milliers de gigaoctets de données. La réplication initiale peut être amorcée vers le noyau cible à l'aide de supports externes. D'habitude, ceci est utile pour de gros ensembles de données ou des sites dont les liens sont lents. Les données d'une archive d'amorçage sont compressées, chiffrées et dédupliquées. Si la taille totale de l'archive est supérieure à l'espace disponible sur un support amovible, l'archive peut être fractionnée sur plusieurs périphériques selon l'espace disponible sur le support. Pendant le processus d'amorçage, les points de restauration incrémentiels se répliquent sur le site cible. Une fois que le core cible a fini de consommer l'archive d'amorçage, les points de restauration incrémentiels répliqués se synchronisent automatiquement.

Restauration

La restauration peut être réalisée sur le site local ou sur le site à distance répliqué. Une fois que le déploiement est stable avec une protection locale et une réplication optionnelles, le système DL1000 Core permet de réaliser une restauration à l'aide de Verified Recovery, Universal Recovery ou Live Recovery.

Restauration en tant que service (RaaS, Recovery-as-a-Service)

Les fournisseurs de services gérés (MSP, Managed Service Providers) peuvent tirer pleinement parti du système DL1000 en tant que plateforme pour fournir des services RaaS. RaaS facilite la restauration complète dans le cloud en répliquant les serveurs physiques et virtuels des clients. Les clouds des fournisseurs de service sont utiles en tant que machines virtuelles pour prendre en charge les tests de restauration ou les opérations de restauration. Les clients qui souhaitent effectuer une restauration dans le cloud peuvent configurer la réplication sur leurs machines protégées sur les cores locaux vers un fournisseur de services AppAssure. En cas de sinistre, les fournisseurs MSP peuvent immédiatement activer les machines virtuelles du client.

Le système DL1000 n’est pas mutualisé. Les fournisseurs MSP peuvent utiliser le système DL1000 sur plusieurs sites et créer un environnement mutualisé.

Virtualisation et cloud

DL1000 Core est prêt pour le cloud, ce qui permet de tirer parti de la capacité de traitement du cloud pour la restauration et l'archivage.

Le système DL1000 peut exporter n'importe quelle machine protégée ou répliquée vers des versions sous licence de VMware ou Hyper-V. Dans le cas d’exportations continues, la machine virtuelle est mise à jour de façon incrémentielle après chaque instantané. Les mises à jour incrémentielles sont rapides et

fournissent des clones de secours prêts à être mis sous tension en un seul clic. Les exportations de machine virtuelle prises en charge sont les suivantes :

- VMware Workstation ou Server dans un dossier
- Exportation directe vers un hôte Vsphere ou ESXi VMware
- Exportation vers Oracle VirtualBox
- Microsoft Hyper-V Server sur Windows Server 2008 (x64)
- Microsoft Hyper-V Server sur Windows Server 2008 R2
- Microsoft Hyper-V Server sous Windows Server 2012 R2

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

Architecture de déploiement du Dell DL1000

L'architecture de déploiement DL1000 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 (MSP) pour effectuer la restauration hors site. Un déploiement local de base comprend un serveur de sauvegarde appelé 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 de reprise après sinistre. DL1000 core utilise des images de base et des instantanés incrémentiels pour compiler les points de restauration des agents protégés.

En outre, le système DL1000 reconnaît les applications car il peut détecter la présence de Microsoft Exchange et SQL et de leurs bases de données et fichiers journaux respectifs. Les sauvegardes sont effectuées à l'aide d'instantanés de niveau bloc avec reconnaissance d'application. Le système DL1000 effectue une troncature des journaux du serveur Microsoft Exchange protégé.

Le diagramme suivant montre un déploiement DL1000 simple. Les agents DL1000 sont installés sur des machines, telles qu'un serveur de fichiers, un serveur de messagerie, serveur de base de données, ou des machines virtuelles sont connectées à un seul DL1000 Core et protégées par ce dernier qui comprend le référentiel de stockage central. Le portail de licences logicielles Dell gère les abonnements aux licences, les groupes et les utilisateurs pour les agents et les cores dans l'environnement. Le port permet aux utilisateurs de se connecter, d'activer des comptes, de télécharger du logiciel et de déployer des agents et des cores en fonction de votre licence pour l'environnement.

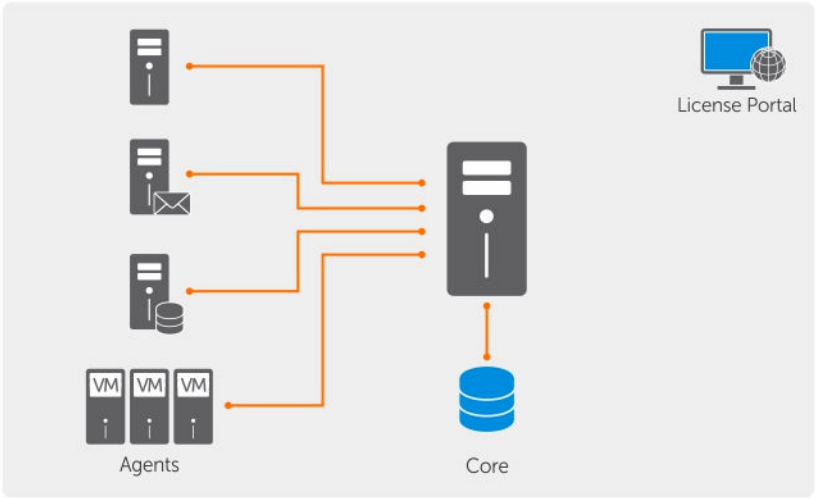

Figure 2. Architecture de déploiement Dell DL1000

Vous pouvez également déployer plusieurs DL1000 Cores, comme le montre le diagramme suivant. Une console centrale gère plusieurs cores.

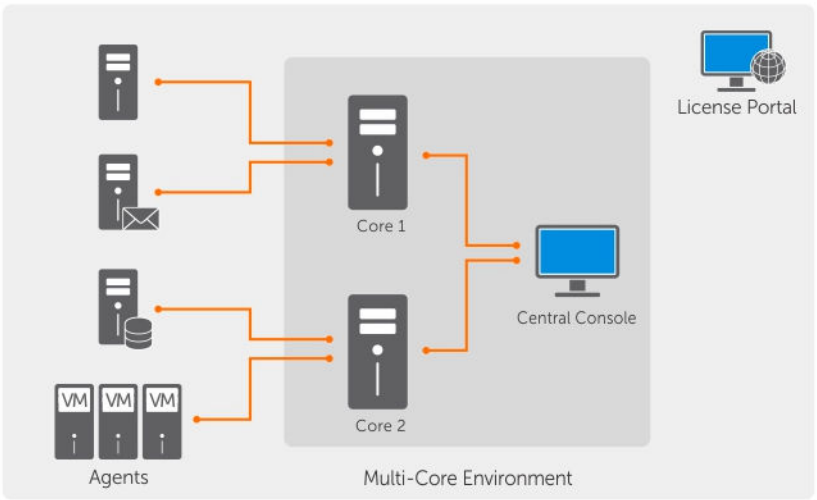

Figure 3. Architecture de déploiement de plusieurs DL1000 Cores

Autres informations utiles

REMARQUE : Pour tous les documents Dell OpenManage, rendez-vous sur **dell.com/openmanagemanuals**.

REMARQUE : Vérifiez toujours si des mises à jour sont disponibles sur le site **dell.com/support/home** et lisez-les en premier, car elles remplacent souvent les informations contenues dans les autres documents.

REMARQUE : Pour toute documentation concernant Dell OpenManage Server Administrator, voir **dell.com/openmanage/manuals**.

Votre documentation de produit inclut :

Guide de mise en route	Présente les fonctions du système, la définition du système et les caractéristiques techniques. Ce document est aussi livré avec votre système.
Présentation des informations système	La Présentation des informations système fournit des informations sur la configuration du matériel et l'installation du logiciel sur votre solution AppAssure.
Manuel du propriétaire	Fournit des informations sur les caractéristiques du système, ainsi que des instructions relatives au dépannage et à l'installation ou au remplacement de composants du système.
Guide de déploiement	Fournit des informations sur le déploiement du matériel et le déploiement initial de l'appliance.
Guide d'utilisation	Fournit des informations sur la configuration et la gestion du système.
Notes de mise à jour	Fournit les informations produit et des informations supplémentaires sur l'appliance Dell DL1000.
Guide d'interopérabilité	Fournit des informations sur les logiciels et matériels pris en charge pour l'appliance DL4000, ainsi que les considérations, recommandations et règles d'utilisation.
Guide d'utilisation d'OpenManage Server Administrator	Fournit des informations sur l'utilisation de Dell OpenManage Server Administrator pour gérer votre système.
Support de ressources	Tous les supports fournis avec le système contiennent de la documentation et des outils permettant de configurer et de gérer le système, notamment ceux qui concernent le système d'exploitation, le logiciel de gestion du système, les mises à jour du système et les composants système achetés avec le système.

2

Utilisation du système DL1000

Accès à la console Core DL1000

Pour accéder à DL1000 Core Console :

1. mettez à jour les sites de confiance dans le navigateur.
2. Configurez le navigateur pour accéder à distance à DL1000 Core Console. Voir Configuration des navigateurs pour accéder à distance Core Console.
3. Effectuez l'une des tâches suivantes pour accéder à DL1000 Core Console :
   - connectez-vous localement au serveur DL1000 Core, puis double-cliquez sur 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 des navigateurs pour accéder à distance à Core Console

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

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

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

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

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

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

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

Pour modifier les paramètres du navigateur Mozilla Firefox :

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

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

Gestion des licences

Vous pouvez gérer les licences DL1000 directement dans Core Console. Depuis la console, vous pouvez modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au portail des licences Dell AppAssure depuis la page **Licences** dans Core Console.

La page **Licences** contient 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
- Contraintes de licence

Modifier une clé de licence

Pour modifier une clé de licence :

1. Accédez à Core Console, puis sélectionnez **Configuration → Licences**.
   La page **Licences** s'affiche.
2. Dans la page **Détails de la licence**, cliquez sur **Modifier**.
   La boîte de dialogue **Modifier la clé de licence** s'affiche.
3. 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

Core Console contacte le serveur de portail pour mettre à jour les modifications apportées au portail de licences. La communication avec le serveur de portail intervient à des intervalles définis, mais vous pouvez établir la communication à la demande.

Pour contacter le serveur de portail :

1. Accédez à la Core Console, puis cliquez sur **Configuration → Licences**.
   La page **Licences** s'affiche.
2. À partir de l'option **Licence Server**, cliquez sur **Contacter maintenant**.

Modification manuelle de la langue d'AppAssure

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

1. Lancez l'Éditeur de registre à l'aide de la commande `regdit`.
2. Rendez-vous sur **HKEY_LOCAL_MACHINE → SOFTWARE → AppRecovery → Core → Localization**.
3. Ouvrez **Lcid**.
4. Sélectionnez **Valeur décimale**.
5. Entrez la valeur correspondant à la langue requise dans la case `Données de la valeur`. Les valeurs correspondant aux langues prises en charge sont les suivantes :

   a. Anglais : 1033
   b. Portugais brésilien : 1046
   c. Espagnol : 1034
   d. Français : 1036
   e. Allemand : 1031
   f. Chinois simplifié : 2052
   g. Japonais : 1041

h. Coréen : 1042

6. Cliquez avec le bouton droit de la souris et redémarrez les services dans l'ordre indiqué :
   a. WMI (infrastructure de gestion Windows)
   b. Service Internet SRM
   c. AppAssure Core
7. Effacez le cache du navigateur.
8. Fermez le navigateur et redémarrez la Core Console depuis l'icône sur le bureau.

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

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

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

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

1. Sur la page **Démarrer**, entrez `Langue`, et assurez-vous que le domaine de recherche est défini sur Paramètres.
2. Dans le volet **Résultats**, sélectionnez **Langue**.
3. Dans le volet **Modifier vos préférences linguistiques** , sélectionnez **Ajouter une langue**.
4. Parcourir ou rechercher la langue que vous souhaitez installer.
   Par exemple, sélectionnez Catalan, puis sélectionnez Ajouter. Le catalan a été ajouté comme l'une des langues.
5. Dans le volet Modifier vos préférences de langue, sélectionnez **Options** en regard de la langue ajoutée.
6. Si un pack de langue est disponible pour votre langue, sélectionnez `Télécharger et installer le pack de langue`.
7. Lorsque le pack de langue est installé, la langue est affichée comme étant disponible en tant que langue d'affichage de Windows.
8. Pour faire de cette langue votre langue d'affichage, déplacez-la en haut de votre liste de langues.
9. Pour que le changement prenne effet, déconnectez-vous de Windows puis reconnectez-vous.

Gestion des paramètres Core

Les paramètres Core permettent de définir divers paramètres de configuration et de performance. La plupart des paramètres sont configurés pour un usage optimal, mais vous pouvez modifier les paramètres suivants :

- Généralités
- Tâches nocturnes
- File d'attente de transfert
- Paramètres d'expiration du délai d'attente client
- Configuration du cache de déduplication
- Paramètres de connexion de base de données

Modification du nom d'affichage du Core

REMARQUE : Il est recommandé de sélectionner un nom d'affichage permanent au cours de la configuration initiale de l'appliance. Si vous le modifiez ensuite, vous devez effectuer plusieurs étapes manuellement pour vous assurer que le nouveau nom d'hôte soit appliqué et que l'appliance fonctionne correctement.

Pour modifier le nom d'affichage du core :

1. Accédez à Core Console, puis cliquez sur **Configuration** → **Paramètres**.
2. Dans la section **Général**, cliquez sur **Modifier**.
   La boîte de dialogue **Nom d'affichage** s'affiche.
3. Dans la zone de texte **Nom d'affichage** entrez le nouveau nom d'affichage du core.
4. Cliquez sur **OK**.

Changement de l'heure des tâches nocturnes

L'option Travail nocturne planifie les tâches telles que le cumul, la capacité d'attachement et la troncature pour les agents protégés par le core.

Pour régler l'heure de tâche nocturne :

1. Accédez à Core Console, puis sélectionnez **Configuration** → **Paramètres**.
2. Dans la section **Tâches nocturnes**, cliquez sur **Modifier**.
   La boîte de dialogue **Tâches nocturnes** s'affiche.
3. Dans la zone de texte **Heure des tâches nocturnes**, 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. Accédez à Core Console, puis cliquez sur **Configuration** → **Paramètres**.
2. Dans la section **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

Paramètres de délai d'attente du client spécifie le nombre de secondes ou minutes pendant lequel le serveur attend avant expiration du délai lors de la connexion à un client.

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

1. Accédez à Core Console, puis cliquez**Configuration** → **Paramètres**.
2. Dans la section **Définition des paramètres de délai d'attente du 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

La déduplication globale réduit la quantité d'espace de stockage disque requis pour les données sauvegardées. Le gestionnaire DVM (Gestionnaire de volumes de déduplication) combine un ensemble d'emplacements de stockage dans un même référentiel. Le cache de déduplication contient les références à des blocs uniques. Par défaut, le cache de déduplication est de 1,5 Go. Si les informations redondantes finissent par saturer le cache, le référentiel ne peut plus tirer pleinement parti de la déduplication dans le référentiel pour les nouvelles données ajoutées. Dans ce cas, vous pouvez augmenter la taille du cache de déduplication en modifiant sa configuration dans Console Core.

Pour configurer les paramètres de cache de déduplication :

1. Accédez à Core Console, puis cliquez sur **Configuration** → **Paramètres**.
2. Dans la section **Configuration du cache de déduplication**, cliquez sur **Modifier**.
   La boîte de dialogue **Configuration du cache de déduplication** s'affiche.
3. Dans la zone de texte **Emplacement du cache principal**, entrez l'emplacement du cache principal mis à jour.
4. Dans la zone de texte **Emplacement du cache secondaire**, entrez l'emplacement du cache secondaire mis à jour.
5. Dans la zone de texte **Emplacement du cache des métadonnées**, entrez l'emplacement du cache des métadonnées mis à jour.
6. Cliquez sur **OK**.

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

Modification des paramètres du moteur

Pour modifier les paramètres du moteur :

1. Accédez à Core Console, puis cliquez sur **Configuration** → **Paramètres**.
2. Dans la section **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 IP spécifique**.
4. Entrez les informations concernant la configuration comme suit :

Zone de texte	Description
Port préférable	Entrez un numéro de port ou acceptez le paramètre par défaut (le port par défaut est 8007). Le port est utilisé pour spécifier le canal de communication du moteur.
Groupe Admin	Entrez le nouveau nom du groupe d'administration. Le nom par défaut est BUILTIN\Administrators.
Longueur d'E/S asynchrones minimale	Entrez la valeur ou choisissez le paramètre par défaut. Elle décrit la longueur entrée/sortie minimale. Le paramètre par défaut est 65536.
Taille du tampon de réception	Entrez une taille du tampon entrant ou acceptez le paramètre par défaut. Le paramètre par défaut est 8192.
Taille du tampon d'envoi	Entrez une taille de tampon d'envoi sortant ou acceptez le paramètre par défaut. Le paramètre par défaut est 8192.
Expiration du délai d'attente de lecture	Entrez la valeur d'expiration du délai d'attente de lecture ou choisissez le paramètre par défaut. Le paramètre par défaut est 00:00:30.
Expiration du délai d'attente d'écriture	Entrez la valeur d'expiration du délai d'attente d'écriture ou choisissez le paramètre par défaut. Le paramètre par défaut est 00:00:30.

5. Sélectionnez **Aucun délai**.
6. Cliquez sur **OK**.

Modification des paramètres de déploiement

Pour modifier les paramètres de déploiement :

1. Accédez à Core Console et cliquez sur l'onglet **Configuration**, puis sur **Paramètres**.
2. Dans le volet **Paramètres de déploiement**, cliquez sur **Modifier**.
   La boîte de dialogue **Paramètres de déploiement** s'ouvre.
3. Dans la zone de texte **Nom du programme d'installation de l'agent**, entrez le nom du fichier exécutable de l'agent. La valeur par défaut est Agentweb. exe.
4. Dans la zone de texte **Adresse de Core**, entrez l'adresse du Core.
5. Dans la zone de texte **Délai de réception ayant échoué**, indiquez le nombre de minutes qui doit s'écouler sans activité avant l'expiration du délai d'attente.
6. Dans le champ **Nombre maximum d'installations parallèles**, entrez le nombre maximal d'installations qui peuvent être réalisées en parallèle.
7. Sélectionnez l'un ou l'autre des paramètres facultatifs suivants ou les deux :
   - Redémarrage automatique après installation
   - Protection après le déploiement
8. Cliquez sur **OK**.

Modification des paramètres de connexion de base de données

Pour modifier les paramètres de connexion de base de données :

1. Accédez à Core Console, puis cliquez sur **Configuration** → **Paramètres**.
2. Dans la section **Paramètres de connexion de base de données**, effectuez l'une des tâches suivantes :
   - pour restaurer la configuration par défaut, cliquez sur **Restaurer la valeur par défaut**.
   - Pour modifier les paramètres de connexion de base de données, cliquez sur **Modifier**.

   Lorsque vous 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**.

Gestion des événements

Le core inclut des ensemble d'événements prédéfinis qui peuvent être utilisés pour signaler aux administrateurs les problèmes critiques sur le core ou les tâches de sauvegarde.

Dans l'onglet **Événements**, vous pouvez gérer les groupes de notification, les paramètres SMTP de messagerie, les paramètres serveur, activer les journaux de trace, configurer le cloud, réduire les répétitions et conserver les événements.

L'option Groupes de notification permet de gérer des groupes de notification 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. Dans Core Console, sélectionnez **Configuration → Événements**.
2. Cliquez sur **Ajouter un groupe**.

   La boîte de dialogue **Ajouter un groupe de notification** s'affiche et présente deux panneaux :
   - **Activer les alertes**
   - **Options de notification**

Activation des alertes

L'activation des alertes permet de définir l'ensemble des événements système à consigner, de créer des rapports et de définir des alertes.

REMARQUE : Pour créer des alertes pour tous les événements, sélectionnez **Toutes les alertes**.

- Pour créer des alertes spécifiques pour les erreurs, les avertissements et les messages d'information ou une combinaison, sélectionnez l'une des options suivantes :
  - icône de triangle rouge (erreur)
  - icône de triangle jaune (avertissement)
  - cercle bleu (information)
  - flèche courbée (restauration de la valeur par défaut)
- Pour créer des alertes pour des événements spécifiques, cliquez sur **>** en regard du groupe concerné et cochez la case pour activer l'alerte.

Configuration des options de notification

1. 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	Définissez les destinataires de la notification par e-mail. Vous pouvez saisir plusieurs adresses e-mail, ainsi que des adresses Cci et Cc, comme indiqué ci-dessous : • **À :** • **Cc** • **Cci :**
Notifier par journal d'événements Windows	Sélectionnez cette option pour que les alertes soient signalées via le journal des événements Windows.
Notifier par syslogd	Sélectionnez cette option pour que les alertes soient signalées via sys logd. Spécifiez les détails de sys logd dans les zones de texte suivantes : • **Nom d'hôte :** • **Port : 1**
Notifier par des alertes Toast	Sélectionnez cette option pour que l'alerte s'affiche sous la forme d'une fenêtre contextuelle dans l'angle inférieur droit de l'écran.

2. Cliquez sur **OK**.

   Le message suivant s'affiche : **Le nom du groupe ne peut pas être modifié après la création du groupe de notification. Voulez-vous vraiment utiliser ce nom ?**.

   - Pour enregistrer le nom du groupe, cliquez sur **Oui**.
   - Pour modifier le nom du groupe, cliquez sur **Non**. Revenez à la fenêtre **Options de notification**, mettez à jour le nom du groupe et les autres paramètres de groupe de notifications et sauvegardez votre travail.

Configuration d'un serveur de messagerie

REMARQUE : Vous devez définir les paramètres de groupe de notification, notamment activer l'option **Notifier par e-mail** pour pouvoir envoyer des messages d'alerte par e-mail.

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

1. Dans Core Console, cliquez sur **Configuration** → **Événements**.
2. Dans le volet **Paramètres Paramètres** de messagerie, cliquez **Serveur SMTP**.

   La boîte de dialogue **Paramètres du serveur SMTP** s'affiche.
3. Entrez les informations du serveur de messagerie comme suit :

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**.
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**.

Zone de texte	Description
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.
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).

4. Cliquez sur **Envoyer un e-mail de test**, puis effectuez les opérations suivantes :
   a. dans la boîte de dialogue Envoyer un e-mail de test, saisissez l'adresse e-mail de destination du message de test et cliquez sur **Envoyer**.
   b. Si le test échoue, quittez la boîte de dialogue d'erreur et la boîte de dialogue **Envoyer un e-mail de test** et changer les paramètres de configuration du serveur de messagerie. Répétez l'étape 4.
   c. Cliquez sur **OK** pour confirmer.
   d. Vérifiez que l'e-mail de test a été envoyé.
   e. Revenez dans la boîte de dialogue Paramètres du serveur SMTP, et cliquez sur **Enregistrer** pour fermer la boîte de dialogue et enregistrer les paramètres.

Configuration d'un modèle de notification par e-mail

Pour pouvoir recevoir des notifications sur les événements, vous devez configurer un serveur de messagerie et un modèle de notification par e-mail.

REMARQUE : Pour pouvoir recevoir des messages d'alerte par e-mail, définissez les paramètres de groupe de notification et activer l'option **Notifier par e-mail** .

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

1. Dans Core Console, cliquez sur **Configuration** → **Événements**.
2. Dans le volet **Paramètres de messagerie**, cliquez sur **Modifier**.
   La boîte de dialogue **Modifier la configuration des notifications par e-mail** apparaît.
3. Sélectionnez **Activer les notifications par e-mail**, puis entrez les informations du serveur de messagerie suivantes :

Zone de texte	Description
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.

4. Cliquez sur **Envoyer un e-mail de test**. Procédez comme suit :

a. dans la boîte de dialogue Envoyer un e-mail de test, saisissez l'adresse e-mail de destination du message de test et cliquez sur **Envoyer**.
b. Si le test échoue, quittez la boîte de dialogue d'erreur et la boîte de dialogue Envoyer un e-mail de test, cliquez sur **OK** pour enregistrer les paramètres du modèle d'e-mail en cours et modifiez les paramètres du serveur de messagerie. Reportez-vous à Configuration d'un serveur de messagerie et d'un modèle de notification par e-mail. Veillez à entrer de nouveau le mot de passe de ce compte de messagerie. Enregistrez les paramètres, puis revenez à l'étape 4.
c. Cliquez sur **OK** pour confirmer.
d. Vérifiez que l'e-mail de test a été envoyé.
e. Revenez dans la boîte de dialogue **Modifier la configuration des notifications par e-mail** et cliquez sur **OK** pour fermer la boîte de dialogue et enregistrer les paramètres.

Configuration de la réduction des répétitions

Pour configurer la réduction des répétitions :

1. Dans Core Console, cliquez sur **Configuration** → **Événements**.
2. Dans la section **Réduction des répétitions**, cliquez sur **Modifier**.
   La boîte de dialogue **Activer la réduction des répétitions** apparaît.
3. Sélectionnez **Activer la réduction des répétitions**.
4. Dans la zone de texte **Stocker les événements pendant** entrez le nombre de minutes de stockage des événements pour la réduction des répétitions.
5. Cliquez sur **OK**.

Configuration de la rétention des événements

Pour configurer la rétention des événements :

1. Dans Core Console, cliquez sur **Configuration** → **Paramètres**.
2. Sous **Paramètres de connexion de base de données**, cliquez sur **Modifier**.
   La boîte de dialogue **Paramètres de connexion de base de données** s'affiche.
3. 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).
4. Cliquez sur **Enregistrer**.

Gestion des référentiels

Un référentiel stocke les instantanés capturés depuis vos stations de travail et serveurs protégés. Le référentiel du modèle DL1000 est préconfiguré. Le référentiel réside sur le stockage interne du système.

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.

Affichage des détails du référentiel

Pour afficher les détails du référentiel :

1. Dans la Core Console, cliquez sur **Configuration** → **Référentiels**.
2. Cliquez sur **>** en regard de la colonne **État** du référentiel dont vous voulez afficher les détails.
3. Les détails du référentiel incluent les emplacements de stockage et les statistiques. Les détails des emplacements de stockage incluent le chemin des métadonnées et celui des données, ainsi que la taille. Les informations statistiques sont les suivantes :
   - **Déduplication** : indiqué sous la forme du nombre de réussites de déduplication de bloc, du nombre d'échecs de déduplication de bloc et du taux de compression de bloc.
   - **E/S d'enregistrement** : les valeurs affichées sont le débit (Mo/s), le débit de lecture (Mo/s) et le débit d'écriture (Mo/s).
   - **Moteur de stockage** : les valeurs affichées sont le débit (Mo/s), le débit de lecture (Mo/s) et le débit d'écriture (Mo/s).

Vérification d'un référentiel

Core Console permet d'effectuer une vérification de diagnostic sur un volume de référentiel lorsque des erreurs se produisent. Les erreurs Core peuvent résulter d'un arrêt incorrect ou d'une défaillance matérielle.

REMARQUE : Cette procédure doit être strictement réservée au diagnostic.

Pour vérifier un référentiel :

1. Cliquez sur **Configuration** → **Référentiels**.
2. Cliquez sur l'icône Paramètres en regard de la colonne Taux de compression sous le bouton **Actions** .
3. Cliquez sur **Vérifier**.
   La boîte de dialogue **Vérifier le référentiel** s'affiche.
4. Dans la boîte de dialogue **Vérifier le référentiel**, cliquez sur **Vérifier**.

   REMARQUE : Lorsque vous effectuez une vérification, toutes les tâches actives associées au référentiel sont annulées. Avant le début de la vérification, un message demandant de confirmer l'exécution de la vérification s'affiche. Il est recommandé de recréer le cache des points de restauration. Si la vérification échoue, vous devez restaurer le référentiel depuis une archive.

Gestion de la sécurité

Le système DL1000 fournit un cryptage renforcé qui rend inaccessibles les machines protégées. Seul l'utilisateur possédant la clé de cryptage peut accéder aux données et les décrypter. Le cryptage n'affecte pas les performances. Les concepts et considérations de sécurité des clés sont les suivants :

- 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 une clé de cryptage définie dans le Core.

Ajout d'une clé de chiffrement

Pour ajouter une clé de chiffrement :

1. Dans Core Console, cliquez sur **Configuration** → **Sécurité**.
2. Dans le menu déroulant **Actions** , cliquez sur **Ajouter une clé de cryptage**.

   La boîte de dialogue **Créer une clé de cryptage** apparaît.
3. Dans la boîte de dialogue **Créer une clé de cryptage**, entrez les détails de la clé comme indiqué ci-dessous.

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

4. Cliquez sur **OK**.

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

Modification d'une clé de chiffrement

Pour modifier une clé de chiffrement :

1. Dans Core Console, cliquez sur **Configuration** → **Sécurité**.

   L'écran **Clés de chiffrement** s'affiche.
2. 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.
3. Dans la boîte de dialogue **Modifier la clé de cryptage**, modifiez le nom ou la description de la clé.
4. 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 Core Console, cliquez sur **Configuration** → **Sécurité**.
2. 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.
3. 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.
4. Cliquez sur **OK**.

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

Importation d'une clé de cryptage

Pour importer une clé de cryptage :

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

Exportation d'une clé de chiffrement

Pour exporter une clé de chiffrement :

1. Dans Core Console, cliquez sur **Configuration** → **Sécurité**.
2. Dans le menu déroulant Configuration de la clé de cryptage à exporter, sélectionnez **Exporter**.
   La boîte de dialogue **Exporter la clé** apparaît.
3. Dans la boîte de dialogue **Exporter une clé**, cliquez sur **Enregistrer le fichier** pour enregistrer et stocker les clés de cryptage dans un emplacement protégé.
4. Cliquez sur **OK**.

Suppression d'une clé de chiffrement

Pour supprimer une clé de chiffrement

1. Dans Core Console, cliquez sur **Configuration** → **Sécurité**.
2. Dans le menu déroulant Configuration de la clé de cryptage à supprimer, sélectionnez **Supprimer**.
   La boîte de dialogue **Supprimer la clé** apparaît.
3. Dans la boîte de dialogue **Supprimer la clé**, cliquez sur **OK** pour supprimer la clé de chiffrement.

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

Gestion des comptes Cloud

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

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

Ajout d'un compte Cloud

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

Pour ajouter un compte Cloud :

1. Dans la Core Console, cliquez sur l'onglet **Outils**.
2. Dans le menu de gauche, cliquez sur **Clouds**.
3. Sur la page **Clouds**, cliquez sur **Ajouter un nouveau compte**.
   La boîte de dialogue **Ajouter un nouveau compte** s'ouvre.
4. Sélectionnez un fournisseur Cloud compatible dans la liste déroulante **Type de Cloud**.
5. Entrez les informations décrites dans le tableau suivant en fonction du type de Cloud sélectionné à l'étape 4.

Tableau 1. Ajout d'un compte Cloud

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

Type de Cloud	Zone de texte	Description
	Nom d'affichage	Créez le nom d'affichage du compte dans AppAssure ; par exemple, Rackspace 1.

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

Modification d'un compte Cloud

Procédez comme suit pour modifier un compte Cloud :

1. dans Core Console, cliquez sur l'onglet **Outils**.
2. Dans le menu de gauche, cliquez sur **Clouds**.
3. En regard du compte Cloud à modifier, cliquez sur le menu déroulant, puis sur **Modifier**.
   La fenêtre **Éditer un compte** s'ouvre.
4. Modifiez les informations de manière appropriée, puis cliquez sur **Enregistrer**.

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

Définition des paramètres d'un compte Cloud

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

1. Dans la console Core, cliquez sur l'onglet **Configuration**.
2. Dans le menu de gauche, cliquez sur **Paramètres**.
3. Dans la page **Paramètres**, faites défiler la page jusqu'à **Configuration Cloud**.
4. Cliquez sur le menu déroulant en regard du compte Cloud à configurer, puis effectuez l'une des opérations suivantes :
   - Cliquez sur **Modifier**.
     La boîte de dialogue **Configuration Cloud** apparaît .
     1. Utilisez les flèches Haut et Bas pour modifier l'une ou l'autre des options suivantes :
        - **Délai d'attente de la demande** : indiquée en minutes et secondes, l'option définit le temps qu'AppAssure doit consacrer à une seule tentative de connexion au compte Cloud quand il existe un retard. Les tentatives de connexion sont interrompues après l'expiration du délai.
        - **Nombre de tentatives :** détermine le nombre de tentatives que doit exécuter AppAssure avant de déterminer que le compte Cloud est inaccessible.
        - **Taille du tampon d'écriture :** détermine la taille de la mémoire tampon réservée à l'écriture des données archivées dans le Cloud.
        - **Taille du tampon de lecture :** détermine la taille du bloc réservé à la lecture des données archivées à partir du Cloud.
     2. Cliquez sur **Suivant**.
   - Cliquez sur **Réinitialiser**. Restaure les paramètres par défaut suivants de la configuration :
     - **Délai d'expiration de la demande :** 01:30 (minutes et secondes)

– **Nombre de tentatives :** 3 (tentatives)

Suppression d'un compte Cloud

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

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

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

Surveillance du système DL1000

Vous pouvez surveiller le statut des sous-systèmes d'appliance DL1000 en utilisant l'onglet **Appliance** de la page **Statut général**. La page **Statut général** affiche un voyant de statut en regard de chaque sous-système, ainsi que la description du statut qui indique l'état d'intégrité du sous-système.

Cette page fournit également des liens d'accès à des outils qui permettent de visualiser des informations détaillées sur chaque sous-système, ce qui qui peut être utile pour résoudre les éventuels avertissements ou erreurs. Le lien **Administrateur système**, disponible pour les sous-systèmes Matériel d'appliance et Matériel de stockage du matériel, demande de vous connecter à l'application d'administration du système utilisée pour la gestion du matériel. Pour plus d'informations sur l'application d'administration du système, voir le document *OpenManage Server Administrator User's Guide* sur le **site dell.com/support/manuals**.

Mise à niveau du système DL1000

REMARQUE : Dell recommande de télécharger la dernière version d'AppAssure depuis le portail d'activation des licences Dell à l'aide du programme d'installation.

REMARQUE : Pour les autres mises à niveau logicielles, vous recevez une notification de mise à niveau vers la dernière version.

Réparation du système DL1000

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

Restauration automatique rapide de l'appliance

RASR (Rapid Appliance Self Recovery) est un processus de restauration BMR (bare metal restore) où l'image par défaut créée en usine est reconstituée.
Pour effectuer la restauration RASR :

REMARQUE : Dell recommande de créer la clé USB RASR une fois que vous avez configuré l'appliance. Pour créer une clé USB RASR, reportez-vous à la section Création de la cléUSB RASR.

1. Insérez la clé USB RASR créée.
2. Redémarrez l'appliance à l'aide de la clé USB RASR.
3. Cliquez sur **Rapid Appliance Self Recovery**.
   Un écran d'accueil s'affiche.
4. Cliquez sur **Suivant**.
   L'écran de vérification **Conditions** s'affiche.

   REMARQUE : Veillez à ce que tous les matériels et les autres conditions soient vérifiés avant d'exécuter la restauration RASR.
5. Cliquez sur **Suivant**.
   L'écran de **sélection du mode de restauration** s'affiche avec trois options :
   - **Restauration du système**
   - **Assistant de récupération Windows**
   - **Restauration des paramètres définis en usine**
6. Sélectionnez **Restaurer les paramètres définis en usine** .
   This option will recover the operating system disk from the factory image.
7. Cliquez sur **Suivant**.
   L'écran **Configuration du stockage** s'affiche.
8. Dans l'écran **de restauration du système d'exploitation** , le message d'avertissement suivant s'affiche : `This operation will recover the operating system. All OS disk data will be overwritten.` dans une boîte de dialogue.
9. Cliquez sur **Oui**.
   Le disque du système d'exploitation commence la restauration du système d'exploitation d'origine.
10. Cliquez sur **Terminer**.

Création de la clé USB RASR

REMARQUE : Après l'installation initiale du logiciel, l **Assistant Configuration de l'appliance AppAssure** démarre automatiquement. L'icône de statut de l'onglet **Appliance** est jaune.

Pour créer une clé USB RASR :

1. accédez l'onglet **Appliance**.
2. Dans le volet de navigation de gauche, sélectionnez **Appliance** → **Sauvegarde**.
   La fenêtre **Créer un lecteur USB RASR** s'affiche.

   REMARQUE : Insérez une clé USB 16 Go ou plus, avant de tenter de créer la clé RASR.
3. Après avoir inséré une clé USB de 16 Go ou plus, cliquez sur **Créer un lecteur USB RASR maintenant**.
   Un message de **vérification de conditions** s'affiche.
   Une fois les conditions vérifiées, la fenêtre **Créer un lecteur USB RASR** affiche la taille minimale requise pour créer le lecteur USB et la **liste des chemins cible possibles.**
4. Sélectionnez la cible et cliquez sur **Créer**.
   Une boîte de dialogue de confirmation s'affiche.
5. Cliquez sur **Oui**.
   La clé de lecteur USB RASR est créée.

6. REMARQUE : Assurez-vous d'utiliser l'option Retirer le lecteur USB en toute sécurité ou la fonction Windows d'éjection de lecteur pour préparer la clé USB au retrait. Sinon, le contenu de la clé USB pourra être endommagé et la clé USB ne fonctionnera pas comme prévu.

Retirez la clé, étiquetez-la et rangez-la en vue d'une utilisation ultérieure.

3

Protection des stations de travail et des serveurs

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

Pour protéger les données en utilisant le système DL1000, ajoutez les postes de travail et les serveurs à protéger dans Core Console ; par exemple, ajoutez le serveur Exchange, SQL Server ou le serveur Linux.

REMARQUE : Dans ce chapitre, le terme *machine* désigne le logiciel AppAssure Agent installé sur la machine.

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

Déploiement d'un agent (installation en mode Pousser)

Le système DL1000 permet de déployer AppAssure Agent Installer sur les machines individuelles Windows à protéger. Exécutez les étapes suivantes pour envoyer le programme d'installation à un agent. Pour déployer des agents sur plusieurs machines simultanément, reportez-vous à Déploiement sur plusieurs machines.

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

Pour déployer un agent

1. Dans la zone de navigation de gauche de Core Console, cliquez sur **Machines protégées**.
2. Cliquez sur **Actions** → **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.

Zone de texte	Description
Redémarrage automatique après installation	Sélectionnez cette option indiquer si le core démarre à la fin du déploiement et de l'installation d'AppAssure Agent Installer.

4. Cliquez sur **Vérifier** pour valider les références que vous avez saisies.

   La boîte de dialogue **Déployer l'agent** affiche un message indiquant que la validation est en cours d'exécution.
5. Cliquez sur **Abandonner** si vous souhaitez annuler le processus de vérification.

   Une fois le processus de vérification terminé, un message s'affiche pour indiquer que la vérification est terminée.
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**.

Protection d'une machine

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

REMARQUE : Le logiciel AppAssure Agent doit être installé sur la machine pour être protégée. Vous pouvez choisir d'installer le logiciel AppAssure Agent avant cette procédure ou vous pouvez déployer le logiciel vers l'agent lorsque vous définissez la protection dans la boîte de dialogue **Connexion**. Pour installer le logiciel Appassure Agent pendant le processus de protection d'une machine, voir Déploiement du logiciel agent lors de la protection d'un agent.

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

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

Pour protéger un ordinateur

1. Redémarrez la machine sur laquelle le logiciel AppAssure Agent est installé, si vous ne l'avez pas déjà fait.
2. Dans la console Core de la machine de Core, cliquez sur **Protéger** → **Protéger une machine** dans la barre d'outils.

   L' **Assistant Protection de la machine** s'affiche.
3. Dans la page **Bienvenue**, sélectionnez les options d'installation appropriée :
   - Si vous n'avez pas besoin de définir un référentiel ni d'établir le cryptage, sélectionnez **Typique**.
   - Si vous ne souhaitez plus voir la page d'**Accueil** de l'**Assistant Protection de la machine**, cochez la case **Ignorer la page d'accueil lors de la prochaine ouverture de l'Assistant** .
4. Cliquez sur **Suivant**.
5. Dans la page **Connexion**, entrez les informations de la machine sur laquelle vous souhaitez vous connecter, comme indiqué 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 Core communique avec l'agent sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à cet ordinateur ; par exemple, administrateur.
Mot de passe	Le mot de passe utilisé pour vous connecter à cet ordinateur

6. Cliquez sur **Suivant**. Si la page **Protection** apparaît dans l'**Assistant Protection de la machine**, passez à l'étape 7.

   REMARQUE : Si la page **Installer l'agent** s'affiche ensuite dans l'**Assistant Protection d'une machine**, cela signifie que le logiciel d'agent n'est pas encore installé sur la machine choisie. Cliquez sur **Suivant** pour installer le logiciel d'agent. Ce logiciel doit être installé sur la machine à protéger et vous devez redémarrer cette dernière avant de pouvoir la sauvegarder vers le Core. Pour que le programme d'installation redémarre la machine d'agent, sélectionnez l'option **Après l'installation, redémarrer automatiquement la machine (recommandé)**, puis cliquez sur **Suivant**.

7. La valeur Nom d'hôte ou Adresse IP indiquée dans la boîte de dialogue **Connexion** s'affiche dans ce champ. (Facultatif) Entrez un nouveau nom pour la machine, qui sera affiché dans la console Core.
8. Sélectionnez la planification de protection appropriée :
   - Pour utiliser la planification de protection par défaut, dans l'option **Paramètres de planification**, sélectionnez **Protection par défaut (instantanés de tous les volumes, pris toutes les 3 heures)**. Avec la planification de protection par défaut, le Core prend des instantanés de la machine d'agent toutes les 3 heures. Ces instantanés de la machine d'agent peuvent être capturés toutes les heures (valeur minimale). Pour modifier les paramètres de protection, à tout moment après avoir fermé l'Assistant, y compris pour choisir les volumes à protéger, accédez à l'onglet Résumé de la machine d'agent spécifique.
   - Pour définir une planification de protection différente à l'aide de l'option **Paramètres de planification**, sélectionnez **Protection personnalisée**.
9. Sélectionnez une des options suivantes :
   - Si vous avez sélectionné une configuration standard dans l'**Assistant Protection de la machine** et défini un protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine que vous avez spécifiée.
   - Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (à savoir un instantané de toutes les données des volumes protégés) est transférée vers le référentiel sur AppAssure Core en fonction de l'horaire que vous avez défini, sauf si vous avez demandé la suspension initiale de la protection.
   - Si vous avez sélectionné la configuration Typique dans l'**Assistant Protection d'une machine** et choisi une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour en savoir plus sur cette opération, voir « Création de planifications de protection personnalisées ».
   - Si vous avez sélectionné la configuration Avancée pour l'**Assistant Protection d'une machine** et choisi la protection par défaut, cliquez sur **Suivant** et passez à l'étape 12 pour afficher les options de référentiel et de cryptage.
   - Si vous avez sélectionné la configuration avancée pour l' **Assistant Protection de la machine** et défini une protection personnalisée, cliquez sur **Suivant** et passez à l'étape 10 pour choisir les volumes à protéger.
10. Sur la page **Protection des volumes**, sélectionnez les volumes sur la machine agent à protéger. Si vous ne voulez pas inclure dans la protection des volumes répertoriés, cliquez dans la colonne Vérifier pour effacer la sélection, puis **Suivant**.

REMARQUE : Il est recommandé de protéger le volume réservé au système et celui qui contient le système d'exploitation (généralement, le lecteur C).

11. Sur la page **Planification de protection**, définissez une planification personnalisée.
12. Dans la page **Référentiel**, sélectionnez **Utiliser un référentiel existant**.
13. Cliquez sur **Suivant**.

    La page **Cryptage** s'affiche.
14. Le cas échéant, pour activer le cryptage, sur la page **Cryptage**, sélectionnez **Activer le cryptage**.

    Les champs **Clé de cryptage** apparaissent sur la page **Cryptage**.

    REMARQUE : Si vous activez le cryptage, il est appliqué aux données de tous les volumes protégés de la machine agent. Vous pouvez changer les paramètres ultérieurement dans l'onglet **Configuration** de Core Console.

    PRÉCAUTION : AppAssure utilise le cryptage 256 bits AES en mode CBC (Cipher Block Chaining) avec des clés 256 bits. Bien que le cryptage soit facultatif, Dell recommande vivement de créer une clé de cryptage et de protéger la phrase de passe que vous définissez. Stockez la phrase de passe dans un endroit sûr, car elle est indispensable à la restauration des données. Sans la phrase de passe la restauration des données est impossible.
15. Entrez les informations décrites dans le tableau suivant pour ajouter une clé de cryptage pour le Core.

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement.
Description	Entrez une description pour fournir des détails supplémentaires pour la clé de cryptage.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès.
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.

16. Cliquez sur **Terminer** pour enregistrer et appliquer vos paramètres.

    Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (instantané de toutes les données des volumes protégés) commence immédiatement à se transférer vers le référentiel sur le Core, sauf si vous avez demandé la suspension initiale de la protection.

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 la protection :

1. dans Core Console, cliquez sur le menu déroulant **Machines protégées** dans la zone de navigation de gauche.
2. Sélectionnez **Suspendre la protection** pour la machine pour laquelle vous souhaitez suspendre la protection.

   La boîte de dialogue **Suspendre la protection** s'affiche.
3. Sélectionnez l'une des options suivantes, puis cliquez sur **OK**.
   - Si vous souhaitez suspendre la protection jusqu'à ce que vous la rétablissiez explicitement, sélectionnez **Suspendre jusqu'à la reprise**.

- Si vous souhaitez suspendre la protection pendant une période, sélectionnez **Suspendre pendant**, puis dans les jours, les heures et les minutes, tapez ou sélectionnez la période de suspension.

REMARQUE : Pour rétablir la protection, sélectionnez **Rétablir la protection** dans le menu déroulant **Machines protégées** .

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. Cliquez sur **Machines protégées** dans le volet de navigation de gauche.
2. Cliquez sur **Actions → Déployer l'agent**.
   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.
   - **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.
   - **Protéger la machine après l'installation** : sélectionnez cette option pour qu'AppAssure crée un instantané de base des données après que vous avez ajouté la machine à la protection. Par défaut, l'option est sélectionnée. Si vous la désélectionnez, vous devez forcer manuellement la création d'un instantané lorsque vous êtes prêt à démarrer la protection des données.
   - **Nom d'affichage** : indique le nom de l'ordinateur qui s'affiche dans Core Console. Ce nom peut être identique au nom d'hôte.
   - **Port** : indique le numéro du port sur lequel le Core communique avec l'agent sur l'ordinateur. La valeur par défaut est 8006.
   - **Référentiel** : sélectionnez le référentiel dans lequel stocker les données de cet agent.

     REMARQUE : Vous pouvez stocker les données de plusieurs agents dans un même référentiel.
   - **Clé de cryptage** : indique si le cryptage doit être appliqué aux données de chaque volume de cet ordinateur à stocker dans le référentiel.

     REMARQUE : Vous définissez les paramètres de cryptage d'un référentiel dans l'onglet **Configuration** de la console Core.
4. Cliquez sur **Déployer**.
   La boîte de dialogue **Déployer un agent** se ferme. Il peut y avoir un délai avant l'affichage de l'agent sélectionné dans la liste d'ordinateurs protégés.

Comprendre les horaires de protection

Un horaire de protection définit le moment où les sauvegardes sont transférées des machines agent protégées vers AppAssure Core.

Les horaires de protection sont initialement définis à l'aide de l' **Assistant Protéger des machines** ou l'**Assistant Protéger plusieurs machines**. Vous pouvez alors modifier la planification existante à tout moment à partir de l'onglet Récapitulatif de la machine de l'agent.

AppAssure fournit un horaire de protection par défaut avec deux périodes de protection définies. La première période concerne les jours de la semaine (du lundi au vendredi), avec une seule période définie (de minuit à 23 h 59). L'intervalle par défaut (période entre les instantanés) est de 3 heures. La seconde période s'applique à la fin de la semaine (samedi et dimanche). L'intervalle par défaut pour la seconde période est de 3 heures.

Lorsque la protection est activée pour la première fois, l'horaire est activé. Ainsi, en utilisant les paramètres par défaut, quelle que soit l'heure du jour, la première sauvegarde a lieu toutes les trois heures.

Le transfert de la première sauvegarde enregistrée dans le core s'appelle une image d'instantané de base. Toutes les données sur tous les volumes (y compris le système d'exploitation, les applications et les paramètres), sont enregistrés dans le core. Par la suite, des instantanés incrémentiels (sauvegardes moins volumineuses, comportant uniquement les données modifiées sur l'agent depuis la dernière sauvegarde) sont enregistrés dans le core régulièrement en fonction de l'horaire défini.

Vous pouvez créer un horaire personnalisé pour modifier la fréquence des sauvegardes. Par exemple, vous pouvez remplacer l'intervalle pour la période pour les jours de la semaine par 60 minutes. Dans ce cas, des instantanés sont créés tous les heures. Vous pouvez également faire passer cet intervalle de 60 minutes à 180 minutes. Dans ce cas, des instantanés sont créés toutes les trois heures lorsque le trafic est faible.

Les autres options de la page de l' **Assistant Horaire de protection** comprennent une option pour l'heure de protection quotidienne. Avec cette option, une seule sauvegarde quotidienne est exécutée pour la période définie (la valeur par défaut est 12 h).

L'option de suspension initiale de la protection empêche la création d'une image de base (et toutes les sauvegardes, en fait) jusqu'à ce que vous rétablissiez la protection de manière explicite. Lorsque vous êtes prêt à protéger les machines en fonction de l'horaire de protection défini, vous devez rétablir explicitement la protection.

Création d'horaires personnalisés

1. Sur la page **Planification de protection** de la **machine protégée** ou de l'**Assistant Protection de plusieurs machines**, pour modifier l'intervalle d'une période, procédez comme suit :
   a. sélectionnez **Périodes**.
      Les périodes s'affichent et peuvent être modifiées. Les champs modifiables sont l'heure de début, l'heure de fin et l'intervalle (en minutes) de chaque période.
   b. Cliquez sur le champ d'intervalle et saisissez un intervalle en minutes.
      Par exemple, mettez en surbrillance l'intervalle existant et remplacez-le par la valeur **60** pour créer des instantanés toutes les 60 minutes pendant cette période.
2. Pour créer une période pleine ou creuse pour les jours de la semaine, modifiez la plage horaire de la période des jours de la semaine de sorte qu'elle n'inclut pas de période de 24 heures, définissez un intervalle optimal pour la période pleine, sélectionnez **Créer des instantanés pour le reste du temps** et définissez un intervalle pour la période creuse en procédant comme suit :
   a. sélectionnez **Périodes**.
      Les périodes s'affichent et peuvent être modifiées.

b. Cliquez sur **De** pour modifier l'heure de début de la période.

   La boîte de **Sélectionner l'heure** s'affiche.

c. Faites glisser les curseurs Heures et Minutes pour définir l'heure de début, puis cliquez sur **Terminé)**. Pour définir l'heure actuelle, cliquez sur **Maintenant**.

d. Cliquez sur **À** pour modifier l'heure de fin de la période.

   La boîte de **Sélectionner l'heure** s'affiche.

e. Faites glisser les curseurs Heures et Minutes pour définir l'heure de début, puis cliquez sur **Terminé)**. Pour définir l'heure actuelle, cliquez sur **Maintenant**.

3. Pour définir une heure pour une sauvegarde unique à effectuer tous les jours, sélectionnez l'option **Heure de la protection quotidienne**, puis entrez une heure dans le format HH:MM AM.
4. Pour définir la planification sans commencer les sauvegardes, sélectionnez **Suspendre initialement la protection**.

   Lorsque vous suspendez la protection dans l'Assistant, elle reste suspendue tant que vous ne la rétablissez pas explicitement. Une fois que vous la rétablissez, les sauvegardes sont exécutées en fonction de la planification que vous avez établie.
5. Cliquez sur **Terminer** ou **Suivant**.

Modification des horaires de protection

Vous pouvez modifier les horaires de protection de volumes spécifiques d'une machine.

Pour modifier des horaires de protection :

1. Dans Core Console, sélectionnez la machine avec un horaire de protection défini à changer.

   L'onglet Récapitulatif correspondant à la machine s'affiche.
2. Sélectionnez les volumes de la machine protégée à changer, puis cliquez sur **Définir un horaire**. Pour sélectionner tous les volumes à la fois, cochez la case dans la ligne d'en-tête.

   Initialement, tous les volumes partagent le même horaire de protection. En règle générale, il est recommandé de protéger, au minimum, le volume réservé du système et le volume contenant le système d'exploitation (généralement le lecteur C).

   La boîte de dialogue **Planification de protection** s'affiche.
3. Dans la boîte de dialogue **Horaire de protection**, si vous avez déjà créé un modèle d'horaire de protection et que vous voulez l'appliquer à l'agent, sélectionnez le modèle dans la liste déroulante, puis passez à l'étape 9.
4. Si vous souhaitez enregistrer le nouvel horaire de protection comme un modèle, entrez le nom du modèle dans la zone de texte.
5. Si vous souhaitez supprimer des périodes de l'horaire, désélectionnez les cases à cocher en regard de chaque option de période. Les options sont les suivantes :
   - **Lundi-vendredi** : cette plage de temps indique une semaine de travail standard de cinq jours.
   - **Samedi-dimanche** : cette plage de temps s'applique à un week-end standard.
6. Si les heures de début et de fin des jours de la semaine sont de minuit à 23h59, une seule période existe. Pour modifier l'heure de début ou de fin d'une période, procédez comme suit :
   a. Sélectionnez la durée appropriée.
   b. Cliquez dans la zone **Heure de début** pour modifier l'heure de début de la période.
   c. Faites glisser les curseurs Heures et Minutes pour définir l'heure de début, puis cliquez sur **Terminé)**. Pour définir l'heure actuelle, cliquez sur **Maintenant**.
   d. Cliquez dans la zone **Heure de fin** pour modifier l'heure de fin de la période.

      La boîte de **Sélectionner l'heure** s'affiche.

   e. Faites glisser les curseurs Heures et Minutes pour définir l'heure de début, puis cliquez sur **Terminé)**. Pour définir l'heure actuelle, cliquez sur **Maintenant**.

f. Modifiez l'intervalle de manière appropriée. Par exemple, si vous définissez une période de forte activité. remplacez l'intervalle de 60 minutes par 20 minutes pour créer des instantanés toutes les trois heures.

7. Si vous avez défini une période autre que minuit-23h59 à l'étape 6, et que vous voulez exécuter les sauvegardes dans les plages de temps restantes, vous devez ajouter d'autres périodes pour définir la protection en procédant comme suit :
   a. cliquez sur **Ajouter une période**.

      Sous la catégorie appropriée (jours de la semaine ou week-ends), une nouvelle période apparaît. Si la première période démarre après minuit, AppAssure démarre automatiquement cette période à 12h00. Par rapport à l'exemple ci-dessus, cette deuxième période commence à minuit. Il peut être nécessaire d'ajuster les heures ou les minutes des heures de début et de fin.
   b. Faites glisser les curseurs Heures et Minutes de manière appropriée pour les heures de heures de début et de fin.
   c. Modifiez l'intervalle en fonction de vos besoins. Par exemple, si vous définissez une période basse, remplacez l'intervalle de 60 minutes par 120 minutes pour créer des instantanés toutes les deux heures.
8. Si nécessaire, continuez à créer d'autres périodes en définissant des heures de début et de fin et des intervalles.

   REMARQUE : Si vous souhaitez supprimer une période ajoutée, cliquez sur la croix **X** à l'extrémité droite de la période. Si vous supprimez une période par erreur, vous pouvez cliquer sur **Annuler**.
9. Lorsque l'horaire de protection vous convient, cliquez sur **Appliquer**.

   La boîte de dialogue **Horaire de protection** se ferme.

Configuration des paramètres de la machine protégée

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. Dans Console Core, accédez à la machine à modifier.
2. Cliquez sur **Configuration** → **Paramètres**.
3. Cliquez sur **Modifier** pour modifier les paramètres de la machine décrits dans le tableau suivant.

Zone de texte	Description
Nom d'affichage	Entrez un nom d'affichage pour la machine. Nom de cette machine à afficher dans Core Console. Par défaut, il s'agit du nom d'hôte de la machine. Vous pouvez modifier le nom d'affichage pour le rendre plus convivial, si nécessaire.
Nom d'hôte	Entrez un nom d'hôte pour la machine.
Port	Entrez un numéro de port pour la machine.

Zone de texte	Description
	Le core utilise ce port 8006 pour communiquer avec cette machine.
Clé de cryptage	Modifiez la clé de chiffrement si nécessaire. Spécifie si le chiffrement doit être appliqué aux données pour chaque volume de cette machine qui sera stocké dans le référentiel.
Référentiel	Sélectionnez le référentiel des points de restauration. Affiche sur le référentiel sur le core dans lequel les données de la machine doivent être stockées. REMARQUE : Ce paramétrage peut uniquement être modifié s'il n'existe pas de points de restauration ou si le référentiel précédent est manquant.

Affichage des informations système d'un ordinateur

Le Core Console affiche toutes les machines protégées.

Pour afficher les informations système d'une machine :

1. Dans la zone de navigation de gauche de Core Console, sous **Machines protégées**, sélectionnez la machine pour afficher des informations détaillées sur le système.
2. Cliquez sur l'onglet **Outils**.

   L'onglet Informations système contient les informations suivantes :

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

   Les informations détaillées sur les volumes de cette machine comprennent :

   - Nom
   - ID de périphérique
   - Système de fichiers
   - Capacité (y compris brute, formatée et utilisée)

   Autres informations affichées sur la machine :

   - Processeurs
   - Cartes réseau
   - Les adresses IP associées à cette machine

Affichage d'informations de licence

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

Pour afficher les informations de licence

1. Dans le panneau de navigation, sélectionnez la machine à afficher.
2. Cliquez sur **Configuration** → **Licences**.
   L'écran **État** affiche les détails de licences produit.

Modification des paramètres de transfert

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

PRÉCAUTION : La modification des paramètres de transfert peut avoir un impact important sur l'environnement AppAssure. Avant de modifier la valeur des paramètres de transfert, consultez le Guide de réglage des performances du transfert dans la base de connaissances Dell AppAssure.

Il existe trois types de transferts dans le système DL1000 :

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.
Restaurer	Un processus permettant de restaurer les informations de sauvegarde sur une machine protégée.

Le transfert de données dans le système DL1000 implique la transmission d'un volume de données sur un réseau, des machines AppAssure Agent vers le core. En cas de réplication, le transfert se produit également du core source vers le core cible.

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

- Nombre de transferts de données d'agent simultanés
- Nombre de flux de données simultanés
- Quantité de données modifiées sur le disque
- Bande passante réseau disponible
- Performances du sous-système de disques du référentiel
- Quantité de mémoire disponible pour la mise en tampon des données

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

Pour modifier les paramètres de transfert :

1. Dans Core Console, accédez à la machine que vous souhaitez modifier.
2. Cliquez sur l'onglet **Configuration**, puis sur **Paramètres de transfert**.
   La page **Paramètres de transfert** actuels s'affiche.
3. Dans la page **Paramètres de transfert**, cliquez sur **Modifier**.
   La boîte de dialogue **Paramètres de transfert** s'affiche.

4. Entrez les options **Paramètres de transfert** de la machine tel que décrit dans le tableau suivant.

Zone de texte	Description
Priorité	Définit la priorité de transfert entre les machines protégées. Vous pouvez attribuer à chaque machine une priorité par rapport aux autres machines protégées. Sélectionnez un numéro de 1 à 10, 1 représentant la priorité la plus élevée. Le paramètre par défaut est la priorité 5. REMARQUE : La priorité s'applique aux transferts se trouvant dans la file d'attente.
Nombre maximal de flux simultanés	Définit le nombre maximal de liaisons TCP envoyées au core pour traitement en parallèle par l'agent. REMARQUE : Dell vous recommande de définir cette valeur sur 8. Si vous constatez une perte de paquets, augmentez cette valeur.
Nombre maximal d'écritures simultanées	Définit le nombre maximal d'actions d'écriture sur disque simultanées pour chaque connexion d'agent. REMARQUE : Dell vous recommande d'utiliser ici la même valeur que pour Nombre maximal de flux simultanés. En cas de perte de paquets, choisissez une valeur légèrement plus faible. Par exemple, si Nombre maximal de flux simultanés est défini sur 8, définissez cette option sur 7.
Nombre maximal de tentatives	Définit le nombre maximal de tentatives pour chaque machine protégée, en cas d'échec de certaines opérations.
Taille maximale de segment	Spécifie la quantité maximale de données, en octets, qu'une machine peut recevoir sur un seul segment TCP. La valeur par défaut est 4194304. **PRÉCAUTION : Ne modifiez pas cette option, conservez la valeur par défaut.**
Profondeur maximale de file d'attente de transfert	Spécifie le nombre de commandes simultanées que vous pouvez envoyer. Vous pouvez définir cette option sur une valeur plus élevée si votre système effectue un grand nombre d'opérations d'entrée/sortie simultanées.
Lectures en attente par flux	Spécifie le nombre d'opérations de lecture en file d'attente qui sont stockées dans le back-end. Ce paramètre permet de contrôler la mise en file d'attente des agents. REMARQUE : Dell vous recommande de définir cette valeur sur 24.
Programmes d'écriture exclus	Sélectionnez un service d'écriture si vous souhaitez l'exclure. Comme les processus d'écriture affichés dans la liste sont propres à la machine que vous configurez, vous ne verrez pas tous les services d'écriture de la liste. Ceux qui s'affichent peuvent être les suivants : • Rédacteur ASR • Rédacteur BITS • Rédacteur COM+ REGDB • Rédacteur de compteurs de performance

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

5. Cliquez sur **OK**.

Archivage des données

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

Création d'une archive

Pour créer une archive :

1. Dans la console Core, cliquez sur **Outils** → **Archive** → **Créer**.
   La boîte de dialogue **Assistant Ajout d'une archive** apparaît.
2. Sur la page **Créer** de l'**Assistant Ajout d'une archive**, sélectionnez l'une des options suivantes dans la liste déroulante **Type d'emplacement** :
   - Local

- Réseau
- Cloud

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

Tableau 2. Création d'une archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où l'archive doit résider. Par exemple, d:\travail\archive.
Réseau	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où l'archive doit résider. Par exemple, \\nom-serveur\nom-partage.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Il est utilisé pour établir les références de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe pour le partage réseau. Il est utilisé pour établir les références de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante. **REMARQUE :** Pour sélectionner un compte Cloud, vous devez commencer par l'ajouter Core Console. Reportez-vous à Ajout d'un compte Cloud.
	Conteneur	Sélectionnez un conteneur associé à votre compte dans le menu déroulant.
	Nom de dossier	Entrez un nom pour le dossier où les données d'archive doivent être enregistrées. Le nom par défaut est AppAssure 5-Archiv-[DATE-CRÉATION]-[HEURE-CRÉATION].

4. Cliquez sur **Suivant**.
5. Dans la page **Machines** de l'Assistant, sélectionnez la machine ou les machines protégées contenant les points de restauration à archiver.

6. Cliquez sur **Suivant**.
7. Dans la page **Options**, saisissez les informations décrites dans le tableau suivant.

Zone de texte	Description
Taille maximale	Les archives de données volumineuses peuvent être divisées en plusieurs segments. Sélectionnez la quantité maximale d'espace à réserver pour la création de l'archive, en effectuant l'une des opérations suivantes : • Sélectionnez Cible entière pour réserver tout l'espace disponible dans le chemin de destination fourni à l'étape 4. (Par exemple, si l'emplacement choisi est D:\travail\archive, tout l'espace disponible sur le disque D: est réservé.) • Sélectionnez la zone de texte vide, utilisez les flèches Haut et Bas pour saisir un montant, puis sélectionnez une unité de mesure dans la liste déroulante pour personnaliser la quantité maximale d'espace à réserver. **REMARQUE :** Les archives de Cloud Amazon sont automatiquement divisées en segments de 50 Go. Les archives de Cloud Windows Azure sont automatiquement divisées en segments de 200 Go.
Action de recyclage	Sélectionnez l'une des options d'action de recyclage suivantes : • **Ne pas réutiliser** : n'écrase ni n'efface aucune des données archivées existantes de l'emplacement. Si le dossier n'est pas vide, l'écriture de l'archive échoue. • **Remplacer ce Core** : écrase toutes les données archivées pré-existantes appartenant à ce Core mais laisse intactes les données des autres Cores. • **Effacer complètement** : efface toutes les données archivées du répertoire avant d'écrire la nouvelle archive. • **Incrémentielle** : permet d'ajouter des points de restauration à une archive existante. Cette option compare les points de restauration pour éviter la duplication des données qui existent déjà dans l'archive.
Commentaire	Entrez toutes les informations supplémentaires dont la capture est nécessaire pour l'archive. Le commentaire s'affiche si vous importez l'archive ultérieurement.
Utiliser un format compatible	Sélectionnez cette option pour archiver vos données dans un format compatible avec les versions précédentes des Cores. **REMARQUE :** Le nouveau format offre de meilleures performances, mais n'est pas compatible avec les anciens Cores.

8. Cliquez sur **Suivant**.
9. Sur la page Plage de dates, entrez la date de début et la date d'expiration des points de restauration à archiver.
   - Pour indiquer une heure, cliquez sur l'heure affichée (valeur par défaut, 8h00 du matin) pour faire apparaître le curseur, et sélectionnez des heures et des minutes.
   - Pour saisir une date, cliquez sur la zone de texte pour afficher le calendrier, puis cliquez sur le jour souhaité.
10. Cliquez sur **Terminer**.

Importation d'une archive

Pour importer une archive :

1. Dans Core Console, cliquez sur **Outils** → **Archive** → **Importer**.
2. Pour **Type d'emplacement**, sélectionnez l'une des options suivantes dans la liste déroulante :
   - Local
   - Réseau
   - Cloud
3. Entrez les détails de l'archive comme l'indique le tableau suivant, selon le type d'emplacement choisi à l'étape 3.

Tableau 3. Importation d'une archive

Option	Zone de texte	Description
Local	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin vers l'emplacement auquel l'archive doit résider. Par exemple, `d:\work \archive`ea.
Réseau	Emplacement de sortie	Indiquez l'emplacement de sortie. Il sert à définir le chemin de l'emplacement où l'archive doit résider. Par exemple, \ \nom-serveur\nom-partage.
	Nom d'utilisateur	Entrez un nom d'utilisateur. Il est utilisé pour établir les références de connexion du partage réseau.
	Mot de passe	Entrez un mot de passe pour le partage réseau. Il est utilisé pour établir les références de connexion du partage réseau.
Cloud	Compte	Sélectionnez un compte dans la liste déroulante. **REMARQUE :** Pour sélectionner un compte Cloud, vous devez commencer par l'ajouter Core Console. Reportez-vous à Ajout d'un compte Cloud.
	Conteneur	Sélectionnez un conteneur associé à votre compte dans le menu déroulant.

Option	Zone de texte	Description
	Nom de dossier	Entrez un nom pour le dossier où les données d'archive doivent être enregistrées. Le nom par défaut est AppAssure 5-Archiv-[DATE-CRÉATION]-[HEURE-CRÉATION].

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.

Archivage dans un Cloud

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

Pour exporter une archive vers un Cloud :

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

Affichage des diagnostics du système

Dans AppAssure, des informations de diagnostic sont disponibles pour afficher les données des journaux des machines protégées. En outre, vous pouvez afficher et télécharger les informations de diagnostic du Core.

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 Core Console, cliquez sur **Outils** → **Diagnostics** → **Afficher le journal**.
   La page **Télécharger le journal du core** s'affiche.
2. Cliquez sur le lien **Cliquez ici pour commencer le téléchargement**
   Un message demande d'ouvrir ou d'enregistrer le fichier.
3. Choisissez la méthode de votre choix pour traiter le fichier journal.

Téléchargement des journaux de la machine

1. Accédez à Core Console, cliquez sur **Outils** → **Diagnostics** → **Télécharger le journal**.

La page **Téléchargement d'un journal** s'affiche.

2. Sélectionnez **Cliquez ici pour commencer le téléchargement**.

   L'onglet Événements s'affiche pour vous permettre d'identifier l'avancement du téléchargement des informations de journal du core et de toutes les machines protégées.

Annulation d'opérations d'un ordinateur

Vous pouvez annuler les opérations en cours d'exécution d'une machine. Vous pouvez annuler l'instantané actuel ou toutes les opérations en cours, qui comprennent les exportations et les réplications.

Pour annuler les opérations d'une machine :

1. Dans Core Console, sélectionnez la machine dont vous voulez annuler les opérations.
2. Dans **Événements**, développer les détails de l'événement ou de l'opération à annuler.
3. Cliquez sur **Annuler**.

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

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

1. Dans Core Console, accédez à la machine protégée à afficher.

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 :

- Nom
- Type de système de fichiers
- Utilisation de l'espace
- Programmation actuelle
- Prochain instantané
- 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 :

- État en ligne
- Nom

- Chemin d'installation
- Version

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 :

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

Gestion de plusieurs machines

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

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

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

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

Déploiement sur plusieurs machines

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

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

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

REMARQUE : Les machines que vous déployez doivent avoir accès à Internet pour télécharger et installer les composants, car AppAssure utilise la version Web d'AppAssure Agent Installer pour déployer les composants d'installation. Si l'accès à Internet n'est pas disponible, vous pouvez envoyer le programme d'installation d'AppAssure Agent depuis la machine Core. Vous pouvez télécharger les mises à jour du core et de l'agent depuis le portail des licences.

Surveillance du déploiement de plusieurs machines

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

Pour surveiller le déploiement de plusieurs machines :

1. Dans Core Console, cliquez sur **Événements → Alertes**.
2. Accédez à l'onglet d'accueil AppAssure Core, puis cliquez sur l'onglet **Événements** .

   Les événements d'alerte apparaissent dans la liste en indiquant l'heure de l'événement et un message. Pour chaque déploiement réussi du logiciel agent, une alerte s'affiche indiquant que la machine protégée a été ajoutée.
3. Le cas échéant, cliquez sur un lien d'une machine protégée.

   L'onglet Récapitulatif de la machine sélectionnée apparaît en affichant des informations pertinentes, notamment :
   - Nom d'hôte de la machine protégée
   - Dernier instantané, le cas échéant
   - Heure de la prochaine création d'instantané planifiée, en fonction de l'horaire de protection que vous avez sélectionné
   - Temps restant
   - Clé de cryptage (éventuelle) utilisée pour cet agent protégé
   - Version du logiciel agent.

Protection de plusieurs machines

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

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

Pour protéger plusieurs machines :

1. Dans Core Console, cliquez sur **Protéger → Protéger en masse**.

   L'**Assistant Protection de plusieurs machines** s'affiche.
2. Sélectionnez l'option d'installation appropriée.
   - Si vous n'avez pas besoin de définir un référentiel ni d'établir le cryptage, sélectionnez **Typique**.
   - Si vous ne souhaitez plus afficher la page d'accueil de l'Assistant Protection de la machine, sélectionnez **Ne plus afficher cette page d'accueil lors de la prochaine ouverture de l'Assistant**.
3. Cliquez sur **Suivant**.

   La page **de connexion** s'affiche.
4. Ajoutez les machines que vous souhaitez protéger en cliquant sur l'une des options suivantes :
   - Cliquez sur **Active Directory** pour spécifier les machines d'un domaine Active Directory. Entrez les informations d'identification décrites dans le tableau ci-dessous, puis cliquez sur **Suivant**.

- Cliquez sur **vCenter/ESXi** pour spécifier des machines virtuelles sur un hôte virtuel vCenter/ESXi. Entrez les informations d'identification décrites dans le tableau ci-dessous, puis cliquez sur **Suivant**.

Zone de texte	Description
Hôte	Nom d'hôte ou adresse IP du domaine Active Directory ou du serveur VMware vCenter ou de l'hôte virtuel ESX(i).
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.

- Pour ajouter des machines manuellement, sélectionnez **Ajouter les machines manuellement**. Cliquez sur **Suivant**.

5. Dans la page **Machines** pour spécifier des machines manuellement, saisissez les informations de connexion suivantes de chaque machine sur une ligne distincte, puis cliquez sur **Suivant**.`hostname::username::password::port`
6. Dans la page **Machines**, pour spécifier les machines identifiées depuis un domaine Active Directory ou un serveur VMware vCenter/hôte virtuel ESX(i), sélectionnez chaque machine appropriée à protéger dans la liste, puis cliquez sur **Suivant**.

   Le système vérifie chaque machine que vous avez ajoutée automatiquement, et la page **Protection** s'affiche.
7. Sur la page **Protection**, sélectionnez la planification de protection :
   - pour utiliser la planification de protection par défaut, dans l'option **Paramètres de planification**, sélectionnez **Protection par défaut (instantanés toutes les heures de tous les volumes)**.
   - Si vous souhaitez définir un horaire de protection différent, dans l'option des paramètres de planification, sélectionnez **Protection personnalisée**, puis cliquez sur **Suivant**.
8. Effectuez la configuration comme suit :
   - si vous avez sélectionné une configuration standard pour l'**Assistant Protéger plusieurs machines** et la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger les machines que vous avez spécifiées.
   - Si vous avez sélectionné une configuration standard pour l'**Assistant Protection de plusieurs machines** et défini une protection personnalisées, cliquez sur **Suivant**, puis définissez un horaire personnalisé.
   - Si vous avez sélectionné Configuration avancée pour l'Assistant Protection de la machine, cliquez sur **Suivant** et passez à l'étape 9 pour afficher les options de référentiel et de cryptage.
9. Dans la page **Référentiel**, sélectionnez **Utiliser un référentiel existant**.
10. Cliquez sur **Suivant**.

    La page **Cryptage** s'affiche.
11. Pour activer le **cryptage**, sur la page Cryptage, Sélectionnez **Activer le cryptage**.

    Les champs de clé de cryptage apparaissent sur la page **Cryptage**.

    REMARQUE : Si vous activez le cryptage, il est appliqué aux données de tous les volumes protégés des machines que vous avez spécifiées pour la protection. Vous pouvez changer les paramètres ultérieurement dans l'onglet **Configuration** de Core Console. Pour en savoir plus sur le cryptage, reportez-vous à Gestion de la sécurité .
12. Entrez les informations décrites dans le tableau suivant pour ajouter une clé de cryptage pour le Core.

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement.

Zone de texte	Description
Description	Entrez une description pour fournir des détails supplémentaires pour la clé de cryptage.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès.
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.

13. Cliquez sur **Terminer** pour enregistrer et appliquer vos paramètres.

Surveillance de la protection de plusieurs machines

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

Pour surveiller la protection de plusieurs machines, accédez à l'onglet d'accueil de Core Console, puis cliquez sur **Événements** .

L'onglet Événements affiche les tâches, les alertes et les événements. Lorsque les volumes sont transférés, le statut et les heures de début et de fin s'affichent dans le volet Tâches. Vous pouvez également filtrer les tâches par statut (actives, en attente, terminée ou ayant échoué).

Lors de l'ajout de chaque machine protégée, une alerte est consignée pour indiquer si l'opération a abouti ou si des erreurs ont été enregistrées.

4

Restauration de données

Gestion de la restauration

L'AppAssure Core peut immédiatement restaurer des données ou restaurer des machines sur des machines physiques ou virtuelles à partir de points de restauration. Les points de restauration contiennent les instantanés de volumes d'agent capturés au niveau du bloc. Ces instantanés prennent en compte les applications ; ainsi, toutes les transactions ouvertes et tous les journaux de transactions de cumul restaurés sont complets et les caches sont vidés sur disque avant la création de l'instantané. L'utilisation d'instantanés prenant en compte l'application en conjonction avec Verified Recovery (Restauration vérifiée) permet au Core d'effectuer plusieurs types de restauration, notamment :

- Restauration de fichiers et de dossiers
- Restauration de volumes de données à l'aide de Live Recovery
- Restauration de volumes de données pour Microsoft Exchange Server et Microsoft SQL Server à l'aide de Live Recovery
- Restauration sans système d'exploitation à l'aide d'Universal Recovery
- Restauration sans système d'exploitation sur un matériel différent à l'aide d'Universal Recovery
- Exportation ad-hoc et exportation continue sur des machines virtuelles

Gestion des instantanés et points de restauration

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

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

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

Affichage de points de restauration

Pour afficher les points de restauration :

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

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

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

Affichage d'un point de restauration spécifique

Pour afficher un point de restauration particulier :

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

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

Informatif	Description
Actions	Le menu **Actions** inclut les opérations suivantes, que vous pouvez réaliser sur le point de restauration sélectionné : **Monter** : sélectionnez cette option pour monter le point de restauration sélectionné. Pour plus d'informations sur le montage du point de restauration sélectionné, voir Montage d'un point de restauration d'une machine Windows. **Exporter** : cette option permet d'exporter le point de restauration sélectionné vers ESXi, un poste de travail VMware ou HyperV. **Restaurer** : sélectionnez cette option pour exécuter une restauration depuis le point de restauration sélectionné vers le volume que vous spécifiez.
Contenu	La zone Contenu contient une ligne pour chaque volume dans le point de restauration développé, qui répertorie les informations suivantes pour chaque volume : **Statut** indique le statut actuel du point de restauration. **Titre** indique le volume dans le point de restauration. **Taille** affiche la quantité d'espace que le point de restauration consomme dans le référentiel.

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 Core Console, sélectionnez la machine à monter sur un système de fichiers local.

   L'onglet **Récapitulatif** correspondant à la machine sélectionnée apparaît.
2. Cliquez sur l'onglet **Points de restauration**.
3. Dans la liste des points de restauration, cliquez sur **>** pour développer le point de restauration à monter.
4. Dans les détails de ce point de restauration, cliquez sur **Monter**.

   La boîte de dialogue **Monter des points de restauration** s'ouvre.
5. 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.
6. Cliquez sur **Monter** pour monter le point de restauration.

Démontage des points de restauration sélectionnés

Pour effectuer un démontage, sélectionnez des points de restauration :

1. Accédez à Core Console, puis cliquez sur **Outils** → **Montages**.
2. Sur la page **Montages locaux**, à côté du point de montage du point de restauration à démonter, cliquez sur **Démonter**.
3. Dans la fenêtre Démontage du point de restauration, cliquez sur **Oui** pour confirmer.

Démontage de tous les points de restauration

Pour démonter tous les points de restauration

1. Accédez à Core Console, puis cliquez sur **Outils** → **Montages**.
2. Sur la page **Montages locaux**, cliquez sur **Démonter tout**.
3. Dans la fenêtre **Démonter le point de restauration**, cliquez sur **Oui** pour confirmer.

Montage d'un point de restauration pour une machine Linux

En utilisant l'utilitaire **aamount** dans AppAssure, vous pouvez monter à distance un volume à partir d'un point de restauration sous la forme d'un volume local sur une machine Linux.

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** d'AppAssure en tant qu'utilisateur root ou super utilisateur, par exemple : **sudo aamount**
4. 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 du serveur Core.
6. Entrez les informations de connexion du serveur Core, c'est-à-dire le nom d'utilisateur et le mot de passe.

   La liste de toutes les machines protégées par le serveur AppAssure s'affiche. Chaque machine est identifiée comme suit : numéro d'article, hôte/adresse IP et numéro d'identification de la machine. Par exemple : 293cc667-44b4-48ab-91d8-44bc74252a4f
7. Entrez la commande suivante pour répertorier les points de restauration qui sont disponibles pour une machine : **lr <line_number_of_machine>**
8. Saisissez la commande suivante pour sélectionner et monter le point de restauration spécifié dans le point/chemin de montage /chemin spécifié : **m <volume_recovery_point_ID_number> <path>**
9. Pour vérifier que le montage a abouti, entrez la commande suivante qui doit indiquer le volume distant attaché : **l**

Suppression de points de restauration

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

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

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

Pour supprimer des points de restauration :

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

Suppression d'une chaîne de points de restauration orphelins

Un point de restauration orphelin est un instantané incrémentiel qui n'est associé à aucune image de base. Les instantanés suivants continuent à être créés à partir de ce point de restauration. Sans image de base, les points de restauration résultants sont incomplets et ne contiendront sans doute pas les données nécessaires pour effectuer une restauration. Ces points de restauration sont considérés faire partie de la chaîne de points de restauration orphelins. Dans ce cas, la meilleure solution consiste à supprimer la chaîne et à créer une 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 Core console, sélectionnez la machine protégée dont vous souhaitez supprimer la chaîne de points de restauration orphelins.
2. Cliquez sur l'onglet **Points de restauration**.
3. Sous **Points de restauration**, développez le point de restauration orphelin.
   Ce point de restauration est marqué (dans la colonne **Type**) de la mention **Incrémentiel orphelin**.
4. En regard de l'option **Actions**, cliquez sur **Supprimer**.
   La fenêtre **Supprimer les points de restauration** s'affiche.
5. Dans la fenêtre **Supprimer les points de restauration**, cliquez sur **Oui**.

   PRÉCAUTION : La suppression de ce point de restauration supprime l'ensemble de la chaîne de points de restauration, y compris les points de restauration incrémentiels qui se produisent avant ou après, jusqu'à l'image de base suivante. Cette opération ne peut pas être annulée.

Forcer un instantané

Le fait de forcer un instantané permet de forcer un transfert de données pour la machine protégée. Lorsque vous forcez un instantané, le transfert démarre immédiatement ou est ajouté à la file d'attente. Seules les données modifiées 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 : cela s'appelle une image de base.

Pour forcer un instantané :

1. Dans Core Console, sélectionnez la machine ou le cluster ayant le point de restauration pour lequel vous souhaitez forcer un instantané.
2. Cliquez sur l'onglet **Récapitulatif** dans la section **Volumes**, puis sélectionnez 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.

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 cible), vous pouvez uniquement exporter les données depuis le core cible à la fin de la réplication.

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

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

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

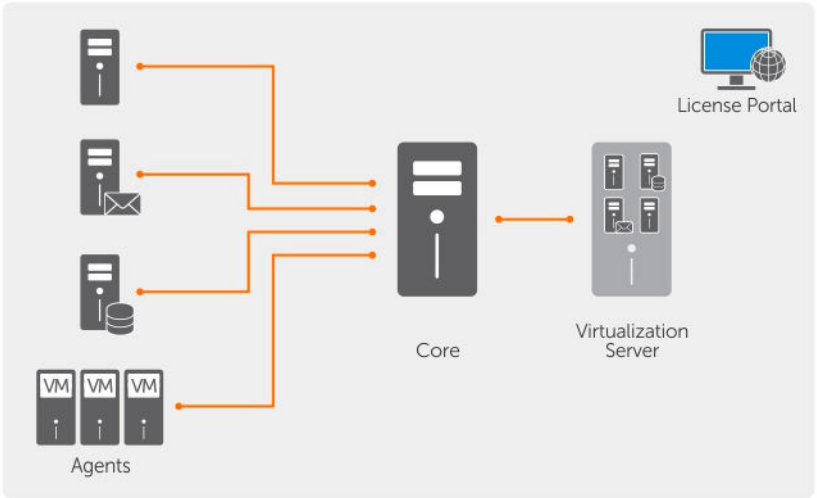

Figure 4. Exportation de données vers une machine virtuelle

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

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

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

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

Limites de support des volumes dynamiques et de base

Dell AppAssure permet de créer des instantanés pour tous les volumes de base et les volumes dynamiques. AppAssure permet également d'exporter des volumes dynamiques simples situés sur un seul disque physique. Les volumes dynamiques simples ne sont pas des volumes agrégés par bande, mis en miroir ou répartis.

Les disques dynamiques (à l'exception des disques de base en disques dynamiques simples, comme expliqué précédemment) ne sont pas disponibles pour la sélection dans l'assistant d'exportation. Les volumes dynamiques non simples comportent des géométries de disque arbitraires impossibles à interpréter entièrement. AppAssure, par conséquent, ne prend pas en charge l'exportation des volumes dynamiques complexes ou non simples.

Gestion des exportations

Sous l'onglet **Disque de secours virtuel** dans Core Console, vous pouvez afficher le statut des exportations que vous avez configurées, y compris les exportations ponctuelles et les exportations continues pour un disque de secours virtuel. Dans cet onglet, vous pouvez gérer les exportations en suspendant, arrêtant ou supprimant les exportations ou en affichant la file d'attente des exportations à venir.

REMARQUE : Seul le système Dell DL1000, 3 To avec 2 machines virtuelles prend en charge l'exportation ponctuelle et l'exportation en continu (disque de secours virtuel).

1. Dans Core Console, accédez à l'onglet **Disque de secours virtuel** .

   Sous l'onglet **Disque de secours virtuel** figure le tableau des paramètres d'exportation enregistrés, qui contient également les informations décrites dans le tableau suivant.

Menu	Description
Condition	REMARQUE : Le statut de la configuration de disque virtuel de secours est définie par la couleur de l'icône. Vert : le disque virtuel de secours est correctement configuré, actif et non suspendu. La prochaine exportation de disque de secours virtuel est effectuée après l'instantané suivant. Jaune : le disque de secours virtuel est suspendu et toujours enregistré par le Core. Cependant, après un nouveau transfert, la tâche d'exportation ne démarre pas automatiquement, et il n'existe pas pas de nouvelles exportations de disque de secours virtuel pour l'agent.
Nom de la machine	Nom de la machine source.
Destination	Machine virtuelle et chemin vers lesquels les données sont exportées.
Type d'exportation	Type de plate-forme de machine virtuelle de l'exportation, tel que ESXi, VMware, Hyper-V ou VirtualBox.
Dernière exportation	Date et heure de la dernière exportation. Si une exportation vient d'être ajoutée et qu'elle n'est pas terminée, un message s'affiche indiquant que l'exportation n'a pas encore été effectuée. Si l'exportation a échoué ou a été annulée, un message d'avertissement s'affiche.

2. Pour gérer les paramètres d'exportation enregistrés, sélectionnez une exportation, puis cliquez sur l'une des options suivantes :
   - **Suspendre** : pour suspendre l'exportation.
   - **Rétablir** : pour rétablir exportation suspendue.
   - **Forcer** : pour forcer une nouvelle exportation. Cette option peut être utile lorsqu'un disque de secours virtuel est suspendu et redémarré, ce qui signifie que la tâche d'exportation redémarre uniquement après un nouveau transfert. Si vous ne souhaitez pas attendre le nouveau transfert, vous pouvez forcer une exportation.
3. Pour supprimer une exportation à partir du système, cliquez sur **Supprimer**. Lorsque vous supprimez une exportation, l'exportation est supprimée définitivement du système et vous ne pouvez pas la redémarrer.
4. Pour afficher des détails concernant les exportations actives en file d'attente à exécuter, cliquez sur **Afficher la file d'attente des exportations**.

   Le tableau suivant s'affiche :

Menu	Description
Nom de la machine	Nom de la machine source.

Menu	Description
Destination	Le disque de secours virtuel est correctement configuré, actif et non suspendu. La prochaine exportation de disque virtuel de secours est effectuée après l'instantané suivant.
Type d'exportation	Le disque virtuel de secours est suspendu et toujours enregistré par le Core. Cependant, après un nouveau transfert, la tâche d'exportation ne démarre pas automatiquement, et il n'existe pas de nouvelles exportations de disque de secours virtuel pour l'agent.
Type de planification	Type d'exportation : ponctuelle ou continue.
Condition	Avancement de l'exportation, affiché sous la forme d'un pourcentage dans une barre d'avancement.

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

Vous pouvez exporter des données à partir des 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 la machine.

REMARQUE : Seul le système Dell DL1000, 3 To avec 2 machines virtuelles prend en charge l'exportation ponctuelle et l'exportation en continu (disque de secours virtuel).

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

1. Dans Core Console, cliquez sur l'onglet **Machines protégées**.
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 :
   - Ponctuelle
   - Disque virtuel de secours

   La boîte de dialogue **Assistant Exportation** apparaît.

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

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

Exécution d'une exportation ESXi ponctuelle

Pour effectuer une exportation ESXi ponctuelle :

1. Dans la Core Console, accédez à la machine à exporter.
2. Sur l'onglet **Récapitulatif**, cliquez sur **Actions** → **Exportation** → **ponctuelle**.
   L' **Assistant Exportation** apparaît sur la page **Machines protégées**.
3. Sélectionnez une machine à exporter, puis cliquez sur **Suivant**.
4. Sur la page **Points de restauration**, sélectionnez le point de restauration à exporter, puis cliquez sur **Suivant**.

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 page **Destination** de l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers une machine virtuelle**, sélectionnez **ESX(i)**.
2. Saisissez les paramètres d'accès 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.

3. Sur la page **Options de la machine virtuelle**, entrez les informations décrites dans le tableau suivant.

Zone de texte	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Stockage des données	Sélectionnez un magasin de données dans la liste déroulante.
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle.
Mémoire	Spécifiez l'utilisation de la mémoire.
Approvisionnement de disque	Sélectionnez le type d'approvisionnement de disque, dynamique ou fixe.
Adressage de disque	Spécifiez le type de mappage : Automatique ou Manuel.
Version	Sélectionnez la version de la machine virtuelle.

4. Cliquez sur **Suivant**.
5. Dans la page **Volumes**, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.
6. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

   REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

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

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

1. Dans Core Console, effectuez l'une des opérations suivantes :
   - Sous l'onglet, Disque de secours virtuel, cliquez sur **Ajouter** pour lancer l' **Assistant Exportation**. Sur la page **Machines protégées** de l'**Assistant Exportation**, sélectionnez la machine protégée à exporter, puis cliquez sur **Suivant**.
   - Accédez à l'ordinateur à exporter, puis cliquez sur **Actions** → **Exporter** → **Disque de secours virtuel**.
2. Dans la page **Destination** de l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers une machine virtuelle**, sélectionnez **ESXi**.

3. Entrez les informations d'accès à la machine virtuelle, décrites dans le tableau suivant, puis cliquez sur **Suivant**.

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

4. Sur la page **Options de la machine virtuelle**, entrez les informations décrites dans le tableau suivant.

Zone de texte	Description
Pool de ressources	Sélectionnez un pool de ressources dans la liste déroulante.
Stockage des données	Sélectionnez un magasin de données dans la liste déroulante.
Nom de la machine virtuelle	Entrez un nom pour la machine virtuelle.
Mémoire	Cliquez sur Utiliser une quantité spécifique de RAM pour spécifier la quantité de RAM à utiliser, par exemple, 4096 Mo. La quantité minimale autorisée est de 512 Mo et le maximum est déterminé par la capacité et les limites des machines hôte.
Approvisionnement de disque	Sélectionnez le type d'approvisionnement de disque, dynamique ou fixe.
Adressage de disque	Spécifiez le type de mappage : Automatique ou Manuel.
Version	Sélectionnez la version de la machine virtuelle.

5. Cliquez sur **Suivant**.
6. Dans la page **Volumes**, sélectionnez les volumes à exporter, puis cliquez sur **Suivant**.
7. Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

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

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

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

Pour effectuer une exportation VMware Workstation ponctuelle

1. Dans la Core Console, accédez à la machine à exporter.
2. Dans le **récapitulatif**, cliquez sur **Actions → Exporter → Ponctuelle**.
   L' **Assistant Exportation** apparaît sur la page **Machines protégées**.

3. Sélectionnez une machine pour l'exportation, puis cliquez sur **Suivant**.
4. Sur la page **Points de restauration**, sélectionnez le point de restauration à exporter, puis cliquez sur **Suivant**.

Définition des paramètres ponctuels pour exporter VMware Workstation

Pour définir des paramètres ponctuels pour effectuer une exportation VMware Workstation

1. Dans la page **Destination** de l'**Assistant Exportation**r, dans le menu déroulant **Restaurer vers une machine virtuelle**, sélectionnez **VMware Workstation**, puis cliquez sur **Suivant**.
2. Sur la page **Options de la machine virtuelle**, entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

Zone de texte	Description
Emplacement	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 les informations d'identification valides d'un compte enregistré sur la machine cible. Le compte doit être disposer des 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.
Nom de la machine virtuelle	Saisissez le nom de la la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4. REMARQUE : Le nom par défaut est le nom de la machine source.
Version	Spécifiez la version de VMware Workstation de la machine virtuelle. Vous pouvez choisir parmi les options suivantes : • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Mémoire	Spécifiez l'utilisation de la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Utiliser la même quantité de RAM que la machine source : pour spécifier que la configuration RAM est la même que pour la machine source. • Utiliser une quantité spécifique de RAM : pour spécifier la quantité de RAM à utiliser. Par exemple, 4 096 Megaoctets (Mo). La quantité minimale

Zone de texte	Description
	permise est 512 Mo et la quantité maximale est déterminée par la capacité et les limitations de la machine hôte. (recommandé)

3. Cliquez sur **Suivant**.
4. Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

   REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

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

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

1. Dans Core Console, effectuez l'une des opérations suivantes :
   - Sous l'onglet Disque de secours virtuel, cliquez sur **Ajouter** pour lancer l'**Assistant Exportation**. Sur la page **Machines protégées** de l'**Assistant Exportation**, sélectionnez la machine protégée à exporter, puis cliquez sur **Suivant**.
   - Accédez à la machine que vous souhaitez exporter, puis, dans l'onglet **Récapitulatif** dans le menu déroulant **Actions** de la machine, cliquez sur **Exporter → Disque de secours virtuel**.
2. Sur la page **Destination** de l'**Assistant Exportation**, cliquez sur **Restaurer dans une machine virtuelle → Poste de travail VMware.**
3. Cliquez sur **Suivant**.
4. Sur la page **Options de la machine virtuelle**, entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

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.
Machine virtuelle	Saisissez le nom de la la machine virtuelle à créer ; par exemple, VM-0A1B2C3D4. REMARQUE : Le nom par défaut est le nom de la machine source.

Zone de texte	Description
Version	Spécifiez la version de VMware Workstation de la machine virtuelle. Vous pouvez choisir parmi les options suivantes : • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Mémoire	Spécifiez la mémoire de la machine virtuelle en cliquant sur l'une des options suivantes : • Utiliser la même quantité de RAM que la machine source : pour spécifier que la configuration RAM est la même que pour la machine source. • Utiliser une quantité spécifique de RAM : pour spécifier la quantité de RAM à utiliser. Par exemple, 4 096 Megaoctets (Mo). La quantité minimale permise est 512 Mo et la quantité maximale est déterminée par la capacité et les limitations de la machine hôte.

5. Sélectionnez **Effectuer une exportation ad-hoc initiale** pour effectuer l'exportation immédiatement et non pas après le prochain instantané planifié.
6. Cliquez sur **Suivant**.
7. Sur la page **Volumes**, sélectionnez les volumes à exporter ; par exemple, C:\ et D: \. Cliquez sur **Suivant**.
8. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

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

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

Exécution d'une exportation Hyper-V ponctuelle

Pour effectuer une exportation Hyper-V ponctuelle

1. Dans la Core Console, accédez à la machine à exporter.
2. Dans l'onglet Récapitulatif, cliquez sur **Actions** → **Exporter** → **Une fois**.

   L'**Assistant Exportation** affiche la page **Machines protégées**.
3. Sélectionnez une machine pour l'exportation, puis cliquez sur **Suivant**.
4. Sur la page **Points de restauration**, sélectionnez le point de restauration à exporter, puis cliquez sur **Suivant**.

Définition de paramètres ponctuels pour effectuer une exportation Hyper-V

Pour définir des paramètres ponctuels pour effectuer une exportation Hyper-V

1. Dans la boîte de dialogue Hyper-V, cliquez sur **Utiliser la machine locale** pour effectuer l'exportation Hyper-V vers une machine local auquel le rôle Hyper-V est attribué.
2. Cliquez sur l'option **Hôte distant** pour indiquer que le serveur Hyper-V est situé sur une machine distante. Si vous avez sélectionné cette option, entrez les paramètres de l'hôte distant, comme suit :

Zone de texte	Description
Nom d'hôte	Entrez une adresse IP ou un nom d'hôte pour le serveur Hyper-V. Ceci représente l'adresse IP ou le nom d'hôte du serveur Hyper-V distant.
Port	Entrez un numéro de port pour la machine. Il représente le port par l'intermédiaire duquel le core communique avec cette machine.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'utilisateur doté de privilèges d'administration de la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe du compte d'utilisateur doté de privilèges d'administration sur la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.

3. Cliquez sur **Suivant**.
4. Sur la page **Options de machines virtuelles** dans la zone de texte **Emplacement de la machine VM**, entrez le chemin d'accès ou l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement VM doit disposer de suffisamment d'espace pour contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
5. Entrez le nom de la machine virtuelle dans la zone de texte **Nom de la machine virtuelle** .

   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
6. Sélectionnez l'une des options suivantes :
   - **Utiliser la même quantité de RAM que la machine source** pour spécifier que l'utilisation de RAM est identique pour la machine virtuelle et la machine source.
   - Cliquez sur **Utiliser une quantité de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo. (recommandé).
7. Pour spécifier le format de disque, en regard de **Format de disque**, cliquez sur l'une des options suivantes :
   - **VHDX**
   - **VHD**

   REMARQUE : Hyper-V Export prend en charge les formats de disque si la machine cible exécute Windows 8 (Windows Server 2012) ou une version supérieure. Si VHDX n'est pas pris en charge pour votre environnement, cette option est désactivée.
8. Sur la page **Volumes**, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une sauvegarde efficace de la machine protégée, incluez le lecteur d'amorçage de la machine protégée, par exemple : C:\.

   Les volumes sélectionnés ne doivent pas dépasser 2 040 Go pour le disque dur virtuel. Si les volumes sélectionnés dépassent 2 040 Go et que vous sélectionnez le format VHD, vous recevez un message d'erreur.
9. Sur la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

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

REMARQUE : Seules les configurations du DL1000 incluant 3 To d'espace avec 2 VM (machines virtuelles) prennent en charge l'exportation ponctuelle et l'exportation en continu (disque de secours virtuel).

Pour effectuer une exportation continue Hyper-V (disque de secours virtuel) :

1. dans Core Console, sur l'onglet **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l' **Assistant Exportation**. Sur la page **Machines protégées** de l'**Assistant Exportation**.
2. Sélectionnez la machine à exporter, puis cliquez sur **Suivant**.
3. Dans l'onglet **Récapitulatif**, cliquez sur **Exporter → Disque de secours virtuel**.
4. Dans la boîte de dialogue Hyper-V, cliquez sur **Utiliser la machine locale** pour effectuer l'exportation Hyper-V vers une machine local auquel le rôle Hyper-V est attribué.
5. Cliquez sur l'option **Hôte distant** pour indiquer que le serveur Hyper-V est situé sur une machine distante. Si vous avez sélectionné cette option, entrez les paramètres de l'hôte distant, comme suit :

Zone de texte	Description
Nom d'hôte	Entrez une adresse IP ou un nom d'hôte pour le serveur Hyper-V. Ceci représente l'adresse IP ou le nom d'hôte du serveur Hyper-V distant.
Port	Entrez un numéro de port pour la machine. Il représente le port par l'intermédiaire duquel le core communique avec cette machine.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'utilisateur doté de privilèges d'administration de la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.
Mot de passe	Entrez le mot de passe du compte d'utilisateur doté de privilèges d'administration sur la station de travail avec le serveur Hyper-V. Ce nom sert à spécifier les références de connexion de la machine virtuelle.

6. Sur la page **Options de machines virtuelles** dans la zone de texte **Emplacement de la machine VM**, entrez le chemin d'accès ou l'emplacement de la machine virtuelle. Par exemple, D:\export. L'emplacement VM doit disposer de suffisamment d'espace pour contenir les métadonnées de machine virtuelle et les disques virtuels requis pour la machine virtuelle.
7. Entrez le nom de la machine virtuelle dans la zone de texte **Nom de la machine virtuelle** .

   Le nom que vous saisissez apparaît dans la liste de machines virtuelles dans la console Hyper-V Manager.
8. Sélectionnez l'une des options suivantes :
   - **Utiliser la même quantité de RAM que la machine source** pour spécifier que l'utilisation de RAM est identique pour la machine virtuelle et la machine source.
   - Cliquez sur **Utiliser une quantité de RAM spécifique** pour spécifier la quantité de mémoire que la machine virtuelle doit posséder après l'exportation ; par exemple, 4 096 Mo (recommandé).
9. Pour spécifier la génération, cliquez sur l'une des options suivantes :
   - Génération 1 (recommandé)
   - Génération 2
10. Pour spécifier le format de disque, en regard de **Format de disque**, cliquez sur l'une des options suivantes :
    - **VHDX** (par défaut)
    - **VHD**

    REMARQUE : L'exportation Hyper-V prend en charge les formats de disque VHDX si la machine cible exécute Windows 8 (Windows Server 2012) ou version ultérieure. Si la VHDX n'est pas prise en charge pour votre environnement, cette option est désactivée. Sur la page Adaptateurs réseau, sélectionnez l'adaptateur virtuel à connecter à un commutateur.
11. Sur la page **Volumes**, sélectionnez le(s) volume(s) à exporter. Pour que la machine virtuelle offre une sauvegarde efficace de la machine protégée, incluez le lecteur d'amorçage de la machine protégée, par exemple : C:\.

Les volumes sélectionnés ne doivent pas dépasser 2 040 Go pour le disque dur virtuel. Si les volumes sélectionnés dépassent 2 040 Go et que vous sélectionnez le format VHD, vous recevez un message d'erreur.

12. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

    REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

Exportation des données Windows à l'aide d'une exportation Oracle VirtualBox

Dans AppAssure, vous pouvez choisir d'exporter les données à l'aide de VirtualBox Export en effectuant une exportation unique ou continue, ou par la mise en place d'une exportation en continu (pour les disques virtuels de secours).

Effectuez les étapes des procédures suivantes pour le type d'exportation appropriée.

REMARQUE : Pour que vous puissiez effectuer ce type d'exportation, Oracle VirtualBox doit être installé sur la machine Core. VirtualBox Version 4.2.18 ou ultérieure est pris en charge pour les hôtes Windows.

Exécution d'une exportation Oracle VirtualBox ponctuelle

Pour effectuer une exportation Oracle VirtualBox ponctuelle :

1. dans Core Console, accédez la machine Linux à exporter.
2. Sur l'onglet **Récapitulatif**, cliquez sur **Actions → Exportation → ponctuelle**.

   L'**Assistant Exportation** affiche la page **Machines protégées**.
3. Sélectionnez une machine pour l'exportation, puis cliquez sur **Suivant**.
4. Sur la page **Points de restauration**, sélectionnez le point de restauration à exporter, puis cliquez sur **Suivant**.
5. Sur la page **Destination** dans l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers une machine virtuelle**, sélectionnez **VirtualBox**, puis cliquez sur **Suivant**.
6. Sur la page **Options de la machine virtuelle**, sélectionnez **Machine Linux distante**.
7. Entrez les paramètres d'accès à la machine virtuelle, comme suit :

Zone de texte	Description
Nom d'hôte VirtualBox	Entrez une adresse IP ou un nom d'hôte pour le serveur VirtualBox. Ce champ représente l'adresse IP ou le nom d'hôte du serveur VirtualBox.
Port	Entrez un numéro de port pour la machine. Il représente le port par l'intermédiaire duquel le core communique avec cette machine.
Nom de la machine virtuelle	Spécifiez un chemin cible pour créer la machine virtuelle.
Nom d'utilisateur	Nom d'utilisateur du compte sur la machine cible, par exemple, root.
Mot de passe	Entrez les références de connexion de la machine hôte.
Mémoire	Spécifiez la mémoire de la machine virtuelle.

8. Dans la page **Volumes**, sélectionnez les volumes de données à exporter, puis cliquez sur **Suivant**.
9. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet Disque de secours virtuel ou Événements.

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

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

1. Dans la console Core, effectuez l'une des opérations suivantes :
   - Sous l'onglet **Disque de secours virtuel**, cliquez sur **Ajouter** pour lancer l'**Assistant Exportation**. Sur la page **Machines protégées** de l'**Assistant Exporter**, sélectionnez la machine protégée à exporter, puis cliquez sur **Suivant**.
   - Accédez à la machine à exporter, puis, dans l'onglet **Récapitulatif**, dans le menu déroulant **Actions** de la machine, cliquez sur **Exporter → Disque de secours virtuel**.
2. Sur la page **Destination** de l'**Assistant Exportation**, dans le menu déroulant **Restaurer vers la machine virtuelle**, sélectionnez **VirtualBox**, puis cliquez sur **Suivant**.
3. Sur la page **Options de la machine virtuelle**, sélectionnez **Utiliser une machine Windows.**
4. Entrez les paramètres d'accès à la machine virtuelle, décrits dans le tableau suivant.

Zone de texte	Description
Nom de la machine virtuelle	Entrez le nom de la machine virtuelle à créer. REMARQUE : Le nom par défaut est le nom de la machine source.
Chemin d'accès cible	Spécifiez un chemin cible local ou distant pour créer la machine virtuelle. REMARQUE : Le chemin d 'accès cible ne doit pas être un répertoire racine. Si vous spécifiez un chemin de partage réseau, vous devez entrer les informations d'identification valides (nom d'utilisateur et mot de passe) d'un compte enregistré dans la machine cible. Le compte doit avoir les autorisations en lecture et en écriture sur le partage réseau.
Mémoire	Spécifiez 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 Megaoctets (Mo). La quantité minimale permise est de 512 Mo et la quantité maximale est déterminée par la capacité et les limitations de la machine hôte.

5. Pour spécifier un compte d'utilisateur pour la machine virtuelle, sélectionnez **Spécifier le compte d'utilisateur sous lequel la machine virtuelle est exportée**, puis entrez les informations suivantes. Elles font référence à un compte d'utilisateur spécifique pour lequel la machine virtuelle sera enregistrée dans le cas où il existe plusieurs comptes utilisateur sur la machine virtuelle. Lorsque ce compte d'utilisateur est connecté, seul cet utilisateur voit la machine virtuelle dans le gestionnaire VirtualBox. Si aucun compte n'est spécifié, la machine virtuelle est enregistrée pour tous les utilisateurs existants sur la machine Windows avec VirtualBox.
   - Nom d'utilisateur : entrez le nom d'utilisateur pour lequel la machine virtuelle est enregistrée.
   - Mot de passe : entrez le mot de passe de ce compte d'utilisateur.
6. Sélectionnez **Effectuer une exportation ad-hoc initiale** pour effectuer l'exportation immédiatement au lieu d'attendre le prochain instantané planifié.

7. Cliquez sur **Suivant**.
8. Dans la page **Volumes** sélectionnez les volumes à exporter ; par exemple, C:\ et D:\, puis cliquez sur **Suivant**.
9. Dans la page **Récapitulatif**, cliquez sur **Terminer** pour fermer l'Assistant et démarrer l'exportation.

   REMARQUE : Vous pouvez surveiller le statut et l'avancement de l'exportation en affichant l'onglet **Disque de secours virtuel** ou **Événements** .

Restauration de volumes à partir d'un point de restauration

Vous pouvez restaurer les volumes sur une machine protégée à partir des points de récupération stockés dans AppAssure Core. Pour restaurer des volumes à partir d'un point de restauration :

1. dans Core Console, cliquez sur l'onglet **Machines**.

   L' **Assistant Restauration d'une machine** s'affiche.
2. Sur la page **Machines protégées**, sélectionnez la machine protégée dont vous souhaitez restaurer les données, puis cliquez sur **Suivant**.

   REMARQUE : La machine protégée doit être disposer du logiciel Agent et de points de récupération depuis lesquels vous allez exécuter l'opération de restauration.

   La page **Points de restauration** s'affiche.
3. Dans la liste des points de restauration, recherchez l'instantané à restaurer vers la machine agent.

   REMARQUE : Si nécessaire, utilisez les boutons de navigation dans le bas de la page pour afficher d'autres points de restauration. Ou bien, si vous voulez limiter le nombre de points de restauration affichés dans la page Points de restauration de l'Assistant, vous pouvez filtrer en fonction des volumes (si définis) ou de la date de création du point de restauration.
4. Cliquez sur n'importe quel point de restauration pour le sélectionner, puis sur **Suivant**.

   La page **Destination** s'affiche.
5. Dans la page **Destination** , sélectionnez la machine vers laquelle vous souhaitez restaurer les données comme suit :
   - si vous souhaitez restaurer les données à partir du point de restauration sélectionné vers la même machine agent (par exemple, la machine 1) et que les volumes à restaurer n'incluent pas le volume système, sélectionnez **Restaurer vers une machine protégée (uniquement les volumes non-système)**, vérifiez que la machine de destination (Machine 1) est sélectionnée, puis cliquez sur **Suivant**. La page **Adressage des volumes** s'affiche. Passez à l'étape 7.
   - Si vous souhaitez restaurer les données depuis le point de restauration sélectionné vers un autre ordinateur protégé (par exemple, remplacer le contenu de Machine 2 par les données de Machine 1), puis sélectionnez **Restaurer vers une machine protégée (uniquement des volumes non système)**, sélectionnez la machine de destination (par exemple, Machine 2) dans la liste, puis cliquez sur **Suivant**. La page **Adressage des volumes** s'affiche. Passez à l'étape 7.
   - Si vous souhaitez effectuer la restauration à partir du point de restauration sélectionné vers la même machine ou une machine différente à l'aide d'un CD d'amorçage et que les volumes à restaurer n'incluent pas le volume système, sélectionnez **Restaurer vers n'importe quelle machine cible en utilisant un CD d'amorçage** .
   - Pour continuer et créer le CD d'amorçage avec les informations du point de restauration sélectionné, cliquez sur **Suivant** et passez à l'étape 10.
   - Si vous avez déjà créé le CD d'amorçage et que la machine cible a été démarrée en utilisant le CD d'amorçage, passez à l'étape 17.
   - Si vous souhaitez effectuer une restauration à partir d'un point de restauration vers un volume système (par exemple, le lecteur C de la machine agent Machine 1), vous devez effectuer une

restauration BMR. Pour plus d'informations sur l'exécution d'une restauration BMR pour Windows, voir Lancement d'une restauration sans système d'exploitation (BMR) pour les machines Windows.

- Pour plus d'informations sur l'exécution d'une restauration BMR pour Linux, reportez-vous à la feuille de route d'exécution d'une restauration BMR pour les machines Linux Lancement d'une restauration BMR pour une machine Linux.

6. Pour vous connecter à la console URC (Universal Recovery Console) sur la machine cible, procédez comme suit :
   a. sélectionnez **J'ai déjà un CD d'amorçage s'exécutant sur la machine cible**.
   b. Dans la zone de texte Adresse IP, entrez l'adresse IP de la machine cible avec le CD d'amorçage.
   c. Dans la zone de texte Clé d'authentification, entrez la clé d'authentification depuis la console URC sur la machine cible, puis cliquez sur **Suivant**.

   La page **Affectation de disques** s'affiche. Passez à l'étape 20.
7. Sur la page **Mappage des volumes**, pour chaque volume dans le point de restauration à restaurer, sélectionnez le volume de destination. Si vous ne souhaitez pas restaurer un volume, dans la colonne Volumes, sélectionnez **Ne pas restaurer**.
8. Sélectionnez **Afficher les options avancées**, puis procédez comme suit :
   - pour restaurer vers des machines Windows, si vous souhaitez utiliser **Live Recovery**.

     En utilisant la technologie de restauration instantanée Live Recovery, vous pouvez récupérer ou restaurer immédiatement des données vers des machines physiques ou virtuelles à partir des points de restauration stockés des machines Windows, ce qui inclut les espaces de stockage Microsoft Windows. Live Recovery n'est pas disponible pour les machines Linux.
   - Si vous souhaitez forcer le démontage, sélectionnez **Forcer le démontage**.

     Si vous ne forcez pas le démontage avant la restauration des données, la restauration peut échouer avec une erreur indiquant que le volume est cours d'utilisation.
9. Passez à l'étape 20.
10. Sur la page CD d'amorçage, effectuez les opérations suivantes :
    a. dans le champ de texte **Chemin de sortie**, tapez le chemin de l'emplacement de destination du stockage de l'image ISO de CD,
    b. Sous **Environnement**, sélectionnez l'architecture la mieux adaptée au matériel que vous restaurez :
       - pour restaurer sur une machine Windows dotée d'une architecture 64 bits, sélectionnez **Windows 8 64 bits**.
       - Pour restaurer sur une machine dotée d'une architecture 32 bits (x86), sélectionnez **Windows 7 32 bits**.
11. Le cas échéant, pour définir les paramètres réseau de l'agent restauré ou utiliser UltraVNC, sélectionnez **Afficher les options avancées** et effectuez l'une des opérations suivantes :
    - Pour établir une connexion réseau pour la machine restaurée, sélectionnez **Utiliser l'adresse IP suivante**, comme décrit dans le tableau suivant.

Option	Description
Adresse IP :	Spécifiez une adresse IP ou un nom d'hôte pour la machine restaurée.
Masque de sous-réseau	Indiquez le masque de sous-réseau de la machine restaurée.
Passerelle par défaut	Indiquez la passerelle par défaut de la machine restaurée.

Option	Description
Serveur DNS	Spécifiez le serveur de noms de domaine de la machine restaurée.

- Pour définir les informations UltraVNC, sélectionnez **Ajouter UltraVNC** tel que décrit dans le tableau suivant. Utilisez cette option si vous avez besoin d'un accès à distance à la console de restauration. Vous ne pouvez pas vous connecter à l'aide de Microsoft Terminal Services pendant l'utilisation du CD d'amorçage.

Option	Description
Mot de passe	Spécifiez le mot de passe de la connexion UltraVNC.
Port	Spécifiez le port de la connexion UltraVNC. Le port par défaut est 5900.

12. Cliquez sur **Suivant**.
13. Pour injecter un pilote, procédez comme suit :
    a. sélectionnez **Ajouter une archive de pilotes**.
    b. Accédez à un fichier ZIP contenant l'archive, sélectionnez le fichier ZIP, puis cliquez sur **Ouvrir**. L'archive est envoyée et s'affiche dans la page d'injection de pilote.
    c. Cliquez sur **Suivant**.
14. Sur la page Image ISO figure le statut pendant la création de l'image ISO du CD d'amorçage. Lorsque le CD de d'amorçage aboutit, cliquez sur **Suivant**.

    La page **de connexion** s'affiche.
15. Démarrez la machine agent pour laquelle vous souhaitez restaurer les données depuis le CD d'amorçage.
    - Démarrez la machine agent à partir d'une image ISO, si possible.
    - Autrement, copiez l'image ISO vers des supports physiques (CD ou DVD), chargez le disque dans la machine agent, configurez la machine pour qu'elle se charge depuis le CD d'amorçage, puis redémarrez depuis le CD d'amorçage.

    REMARQUE : Il peut être nécessaire de changer les paramètres du BIOS de la machine agent pour vous assurer que le volume qui se charge en premier est le CD d'amorçage.

    La machine agent, lorsqu'elle est démarrée depuis le CD d'amorçage affiche l'interface URC (Universal Recovery Console). Cet environnement est utilisé pour restaurer le lecteur système ou les volumes sélectionnés directement depuis AppAssure Core. Notez l'adresse IP et les informations de clé d'authentification dans la console URC sont actualisées chaque fois que vous démarrez à partir du CD d'amorçage.
16. Dans la console Core Console, sur la page **Connexion**, entrez les informations d'authentification de l'instance URC de la machine à restaurer, comme suit :
    a. dans la zone de texte Adresse IP, entrez l'adresse IP de la machine sur laquelle vous effectuez la restauration à partir d'un point de restauration.
    b. Dans la zone de texte Clé d'authentification, entrez les informations de la console URC.
    c. Cliquez sur **Suivant**.

    La page **Adressage de disques** s'affiche.
17. Pour adresser des volumes manuellement, passez à l'étape 18. Pour adresser automatiquement des volumes, procédez comme suit :
    a. sélectionnez **Adressage automatique des volumes**.
    b. Dans la zone de **Adressage automatique des volumes**, sélectionnez les volumes à restaurer. Si vous ne souhaitez pas restaurer un volume répertorié, désélectionnez l'option.

    REMARQUE : Au moins un volume doit être sélectionné afin d'effectuer la restauration.

c. Sélectionnez le disque de destination de la restauration.
d. Cliquez sur **Suivant**, puis passez à l'étape 19.

18. Si vous souhaitez adresser les volumes manuellement, procédez comme suit :
    a. sélectionnez **Adressage manuel des volumes**.
    b. Dans la zone de **Adressage manuel des volumes**, dans la liste déroulante **des volumes de destination** de chaque volume, sélectionnez le volume à restaurer. Si vous ne souhaitez pas restaurer un volume répertorié, désélectionnez l'option.

       REMARQUE : Au moins un volume doit être sélectionné afin d'effectuer la restauration.

    c. Cliquez sur **Terminer**.

       PRÉCAUTION : Si vous sélectionnez Terminer, toutes les partitions et données existantes sur le 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.

    L' **Assistant Restauration d'une machine** se ferme et les données sont restaurées depuis les volumes sélectionnés du point de restauration de la machine cible. Passez à l'étape 22.

19. Dans la page **Aperçu de l'adressage de disques**, vérifiez les paramètres des actions de restauration que vous avez sélectionnées. Pour effectuer la restauration, cliquez sur **Terminer**.

    PRÉCAUTION : Si vous sélectionnez Terminer, toutes les partitions et données existantes sur le 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.

    L' **assistant Restaurer une machine** se ferme et les données sont restaurées depuis les volumes sélectionnés du point de restauration de la machine cible. Passez à l'étape 22.

20. Si les volumes à restaurer contiennent des bases de données SQL ou Microsoft Exchange, sur la page **Démonter les bases de données**, un message demande de démonter ces bases de données. Si vous souhaitez remonter ces bases de données une fois la restauration terminée, sélectionnez **Remonter automatiquement toutes les bases de données après la restauration du point de restauration**. Cliquez sur **Terminer**.
21. Cliquez sur **OK** pour confirmer le message de statut indiquant que le processus de restauration a commencé.
22. Pour surveiller l'avancement de l'action de restauration, dans Core Console, cliquez sur **Événements**.

Restauration des volumes d'une machine Linux à l'aide de la ligne de commande

Dans AppAssure, vous pouvez restaurer les volumes sur les machines Linux protégées en utilisant l'utilitaire de ligne de commande `aamount`. Pour restaurer les volumes d'une machine Linux à l'aide de la ligne de commande :

PRÉCAUTION : Vous ne devez pas tenter de restaurer le volume système ou root (/).

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. Entrez la commande suivante pour lister les points de restauration actuellement montés de la machine spécifiée :

   `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`.

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`.

Lancement d'une restauration sans système d'exploitation (BMR) pour des machines Windows

AppAssure 5 permet d'effectuer une restauration sans système d'exploitation (BMR) pour les machines Windows que le matériel soit similaire ou non. Ce processus consiste à créer une image de CD d'amorçage, graver l'image sur un disque, amorcer le serveur cible à partir du disque, se connecter l'instance de console de restauration, mapper les volumes, initialiser la restauration, puis surveiller le processus. À la fin de la restauration BMR, vous pouvez poursuivre en exécutant la tâche de chargement

du système d'exploitation et des applications logicielles sur le serveur restauré, puis des paramètres et de la configuration uniques.

Vous pouvez aussi choisir d'effectuer une restauration sans système d'exploitation dans le cadre d'une mise à niveau matérielle ou d'un remplacement de serveur.

La fonctionnalité BMR est aussi prise en charge par les machines Linux protégées à l'aide de l'utilitaire de ligne de commande `aamount`. Pour en savoir plus, reportez-vous à Lancement d'une restauration BMR pour une machine Linux.

Stratégie d'exécution d'une restauration complète (BMR) d'une machine Windows

Pour effectuer une BMR d'un ordinateur Windows :

1. Créez un CD d'amorçage.
2. Gravez l'image sur le disque.
3. Amorcez le serveur cible depuis le CD d'amorçage.
4. Connectez-vous au disque de restauration.
5. Mappez les volumes.
6. Lancez la restauration.
7. Surveillez l'avancement.

Création d'un CD d'image ISO amorçable

Pour exécuter une restauration BMR d'une machine Windows, vous devez créer une image CD/ISO amorçable dans Core Console, qui contient l'interface AppAssure Universal Recovery Console. Cette console est un environnement qui permet de restaurer le lecteur système ou l'ensemble du serveur directement depuis AppAssure Core.

L'image ISO que vous créez est adaptée à la machine que vous restaurez ; par conséquent, elle doit contenir les pilotes de réseau et de stockage de masse corrects. Si vous prévoyez d'effectuer la restauration sur un matériel différent de celui de la machine où vous créez le CD d'amorçage, vous devez inclure le contrôleur de stockage et d'autres pilotes sur le CD d'amorçage.

REMARQUE : L'ISO (International Organization for Standardization) est un organisme international réunissant des représentants de différentes organisations nationales, qui détermine et définit les normes des systèmes de fichiers. La norme ISO 9660 est une norme de système de fichiers utilisée pour les supports de disque optique pour l'échange de données. Elle prend en charge divers systèmes d'exploitation, notamment Windows. Une image ISO est un fichier d'archive ou une image de disque qui contient des données pour chaque secteur du disque, ainsi que pour le système de fichiers du disque.

Pour créer une image ISO de CD amorçable :

1. Dans Core Console où se trouve le serveur à restaurer, sélectionnez le **Core**, puis cliquez sur l'onglet **Outils**.
2. Cliquez sur **CD d'amorçage**.
3. Sélectionnez **Actions**, puis cliquez sur **Créer une image ISO d'amorçage**.

   La boîte de dialogue **Créer un CD d'amorçage** s'affiche. Pour remplir les champs de cette boîte de dialogue, appliquez les procédures suivantes.

Attribution d'un nom au fichier de CD d'amorçage et définition du chemin

Pour nommer le CD d'amorçage et configurer le chemin :

Dans la boîte de dialogue **Créer un CD d'amorçage**, entrez le chemin ISO où l'image d'amorçage sera stockée sur le serveur core.

Si le partage sur lequel vous souhaitez stocker l'image manque de l'espace de disque, vous pouvez définir le chemin au besoin ; par exemple, D:\nomdufichier.iso.

REMARQUE : L'extension de fichier doit être .iso. Lorsque vous spécifiez ce chemin, utilisez uniquement des caractères alphanumériques, des tirets ou des points (uniquement pour séparer les noms d'hôtes et les domaines). Les lettres a à z ne sont pas sensibles à la casse. N'utilisez aucun espace. Aucun autre symbole ou caractère de ponctuation n'est admis.

Création de connexions

Pour créer des connexions :

1. Sous **Options de connexion**, effectuez l'une des opérations suivantes :
   - Pour obtenir dynamiquement l'adresse IP avec le protocole DHCP (Dynamic Host Configuration Protocol, protocole de configuration dynamique de l'hôte), sélectionnez **Obtenir automatiquement l'adresse IP**.
   - (Facultatif) Pour spécifier une adresse IP statique pour la console de restauration, sélectionnez **Utiliser l'adresse IP suivante**, puis entrez l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le serveur DNS dans les champs prévus à cet effet. Vous devez remplir tous ces champs.
2. Si nécessaire, sous **Options UltraVNC**, sélectionnez **Ajouter UltraVNC** et entrez les options appropriées. Les paramètres UltraVNC vous permettent de gérer la console de restauration à distance lorsqu'elle est en cours d'exécution.

   REMARQUE : Cette étape est facultative. Si vous avez besoin d'un accès à distance à la console de restauration, vous devez configurer et utiliser UltraVNC. Vous ne pouvez pas vous connecter à l'aide des services de terminal Microsoft lorsque vous utilisez le CD d'amorçage.

Insertion de pilotes dans le CD d'amorçage

L'insertion de pilotes est utilisée pour faciliter les opérations entre la console de restauration, la carte réseau et le stockage sur le serveur cible.

Si vous prévoyez de restaurer les données sur un matériel différent, vous devez injecter les pilotes de contrôleur de stockage, de RAID, d'AHCI, de jeu de puces et autres dans le CD d'amorçage. Ces pilotes permettent au système d'exploitation de détecter et de faire fonctionner les périphériques avec succès.

REMARQUE : N'oubliez pas que le CD d'amorçage contient automatiquement les pilotes Windows 7 PE 32 bits.

Pour insérer des pilotes dans un CD d'amorçage

1. Téléchargez les pilotes pour le serveur depuis le site Web du fabricant, puis décompressez-les.
2. Compressez le dossier qui contient les pilotes, à l'aide d'un utilitaire de compression tel que WinZip.
3. Dans la boîte de dialogue **Créer un CD d'amorçage**, accédez au panneau **Pilotes** et cliquez sur **Ajouter un pilote**.
4. Pour trouver le fichier de pilote compressé, naviguez dans le système de fichiers. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

   Les pilotes insérés apparaissent en surbrillance dans le volet **Pilotes**.

Création du CD d'amorçage

Pour créer un CD d'amorçage, vous devez, après avoir nommé le CD d'amorçage et spécifié le chemin, créé une connexion et (facultatif) injecté les pilotes, ouvrir l'écran **Créer un CD d'amorçage** et cliquer sur **Créer un CD d'amorçage**. L'image ISO est créée.

Affichage de l'avancement de la création de l'image ISO

Pour afficher l'avancement de la création de l'image ISO, sélectionnez l'onglet **Événements**, puis **Tâches**.

REMARQUE : Vous pouvez également afficher l'avancement de la création de l'image ISO image dans la boîte de dialogue **Surveiller la tâche active**.

Lorsque la création de l'image ISO est terminée, cette image apparaît dans la page **CD d'amorçage**, accessible depuis le menu **Outils**.

Accès à l'image ISO

Pour accéder à l'image ISO, naviguez jusqu'au chemin de sortie que vous avez indiqué ou cliquez sur le lien pour télécharger l'image à un emplacement à partir duquel vous pourrez la charger sur le nouveau système, par exemple, un lecteur de réseau.

Chargement d'un CD d'amorçage

Après avoir créé l'image du CD d'amorçage, amorcez le serveur cible avec le CD d'amorçage nouvellement créé.

REMARQUE : Si vous avez créé le CD d'amorçage avec DHCP, notez l'adresse IP et le mot de passe.

Pour charger un CD d'amorçage :

1. Naviguez jusqu'au nouveau serveur, chargez le CD d'amorçage, puis démarrez la machine.
2. Activez l'option **Amorcer à partir du CD-ROM**, qui charge les éléments suivants :
   - Windows 7 PE
   - Logiciel AppAssure Agent

   La console AppAssure Universal Recovery démarre, et affiche l'adresse IP et le mot de passe d'authentification de la machine.
3. Prenez note de l'adresse IP qui s'affiche dans le panneau des paramètres d'adaptateur réseau, ainsi que du mot de passe d'authentification affiché dans le panneau Authentification. Vous utiliserez ces informations ultérieurement au cours du processus de restauration des données, pour vous reconnecter à la console.
4. Pour modifier l'adresse IP, sélectionnez-la et cliquez sur **Modifier**.

   REMARQUE : Si vous avez spécifié une adresse IP dans la boîte de dialogue Créer un CD d'amorçage, la console Universal Recovery l'utilise et l'affiche dans l'écran **Paramètres d'adaptateur réseau**.

Injection de pilotes sur votre serveur cible

Si vous restaurez les données sur un matériel différent, vous devez injecter les pilotes de contrôleur de stockage, de RAID, d'AHCI, de jeu de puces et autres dans le CD d'amorçage s'ils n'y figurent pas. Ces pilotes permettent au système d'exploitation de faire fonctionner avec succès tous les périphériques du serveur cible.

Si vous n'êtes pas certain des pilotes dont votre serveur cible a besoin, cliquez sur l'onglet Infos système dans la console Universal Recovery. Cet onglet affiche tout le matériel système et tous les types de périphérique du serveur cible sur lequel vous souhaitez restaurer les données.

REMARQUE : N'oubliez pas que votre serveur cible contient automatiquement les pilotes Windows 7 PE 32 bits.

Pour injecter des pilotes dans votre serveur cible :

1. Téléchargez les pilotes pour le serveur depuis le site Web du fabricant, puis décompressez-les.
2. Compressez le dossier qui contient les pilotes, à l'aide d'un utilitaire de compression tel que WinZip, puis copiez-le vers le serveur cible.
3. Dans la console Universal Recovery, cliquez sur **Injection de pilotes**.
4. Pour trouver le fichier de pilote compressé, naviguez dans le système de fichiers et sélectionnez le fichier.
5. Si vous avez cliqué sur **Injection de pilotes** à l'étape 3, cliquez sur **Ajouter un pilote**. Si vous avez choisi **Charger un pilote** à l'étape 3, cliquez sur **Ouvrir**.

   Les pilotes sélectionnés sont injectés ; ils sont chargés dans le système d'exploitation lorsque vous redémarrez le serveur cible.

Lancement d'une restauration à partir d'AppAssure Core

Pour lancer une restauration à partir d'AppAssure Core

1. Si les cartes réseau qui figurent sur tout système en cours de restauration sont associées (liées), retirez tous les câbles, à l'exception d'un d'entre eux.

   REMARQUE : AppAssure Restore ne reconnaît pas les cartes réseau associées. En présence de plus d'une connexion, le processus ne peut pas savoir quel carte réseau utiliser.
2. Accédez au serveur Core, puis ouvrez Core Console.
3. Dans l'onglet **Machines**, sélectionnez l'ordinateur à partir duquel vous souhaitez restaurer les données.
4. Cliquez sur le menu **Actions** de l'ordinateur, puis sélectionnez **Points de restauration** pour afficher la liste de tous les points de restauration de cet ordinateur.
5. Développez le point de restauration à partir duquel vous souhaitez effectuer la restauration, puis cliquez sur **Restaurer**.
6. Dans la boîte de dialogue **Restaurer**, sous Choisir une **destination**, sélectionnez **Instance Recovery Console**.
7. Dans les champs **Hôte** et **Mot de passe**, entrez l'adresse IP et le mot de passe d'authentification du nouveau serveur sur lequel vous restaurerez les données.

   REMARQUE : Les valeurs Hôte et Mot de passe sont les références que vous avez enregistrées au cours de la tâche précédente. Pour en savoir plus, voir .
8. Cliquez sur **Charger les volumes** pour charger les volumes cibles sur le nouvel ordinateur.

Mappage/adressage de volumes

Vous pouvez choisir d'adresser des volumes sur les disques du serveur cible automatiquement ou manuellement. Pour l'alignement automatique des disques, le disque est nettoyé et repartitionné, et toutes les données sont supprimées. L'alignement est réalisé dans l'ordre où les volumes sont répertoriés, puis les volumes sont alloués aux disques de manière appropriée, en fonction de la taille, etc. Plusieurs volumes peuvent utiliser un même disque. Si vous adressez manuellement les lecteurs, vous ne pouvez pas utiliser deux fois le même disque.

Pour l’adressage manuel, vous devez avoir formaté la machine correctement avant de la restaurer.

Pour adresser les volumes :

1. Pour adresser automatiquement des volumes, procédez comme suit :
   a. Dans la page **Adressage de disques** de l'**Assistant Restaurration d'une machine**, 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 **Restaurer**, puis passez à l'étape 3.
2. Pour adresser manuellement des volumes, procédez comme suit :
   a. Dans la page **Adressage des disques** de l'**Assistant Restauration d'une machine**, 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)**.

   PRÉCAUTION : Si vous sélectionnez Démarrer le cumul (rollback), toutes les partitions et données existantes du lecteur cible sont définitivement supprimées, puis remplacées par le contenu du point de restauration sélectionné, y compris le système d'exploitation et toutes les données.

Affichage de l'avancement de la restauration

Pour afficher l'avancement de la restauration :

1. Une fois que vous avez lancé le processus de restauration (rollback), la boîte de dialogue **Tâche active** s'affiche et montre que l'action de restauration (rollback) a été démarrée.

   REMARQUE : Cet affichage de la boîte de dialogue **Tâche active** n'indique pas que la tâche s'est achevée avec succès.
2. (Facultatif) Pour surveiller l'avancement de la tâche de restauration (rollback), ouvrez la boîte de dialogue Tâche active et cliquez sur **Ouvrir la fenêtre de surveillance**. Vous pouvez affiche l'état de la restauration, ainsi que l'heure de début et de fin, dans la fenêtre **Surveiller la tâche ouverte**.

   REMARQUE : Pour revenir aux points de restauration correspondant à la machine source depuis la boîte dialogue **Tâche active**, cliquez sur **Fermer**.

Démarrage du serveur cible restauré

Pour démarrer le serveur cible restauré :

1. Naviguez pour revenir au serveur cible, puis, dans l'interface de la **console AppAssure Universal Recovery**, cliquez sur **Redémarrer** pour démarrer la machine.
2. Spécifiez que Windows doit démarrer normalement.
3. Connectez-vous à la machine.

   Le système est restauré à son état tel qu'il était avant la restauration sans système d'exploitation.

Réparation des problèmes de démarrage

Notez que si vous avez restauré les données sur un matériel différent, vous devez avoir injecté les pilotes de contrôleur de stockage, RAID, AHCI, de jeu de puces et d'autres pilotes s'ils n'y figurent pas sur le CD d'amorçage. Ces pilotes permettent au système d'exploitation de faire fonctionner tous les périphériques du serveur cible.

Pour réparer les problèmes de démarrage :

1. Si vous rencontrez des difficultés lors du démarrage du serveur cible restauré, ouvrez la console Universal Recovery en rechargeant le CD d'amorçage.
2. Dans la console Universal Recovery, cliquez sur **Injection de pilotes**.
3. Dans la boîte de dialogue Injection de pilotes, cliquez sur **Reparer les problèmes d'amorçage**.

   Les paramètres de démarrage figurant dans l'enregistrement de serveur cible sont automatiquement réparés.
4. Dans la console Universal Recovery, cliquez sur **Redémarrer**.

Exécution d'une restauration sans système d'exploitation (BMR) pour une machine Linux

Le système DL1000 peut exécuter une restauration BMR pour une machine Linux, y compris la restauration du volume système. À l'aide de l'utilitaire de ligne de commande AppAssure, `aamount`, effectuez la restauration de l'image de base du volume d'amorçage. Avant toute restauration BMR, vous devez effectuer les opérations suivantes :

- Obtenir un fichier Live CD BMR auprès du service de support AppAssure ; ce fichier inclut une version amorçable de Linux.

  REMARQUE : Vous pouvez également télécharger le fichier Live CD Linux depuis le portail de licences, à l'adresse **https://licenseportal.com**.
- Assurez-vous que l'espace sur le disque dur est suffisant pour créer les partitions de destination sur la machine cible et pour y stocker les volumes source. Chaque partition de destination doit être au moins aussi volumineuse que la partition source d'origine.
- Identifiez le chemin de restauration (rollback), c'est-à-dire le chemin du descripteur de fichier du périphérique. Pour identifier ce chemin, utilisez la commande `fdisk` à partir d'une fenêtre de terminal.

  REMARQUE : Avant de commencer à utiliser les commandes AppAssure, vous pouvez installer 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 effectuer la restauration sans système d'exploitation d'une machine Linux :

1. À l'aide du fichier Live CD que vous avez reçu d'AppAssure, démarrez la machine Linux et ouvrez une fenêtre de terminal.
2. Si nécessaire, créez une nouvelle partition de disque, par exemple en exécutant la commande `fdisk` en tant qu'utilisateur root, puis rendez cette partition amorçable en utilisant la commande `a`.
3. Exécutez l'utilitaire `aamount` d'AppAssure comme root, par exemple :

   ```
   sudo aamount
   ```
4. En réponse à l'invite de montage d'AppAssure, entrez la commande suivante pour répertorier les machines protégées :

   ```
   lm
   ```
5. Lorsque vous y êtes invité, entrez l'adresse IP ou le nom d'hôte de votre serveur AppAssure Core.

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

   La liste qui s'affiche indique les machines protégées par ce serveur AppAssure Core. Elle répertorie les machines trouvées en affichant le numéro d'article, l'adresse IP/nom d'hôte et l'ID de machine (par exemple : `293cc667-44b4-48ab-91d8-44bc74252a4f`).

7. Pour répertorier les points de restauration récemment montés pour la machine à restaurer, entrez la commande suivante :

   `lr <machine_line_item_number>`

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

   La liste qui s'affiche indique les points de restauration de base et incrémentiels de cette machine. Cette liste inclut un numéro d'article figurant sur une ligne, l'horodatage/date, l'emplacement du volume, la taille de point de restauration et un numéro d'ID de volume comprenant en dernier lieu un numéro de séquence (par exemple, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), qui identifie le point de restauration.

8. Pour sélectionner le point de restauration d'image de base à restaurer (rollback), entrez la commande suivante :

   `r <volume_base_image_recovery_point_ID_number> <path>`

   PRÉCAUTION : Vous devez vous assurer que le volume système n'est pas monté.

   Cette commande entraîne la restauration (rollback) de l'image de volume spécifiée par l'ID entré, du core vers le chemin d'accès spécifié. Le chemin de restauration (rollback) est celui du descripteur de fichier de périphérique et non celui du répertoire dans lequel il est monté.

   REMARQUE : Pour identifier le point de restauration, vous pouvez également indiquer un numéro de ligne dans la commande au lieu du numéro d'ID du point de restauration. Dans ce cas, utilisez le numéro de ligne de l'agent/la machine (à partir de la sortie lm), suivi du numéro de ligne du point de restauration et de la lettre du volume, puis du chemin d'accès, par exemple,**r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. Dans cette commande, `<path>` est le descripteur de fichier du volume réel.

9. Lorsque vous êtes invité à continuer, entrez `y` pour Yes (o pour Oui).

   Une série de messages s'affiche au cours de la restauration pour vous informer de l'état.

10. Une fois la restauration réussie, le cas échéant, mettez à jour l'enregistrement d'amorçage principal à l'aide du chargeur de démarrage.

    REMARQUE : Il n'est nécessaire de réparer ou configurer le chargeur de démarrage que si ce disque est nouveau. S'il s'agit d'une simple restauration vers le même disque, il n'est pas nécessaire de configurer le chargeur de démarrage.

    PRÉCAUTION : Ne démontez pas manuellement un volume Linux protégé. Si vous devez le faire, veillez à exécuter la commande suivante avant de démonter le volume : bsctl -d <path to volume>.

    Dans cette commande, `<path to volume>` (chemin d'accès au volume) ne désigne pas le point de montage du volume mais le descripteur de fichier du volume ; il doit se présenter sous une forme similaire à la suivante : **/dev/sda1**.

Installation de l'utilitaire d'écran

Avant de commencer à utiliser les commandes AppAssure, vous pouvez installer l'utilitaire d'écran. Il vous permet de faire défiler l'écran pour afficher de plus grandes quantités de données, comme la liste des points de restauration.

Pour installer l'utilitaire d'écran :

1. Utilisez le fichier Live CD pour démarrer la machine Linux.

   Une fenêtre de terminal s'ouvre.
2. Entrez la commande suivante : `sudo apt-get install screen`
3. Pour démarrer l'utilitaire d'écran, entrez `screen` à l'invite de commande.

Création de partitions amorçables sur une machine Linux

Pour créer des partitions amorçables sur une machine Linux à l'aide de la ligne de commande :

1. Rattachez tous les périphériques à l'aide de l'utilitaire **bsctl** en exécutant la commande suivante en tant qu'utilisateur root : `sudo bsctl --attach-to-device /dev/<restored volume>`

   REMARQUE : Répétez cette étape pour chaque volume restauré.
2. Montez chaque volume restauré à l'aide des commandes suivantes :

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   REMARQUE : Certaines configurations système peuvent inclure le répertoire d'amorçage comme élément du volume racine.
3. Montez les métadonnées d'instantané de chaque volume restauré à l'aide des commandes suivantes :

   ```
   sudo bsctl --reset-bitmap-store /dev/<restored volume>

   sudo bsctl --map-bitmap-store /dev/<restored volume>
   ```
4. Vérifiez que l'UUID (Universally Unique Identifier, ID universel unique) contient bien les nouveaux volumes, à l'aide de la commande `blkid` ou de la commande `ll /dev/disk/by-uuid`.
5. Vérifiez que le dossier `/etc/fstab` contient les UUID corrects pour le volume racine et le volume d'amorçage.
6. Installez GRUB (Grand Unified Bootloader, grand chargeur d'amorçage unifié) à l'aide des commandes suivantes :

   ```
   mount --bind /dev/ /mnt/dev

   mount --bind /proc/ /mnt/proc

   chroot/mnt/bin/bash

   grub-install/dev/sda
   ```
7. Vérifiez que le fichier **/boot/grub/grub.conf** contient l'UUID correct pour le volume racine ou mettez-le à niveau selon vos besoins à l'aide d'un éditeur de texte.
8. Retirez le disque Live CD du lecteur de CD-ROM et redémarrez la machine Linux.

5

Réplication de points de restauration

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.

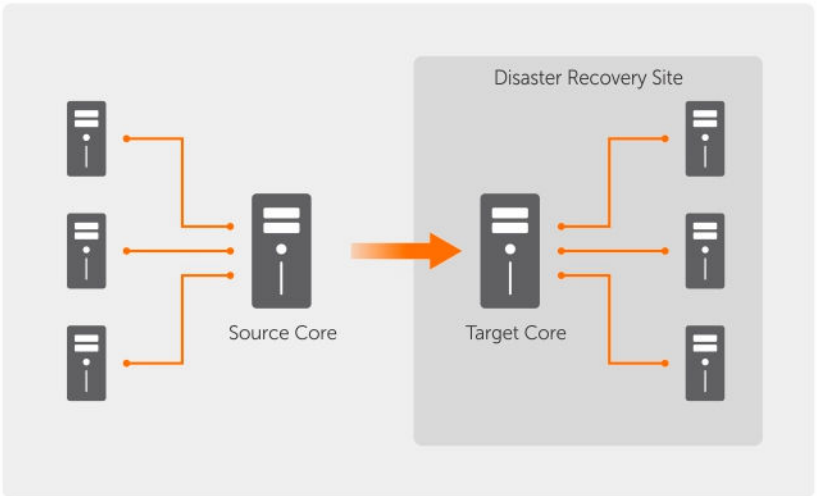

Figure 5. Architecture de réplication de base

La réplication commence par l'amorçage, à savoir le transfert initial des images de base dédupliquées et des instantanés incrémentiels des agents protégés ; cela peut représenter des centaines ou des milliers de gigaoctets de données. La réplication initiale peut être amorcée vers le core cible en utilisant un support externe. En général, cela s'avère utile pour les ensembles de données volumineux ou les sites avec des liaisons lentes. Les données dans une archive d'amorçage 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 répartie sur plusieurs périphériques, selon l'espace disponible sur le support. Pendant le processus d'amorçage, les points de restauration incrémentiels sont répliqués vers le site cible. Une fois

que le core cible a consommé l'archive d'amorçage, les nouveaux points de restauration incrémentiels répliqués se synchronisent automatiquement.

Schéma d'exécution d'une réplication

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

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

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

Réplication vers un core autogéré

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

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

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

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

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

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

Zone de texte	Description
Nom d'hôte	Entrez le nom d'hôte ou l'adresse IP de la machine core vers lequel vous souhaitez répliquer.
Port	Entrez le numéro de port sur lequel AppAssure Core communique avec la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Entrez le nom d'utilisateur pour accéder à la machine ; par exemple, **Administrateur.**
Mot de passe	Entrez le mot de passe d'accès à la machine.

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

a. sélectionnez **Utiliser un core cible existant**.
b. Sélectionnez le core cible dans la liste déroulante.
c. Cliquez sur **Suivant**.
d. Passez à l'étape 7.

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

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

   a. Sur la page **Agents**, sélectionnez **Utiliser un lecteur de départ pour effectuer un transfert initial**. Si un ou plusieurs agents répliquent vers un core cible , vous pouvez inclure ces machines protégées dans le lecteur source, en sélectionnant **Avec déjà répliqué**.
   b. Cliquez sur **Suivant**.
   c. Sur la page **Emplacement du lecteur de départ**, utilisez la liste déroulante **Type d'emplacement** pour sélectionner l'une des options suivantes :
      - Local : dans la zone de texte **Emplacement**, entrez l'emplacement dans lequel AppAssure doit enregistrer le lecteur source ; par exemple, D :\work\archive.
      - Réseau : dans la zone de texte **Emplacement**, entrez l'emplacement dans lequel AppAssure doit enregistrer le lecteur de source, puis entrez vos informations d'identification pour le partage réseau dans les zones de texte **Nom d'utilisateur** et **Mot de passe**.
      - Cloud : Dans la zone de texte **du compte** , sélectionnez le compte. Pour sélectionner un compte Cloud, vous devez, en premier lieu, avoir ajouté dans la Core Console. Pour en savoir plus, reportez-vous à la section Ajout d'un Compte Cloud. Sélectionnez le **conteneur** associé à votre compte. Sélectionnez le **Nom du dossier** vers lequel les données d'archives doit être enregistré.
   d. Cliquez sur **Suivant**. ntainer
9. Dans la boîte de dialogue **Options de lecteur de départ**, saisissez les informations décrites ci-dessous :

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

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

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

Consommation du lecteur de départ sur un core cible

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

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

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

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

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

   Une fois que le core a vérifié le fichier, il remplit automatiquement le champ **Plage de dates** avec les dates du point de restauration le plus ancien et du point de restauration le plus récent figurant dans le lecteur de départ. Il importe également les commentaires entrés dans Configuration de la réplication d'un core autogéré .
7. Sous **Noms d'agent** dans la fenêtre **Consommer**, sélectionnez les machines pour lesquelles vous voulez consommer les données, puis cliquez sur **Consommer**.

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

Abandon d'un lecteur de départ en attente

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

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

Pour abandonner un lecteur de départ en attente :

1. Dans Core console sur le core source, cliquez sur l'onglet **Réplication**.
2. Cliquez sur **Lecteur de départ en attente (No.)**.
   La section **Lecteurs de départ en attente** s'affiche. Elle inclut le nom du noyau cible distant, la date et l'heure de création du lecteur de départ, et la plage de données des points de restauration inclus dans le lecteur de départ.
3. Cliquez sur le menu déroulant correspondant au lecteur à abandonner, puis sélectionnez **Abandon**.
   La fenêtre **Lecteur de départ en attente** s'ouvre.
4. Cliquez sur **Oui** pour confirmer l'opération.
   Le lecteur de départ est supprimé. S'il n'en existe aucun autre sur le core source, la prochaine fois que vous ouvrirez l'onglet **Réplication**, vous ne verrez pas apparaître le lien **Lecteur de départ en attente (No.)** ni la section **Lecteurs de départ en attente**.

Réplication vers un core géré par un tiers

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

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

Réplication d'un nouvel agent

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

Pour répliquer un nouvel agent :

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

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

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

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

6. Cliquez sur **Protéger**.

Réplication de données d'agent d'une machine

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

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

   La boîte de dialogue **Activer les réplications** s'ouvre.
4. Dans le champ **Hôte**, entrez un nom d'hôte.
5. Sous **Agents**, sélectionnez la machine qui contient l'agent et les données à répliquer.
6. Le cas échéant, cochez la case **Utiliser un lecteur de départ pour le transfert initial**.
7. Cliquez sur **Add** (Ajouter).

8. Pour suspendre ou reprendre la réplication, cliquez sur **Réplication** dans le menu déroulant **Actions**, puis sélectionnez **Suspendre** ou **Reprendre**, selon vos besoins.

Définir la priorité de réplication d'un agent

Pour établir la priorité de réplication d'un agent :

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

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

Surveillance de la réplication

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

Pour surveiller la réplication :

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

Tableau 4. Surveillance de la réplication

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

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

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

Paramètres de gestion de réplication

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

Pour gérer les paramètres de réplication :

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

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

4. Cliquez sur **Enregistrer**.

Suppression d'une réplication

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

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

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

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

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

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

Suppression d'une machine protégée sur le Core cible

Pour supprimer une machine protégée sur le Core cible :

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

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

Supprimer un core cible de la réplication

Pour supprimer un core cible de la réplication :

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

Supprimer un core source de la réplication

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

Pour supprimer un core source de la réplication

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

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

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

Restauration de données répliquées

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

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

Réalisez les options de restauration suivantes depuis le core cible :

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

Présentation du basculement et de la restauration

AppAssure prend en charge le basculement et la restauration dans des environnements répliqués en cas de panne grave au cours de laquelle le core source et les agents échouent. Le basculement fait référence à l'utilisation d'une cible redondante ou de secours (AppAssure Core) en cas de défaillance système ou de fin anormale d'un core source et de ses agents. La fonction principale du basculement est de lancer un nouvel agent identique à l'agent en panne. La seconde fonction est de faire passer le core cible dans un autre mode pour qu'il protège l'agent de basculement de la même manière que le core source protégeait l'agent initial avant la panne. Le core cible peut récupérer les instances depuis les agents répliqués et commencer immédiatement la protection sur les machines basculées.

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.

Exécution d'un basculement

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

Pour effectuer un basculement sur le core cible

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

   La boîte de dialogue **Basculement** s'affiche avec les étapes suivantes requises pour terminer un basculement.
4. Cliquez sur **Continuer**.
5. Dans la zone de navigation à gauche, sous **Machines protégées**, sélectionnez la machine dont le logiciel de l'agent AppAssure est associé avec les points de restauration.
6. Exportez les informations sur les points de restauration de sauvegarde sur cet agent vers une machine virtuelle.
7. Exportez les informations sur les points de restauration de sauvegarde sur cet agent vers une machine virtuelle.
8. 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.
9. Redémarrez la machine virtuelle, puis attendez que le service de l'agent démarre.
10. Revenez dans Core Console du core cible, puis vérifiez que le nouvel agent apparait sous **Machines protégées** et sur l'onglet **Réplication** sous **Réplication entrante**.
11. Forcez plusieurs instantanés, puis vérifiez qu'ils s'exécutent correctement.

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

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

Effectuer une restauration

Après avoir réparé ou remplacé le core 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. Accédez à Core Console sur le core cible, puis cliquez sur 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 **Restauration** s'ouvre pour décrire les étapes que vous devez suivre avant de cliquer sur le bouton **Continuer** pour terminer la restauration.
4. Cliquez sur **Annuler**.
5. Si la machine de basculement exécute Microsoft SQL Server ou Microsoft Exchange Server, arrêtez ces services.
6. Forcez un instantané de la machine. Pour plus d'informations, voir Forcer un instantané.
7. Arrêtez la machine basculée.
8. 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, reportez-vous à Création d'une archive.
9. Une fois l'archive créée, naviguez jusqu'à la console Core dans le core source récemment réparé, puis cliquez sur l'onglet **Outils**.
10. Importez l'archive que vous avez créée au cours de l'étape 7.

    Pour en savoir plus, voir Importation d'une archive.
11. Naviguez de nouveau jusqu'à la console Core sur le core cible, puis cliquez sur l'onglet **Réplication**.
12. Sous **Réplication entrante**, sélectionnez l'agent de basculement, puis développez les détails.
13. Dans la boîte de dialogue **Restauration**, cliquez sur **Continuer**.
14. Arrêtez la machine qui contient l'agent exporté créé au cours du basculement.
15. Effectuez une restauration sans système d'exploitation (BMR) du core source et de l'agent.

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

    Pour plus d'informations, reportez-vous à Définition des paramètres de la machine.
18. Naviguez jusqu'à la console Core sur le core cible, puis supprimez l'agent de l'onglet **Réplication**.
19. Dans la console Core sur le core source, redéfinissez la réplication entre la source et la cible en cliquant sur l'onglet **Réplication**, puis en ajoutant le core cible à la réplication.

6

Rapports

À propos des rapports

Le système DL permet de générer et d'afficher les informations de conformité, d'erreurs et récapitulatives de plusieurs machines core et agent.

Vous pouvez choisir d'afficher des rapports en ligne, d'imprimer des rapports ou de les exporter et de les enregistrer à l'un de plusieurs formats pris en charge. Vous pouvez choisir parmi les formats suivants :

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- txt
- CSV
- Image

À propos de la barre d'outils Rapports

La barre d'outils de tous les rapports vous permet d'imprimer et d'enregistrer de deux façons différentes. Le tableau suivant décrit les options d'impression et d'enregistrement.

Icon	Description
	Imprimer le rapport
	Imprimer la page actuelle
	Exporter un rapport et l'enregistrer sur le disque
	Exporter un rapport et l'afficher dans une nouvelle fenêtre Utilisez cette option pour copier, coller et envoyer par e-mail l'URL afin que d'autres puissent visualiser le rapport avec un navigateur Web.

À propos des rapports de conformité

Les rapports de conformité sont disponibles pour le Core et AppAssure Agent. Ils permettent de visualiser le statut des tâches effectuées par un core ou un agent sélectionné. Les tâches qui ont échoué apparaissent en rouge. Les informations du rapport de conformité du core non associé à un agent ne s'affichent pas.

Les détails sur les cores s'affichent par colonne et incluent les catégories suivantes :

- Core
- Agent protégé
- Type
- Résumé
- Condition
- Erreur
- Heure de début
- Heure de fin
- Heure
- Travail total

À propos des rapports d'erreurs

Les rapports d'erreurs sont des sous-ensembles des Rapports de conformité et sont disponibles pour les cores et les agents AppAssure. Ces rapports contiennent uniquement les tâches ayant échoué listées dans les rapports de conformité et les compilent dans un rapport unique pouvant être imprimé et exporté.

Les détails sur les erreurs s'affichent dans une vue de colonne et incluent les catégories suivantes :

- Core
- Agent
- Type
- Résumé
- Erreur
- Heure de début
- Heure de fin
- Temps écoulé
- Travail total

.

À propos du rapport de résumé de core

Le **rapport récapitulatif du core** contient des informations sur les référentiels du core sélectionné et sur les agents protégés par le core. Les informations s'affichent sous forme de deux résumés dans un rapport.

Résumé des référentiels

La partie **Référentiels** du **Rapport de résumé de core** comprend des données des référentiels se trouvant dans le core sélectionné. Les détails concernant les référentiels sont affichés dans une vue de colonne sous les catégories suivantes :

- Nom
- Chemin de données
- Chemin des métadonnées

- Espace alloué
- Espace utilisé
- Espace libre
- Ratio de compression/déduplication

Résumé des agents

La partie **Agents** du **Rapport de résumé Core** comprend les données de tous les agents protégés par le core sélectionné.

Les détails concernant les agents s'affichent en colonnes et incluent les catégories suivantes :

- Nom
- Volumes protégés
- Quantité d'espace protégé
- Quantité d'espace actuellement protégé
- Taux de changement quotidien (**Moyenne**, **Médian**)
- Statistiques de tâche (**Réussite**, **En échec**, **Annulé**)

Génération d'un rapport pour un core ou un agent

Pour générer un rapport pour un core ou un agent:

1. Accédez à Core Console et sélectionnez le core ou l'agent pour lequel vous souhaitez exécuter le rapport.
2. Cliquez sur l'onglet **Outils**.
3. Dans l'onglet **Outils**, développez **Rapports** dans la zone de navigation à gauche.
4. Dans la zone de navigation à gauche, sélectionnez le rapport à exécuter. La disponibilité des rapports dépend de la sélection effectuée à l'Étape 1. Vous trouverez la description des rapports ci-dessous.

Ordinateur	Rapports disponibles
Core	Rapport de conformité
	Rapport de résumé
	Rapport d'erreurs
Agent	Rapport de conformité
	Rapport d'erreurs

5. Dans le calendrier déroulant **Heure de début**, sélectionnez une date de début, puis entrez une heure de début pour l'exportation.

   REMARQUE : Aucune donnée n'est disponible tant que le core ou l'agent n'a pas été déployé.
6. Dans le calendrier déroulant **Heure de fin**, sélectionnez une date de fin, puis entrez une heure de fin de rapport.
7. Pour un **Rapport de résumé de core**, cochez la case **Tout le temps** si vous souhaitez que l'**Heure de début** et l'**Heure de fin** couvrent la totalité de la durée de vie du core.
8. Pour un **Rapport de conformité du core** ou un **Rapport d'erreurs du core**, utilisez la liste déroulante **Cores cibles** pour sélectionner le core dont vous souhaitez afficher les données.
9. Cliquez sur **Générer un rapport**.

Une fois le rapport généré, utilisez la barre d'outils pour imprimer ou exporter le rapport.

À propos des rapports de core de la Central Management Console

Le système DL permet de générer et afficher des informations de conformité, d'erreur et récapitulatives pour plusieurs cores. Les informations sur les cores s'affichent dans des colonnes avec les catégories décrites dans cette section.

Génération d'un rapport depuis la Central Management Console

Pour générer un rapport depuis la Central Management Console :

1. À l'écran **Bienvenue dans Central Management Console**, cliquez sur le menu déroulant situé dans le coin supérieur droit.
2. Dans le menu déroulant, cliquez sur **Rapports**, puis sélectionnez une des options suivantes :
   - **Rapport de conformité**
   - **Rapport de résumé**
   - **Rapport des échecs**
3. Dans la zone de navigation de gauche, sélectionnez le ou les cores pour lesquels vous souhaitez exécuter le rapport.
4. Dans le calendrier déroulant **Heure de début**, sélectionnez une date de début, puis entrez une heure de début pour le rapport.

   REMARQUE : Aucune donnée n'est disponible tant que les cores n'ont pas été déployés.
5. Dans le calendrier déroulant **Heure de fin**, sélectionnez une date de fin, puis entrez une heure de fin de rapport.
6. Cliquez sur **Générer un rapport**.

   Une fois le rapport généré, utilisez la barre d'outils pour imprimer ou exporter le rapport.

7

Obtention d'aide

Recherche de documentation et de mises à jour logicielles

Des liens d'accès direct à la documentation AppAssure, et de l'appliance DL1000 et aux mises à jour logicielles sont disponibles depuis Core Console.

Documentation

Pour accéder au lien de documentation :

1. dans la Core Console, cliquez sur l'onglet **Appliance** .
2. Dans le volet de gauche, accédez au lien **Appliance** → **Documentation**.

Mises à jour logicielles

Pour accéder au lien des mises à jour de logiciel :

1. dans la Core Console, cliquez sur l'onglet **Appliance** .
2. Dans le volet de gauche, accédez au lien **Appliance** → **Mises à jour de logiciel**.

Contacter Dell

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, reportez-vous à la section **software.dell.com/support**.

Commentaires sur la documentation

Cliquez sur le lien **Commentaires** sur n'importe quelle page de documentation Dell, remplissez le formulaire et cliquez sur **Envoyer** pour envoyer vos commentaires.