




Appliance Dell DL1300

Guide de déploiement



Remarques, précautions et avertissements

-  **REMARQUE** : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre ordinateur.
-  **PRÉCAUTION** : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.
-  **AVERTISSEMENT** : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

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

2016 - 05

Rév. A01

Table des matières

1 Présentation du système DL1300.....	6
Technologies de base du DL1300.....	6
Live Recovery	6
Universal Recovery	6
Déduplication globale réelle	7
Cryptage.....	7
Fonctions de protection des données du Dell DL1300.....	7
Dell DL1300 Core.....	7
Agent intelligent Dell DL1300.....	8
Processus d'instantané.....	8
Réplication : site de reprise après sinistre ou fournisseur de services.....	8
Restauration.....	9
Restauration en tant que service (RaaS, Recovery-as-a-Service)	9
Virtualisation et cloud.....	9
Architecture de déploiement du Dell DL1300.....	10
Autres informations utiles.....	11
2 Installation de votre Dell DL1300.....	13
Introduction.....	13
Configurations disponibles.....	13
Présentation de l'installation.....	13
Spécifications d'installation.....	14
Configuration réseau requise.....	14
Infrastructure de réseau conseillée.....	14
Configuration du matériel.....	14
Installation de l'appliance DL1300 dans un rack.....	14
Utilisation du système sans rack.....	14
Câblage de l'appliance.....	15
Branchement du bras de maintien des câbles (en option).....	15
Mise sous tension de l'appliance DL1300.....	15
Configuration initiale du logiciel.....	15
Assistant Configuration de l'appliance AppAssure.....	16
Utilitaire de récupération et de mise à jour.....	19
Restauration automatique rapide de l'appliance.....	19
Création de la clé USB RASR.....	19
Exécution du RASR.....	20
3 Configuration de votre Dell DL1300.....	22

Présentation de la configuration.....	22
Configuration de navigateurs pour accéder à Core Console DL1300.....	22
Modification des paramètres de navigateur dans Internet Explorer et Chrome	22
Configuration des paramètres de navigateur dans Firefox.....	23
Accès à la Core Console DL1300.....	23
Mise à jour des sites de confiance dans Internet Explorer.....	23
Gestion des licences	24
Contacter le serveur de Portail de licences	24
Modifier une clé de licence	24
Modification manuelle de la langue d'AppAssure.....	25
Modification de la langue du système d'exploitation au cours de l'installation.....	25
Cryptage de données d'instantanés d'agent.....	26
Configuration d'un serveur de messagerie et d'un modèle de notification par courrier électronique	27
4 Préparation de la protection de vos serveurs.....	29
Présentation.....	29
Protection des machines.....	29
Vérification de la connectivité du réseau.....	30
Vérification des paramètres du pare-feu.....	30
Vérification de la résolution DNS.....	30
Association de cartes réseau.....	30
Réglage de flux simultanés.....	32
Installation des agents sur les clients.....	32
Installation à distance des agents (pousser).....	32
Déploiement du logiciel de l'agent lors de la protection d'une machine.....	33
Installation des agents Microsoft Windows sur le client.....	34
Ajout d'un agent à l'aide du portail de licences.....	34
Installation d'agents sur des ordinateurs Linux.....	35
Emplacement des fichiers de l'agent Linux.....	36
Dépendances de l'agent.....	36
Installation de l'agent sur Ubuntu.....	37
Installation de l'agent sur Red Hat Enterprise Linux et CentOS.....	38
Installation de l'agent sur SUSE Linux Enterprise Server.....	38
5 Scénarios d'utilisation courants.....	40
Protection des machines.....	40
Instantanés.....	40
Agents intelligents DL1300	40
Déploiement d'agents intelligents.....	40
Configuration des tâches de protection.....	42
Protection d'une machine	42

Restauration de données.....	44
Restauration de répertoires ou de fichiers.....	44
Restauration de volumes.....	45
Restauration sans système d'exploitation (BMR).....	46
Conditions requises pour l'exécution d'une restauration BMR d'une machine Windows.....	47
Stratégie d'exécution d'une restauration sans système d'exploitation d'une machine Windows	47
Réplication de points de restauration.....	47
Configuration de votre environnement.....	48
Étapes de configuration de la réplication.....	49
Utilisation de disques virtuels de secours.....	50
Exécution d'une exportation Hyper-V ponctuelle	50
Exécution d'une exportation Hyper-V continue (disque de secours virtuel)	52
Gestion des points de restauration.....	53
Archivage des données.....	53
Archivage dans un Cloud.....	56
6 Obtention d'aide.....	57
Recherche de documentation et de mises à jour logicielles.....	57
Documentation.....	57
Mises à jour logicielles.....	57
Contacter Dell.....	57
Commentaires sur la documentation.....	57

Présentation du système DL1300

Le système DL1300 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.

Votre DL1300 prend en charge les environnements à plusieurs hyperviseurs sur les clouds privés et publics VMware vSphere, Oracle VirtualBox et Microsoft Hyper-V.

Technologies de base du DL1300

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 DL1300 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 machines 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 DL1300 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 DL1300

Dell DL1300 Core

Le Core est le composant central de l'architecture de déploiement DL1300. 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 autonome sur le réseau, qui exécute 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 DL1300

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 DL1300 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. L'agent DL1300 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 DL1300 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 Core DL1300 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 DL1300 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 DL1300 n'est pas mutualisé. Les fournisseurs MSP peuvent utiliser le DL1300 sur plusieurs sites et créer un environnement mutualisé.

Virtualisation et cloud

Le core DL1300 est prêt pour le cloud, ce qui permet de tirer parti de la capacité de traitement du cloud pour la restauration et l'archivage.

DL1300 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 DL1300

L'architecture de déploiement du DL1300 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. Le core DL1300 utilise des images de base et des instantanés incrémentiels pour compiler les points de restauration des agents protégés.

En outre, le système DL1300 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 DL1300 effectue une troncature des journaux du serveur Microsoft Exchange protégé.

Le diagramme suivant montre un déploiement DL1300 simple. Les agents DL1300 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 core DL1300 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.

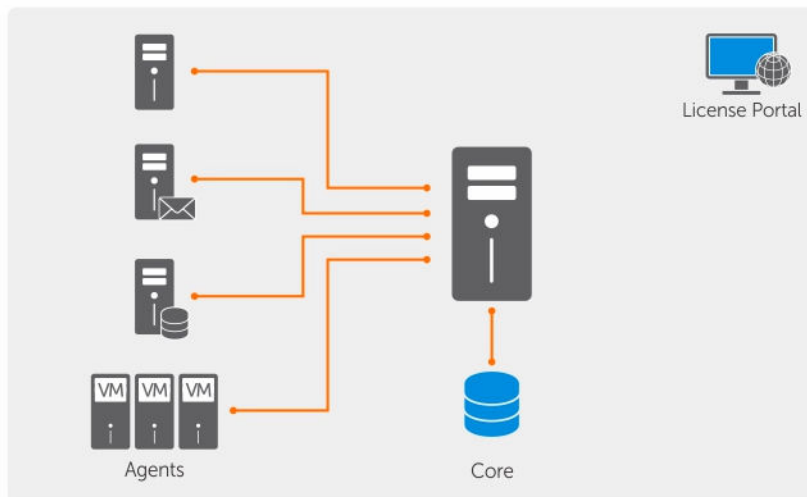


Figure 2. Architecture de déploiement Dell DL1300

Vous pouvez également déployer plusieurs cœurs DL1300, comme le montre le diagramme suivant. Une console centrale gère plusieurs cœurs.

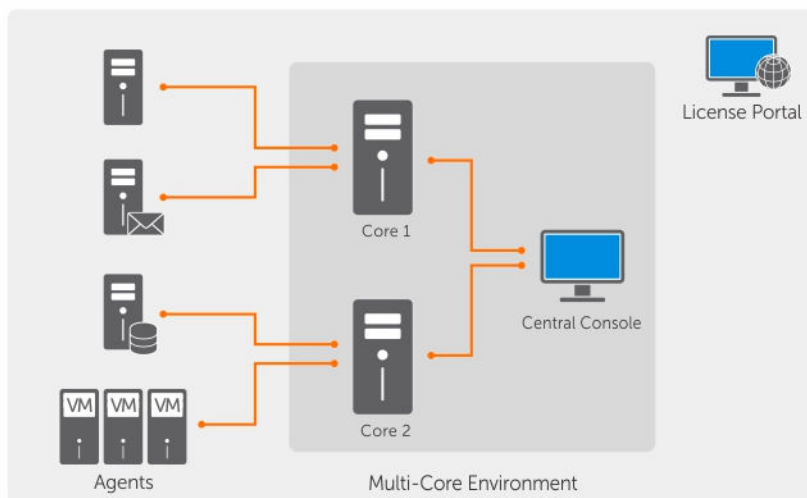


Figure 3. Architecture de déploiement de plusieurs cœurs DL1300

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 la configuration du système et les caractéristiques techniques. Ce document est aussi fourni avec votre système.
Présentation des informations système	Fournit des informations sur la configuration du matériel et l'installation du logiciel sur votre appliance.
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 DL1300.
Guide d'interopérabilité	Fournit des informations sur les logiciels et matériels pris en charge pour l'appliance, 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.

Installation de votre Dell DL1300

Introduction

La DL Backup to Disk Appliance (Appliance de sauvegarde sur disque DL) offre :

- des sauvegardes et des scénarios de restauration plus rapides que les périphériques sur bande traditionnels et que les méthodologies de sauvegarde habituelles
- la possibilité de déduplication en option
- une protection continue des données pour les serveurs de centre de données et de bureau distants
- un déploiement facile et rapide qui réduit le temps nécessaire à la protection des données critiques

Configurations disponibles

L'appliance DL est fournie dans les configurations suivantes :

Tableau 1. Configurations disponibles

Capacité	Configuration matérielle
2 To	Quatre disques durs de 4 To avec 2 To d'espace de référentiel utilisable
3 To avec 2 machines virtuelles	Quatre disques durs de 4 To avec 3 To d'espace de référentiel utilisable et espace VM ajustable
4 To avec 2 machines virtuelles	Quatre disques durs de 4 To 4 To d'espace de référentiel utilisable et espace VM ajustable

Chaque configuration inclut également les matériels et logiciels suivants :


- Système Dell DL1300
- Contrôleurs RAID Dell PowerEdge (PERC)
- Logiciel Dell AppAssure

Présentation de l'installation

L'installation du DL1300 comprend l'installation des services de Core AppAssure 5 et d'agent AppAssure 5 sur les systèmes à protéger. Si d'autres Cores sont configurés, vous devez installer les services de console de gestion centrale AppAssure 5 Central Management Console.

Pour installer le DL1300, procédez comme suit :

1. Procurez-vous la clé de licence permanente. Dans Core Console, vous pouvez gérer vos licences DL1300 directement, modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au Portail de licences Dell AppAssure depuis la page de Gestion des licences dans Core Console.

 **REMARQUE** : L'appliance est configurée et livrée avec une licence logicielle temporaire de 30 jours.

2. Passez en revue les conditions préalables à l'installation.
3. Configuration du matériel.
4. Configuration du logiciel initial (Assistant Configuration de l'appliance AppAssure).
5. Installation de la console de gestion du Core.

Spécifications d'installation

Configuration réseau requise

Votre appliance nécessite l'environnement réseau suivant :


- Réseau actif avec câbles et connexions Ethernet disponibles
- Adresse IP statique et adresse IP de serveur DNS, si le protocole de configuration Dynamic Host Configuration Protocol (DHCP) ne les a pas fournies
- Un nom d'utilisateur et un mot de passe et des privilèges d'administrateur

Infrastructure de réseau conseillée

Dell recommande d'utiliser des commutateurs aux entreprises de 1 GbE ou plus avec AppAssure pour des performances optimales.

Configuration du matériel.

L'appliance est livrée avec un seul système DL1300. Avant de configurer le matériel de l'appliance, voir le manuel DL1300 de votre système, livré avec l'appliance. Déballiez et configurez le matériel de l'appliance DL1300.

 **REMARQUE** : Le logiciel est préinstallé sur le serveur. Tous les supports inclus avec le système doivent être utilisés uniquement en cas de restauration du système.

Pour configurer le matériel DL1300 :

1. Montez le système DL1300 en rack et câblez-le.
2. Mettez le système DL1300 sous tension.


Installation de l'appliance DL1300 dans un rack

Si votre système inclut un kit de rails, recherchez la section *Instructions d'installation en rack* fournies avec ce kit. Suivez ces instructions pour installer les rails et l'appliance DL1300 dans le rack.

Utilisation du système sans rack

Vous pouvez utiliser le système sans le rack de serveur. Lorsque vous utilisez le système sans rack, assurez-vous de suivre les directives suivantes :

- Le système doit être placé sur une surface stable et solide qui supporte tout le système.

 **REMARQUE** : Le système ne doit pas être placé à la verticale.

- Ne placez pas le système sur le sol.

- Ne placez pas quoi que ce soit sur la partie supérieure du système. Le panneau du haut risquerait de se déformer sous le poids et d'endommager le système.
- Vérifiez qu'il y a assez d'espace autour du système pour une ventilation correcte.
- Vérifiez que le système est installé dans les conditions de température recommandées, telle qu'elles sont indiquées dans la section relative aux caractéristiques techniques de l'environnement dans le document *Dell DL1300 Appliance Owner's Manual* (Manuel du propriétaire de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

⚠ PRÉCAUTION : Le non-respect de ces consignes risque d'entraîner l'endommagement du système ou des blessures corporelles.

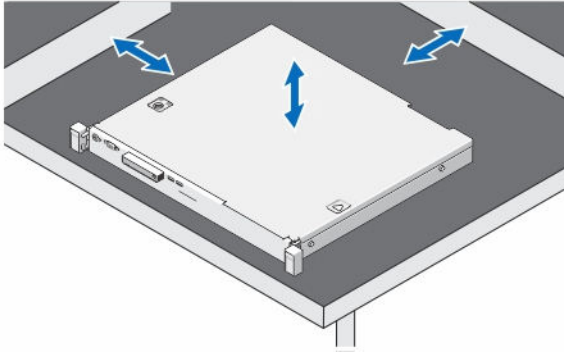


Figure 4. Utilisation du système sans rack

Câblage de l'appliance

Localisez le document *Dell DL1300 Appliance Getting Started Guide* fourni avec l'appliance et suivez ses instructions pour rattacher le clavier, la souris, l'écran, l'alimentation et les câbles réseau au système DL1300.

Branchement du bras de maintien des câbles (en option)

Si le serveur inclut un bras de maintien des câbles (Cable Management Arm - CMA), localisez les *Instructions d'installation* livrées avec le kit CMA et suivez les instructions qui y figurent pour l'installer.

Mise sous tension de l'appliance DL1300

Après avoir connecté l'appliance, mettez votre système sous tension.


REMARQUE : Pour une fiabilité et une disponibilité maximales, il est recommandé de connecter l'appliance à un onduleur (UPS). Pour plus d'informations, voir le document *Dell DL1300 Getting Started Guide* (Guide de démarrage du Dell DL1300) disponible sur Dell.com/support/manuals.

Configuration initiale du logiciel


Lorsque vous mettez l'appliance sous tension pour la première fois et que vous modifiez le mot de passe système, l'**Assistant Configuration de l'appliance AppAssure** démarre automatiquement.

1. Après la mise sous tension du système, choisissez une langue pour le système d'exploitation à partir des options de langue offertes par Windows.


- Le CLUF (Contrat de licence utilisateur final) de Microsoft s'affiche sur la page **Paramètres**.
2. Pour accepter le CLUF, cliquez sur le bouton **J'accepte**.
Une page permettant de modifier le mot de passe d'administration apparaît.
 3. Cliquez sur **OK** en réponse au message vous invitant à modifier le mot de passe d'administrateur.
 4. Saisissez et confirmez le nouveau mot de passe.
Un message vous invite à confirmer la modification du mot de passe.
 5. Cliquez sur **OK**.
 6. À partir de l'écran **Dell readme.htm**, faites défiler la page et cliquez sur **Poursuivre/Continuer**.
Après avoir entré le mot de passe, l'écran **Appuyez sur Ctrl+Alt+Suppr pour vous connecter** s'affiche.
 7. Connectez-vous en utilisant le mot de passe d'administrateur modifié.
L'écran **Sélectionnez la langue de appliance AppAssure** s'affiche.
 8. Sélectionnez la langue de votre appliance à partir de la liste des langues prises en charge.
L'écran **EULA** s'affiche.
 9. Pour accepter le CLUF, cliquez sur le bouton **CLUF**.

 **REMARQUE** : Vous pouvez continuer d'exécuter l'Assistant Configuration de l'appliance AppAssure uniquement si vous acceptez le CLUF. Sinon, l'appliance se met hors tension immédiatement.

L'écran d'accueil de l'**Assistant Configuration de l'appliance AppAssure** s'affiche.

 **REMARQUE** : Il faut parfois jusqu'à 30 secondes pour que l'**Assistant Configuration de l'appliance AppAssure** s'affiche sur la console système.

Assistant Configuration de l'appliance AppAssure

 **PRÉCAUTION** : Assurez-vous d'avoir effectué toutes les étapes de l'Assistant Configuration de l'appliance AppAssure avant d'effectuer toute autre tâche ou de modifier des paramètres sur l'appliance. N'effectuez aucune modification via le panneau de configuration, n'utilisez pas Microsoft Windows Update, ne mettez pas à jour le logiciel AppAssure et n'installez aucune licence tant que l'Assistant n'a pas terminé. Le service de mise à jour Windows est désactivé temporairement pendant le processus de configuration. Si vous quittez l'Assistant Configuration de l'appliance AppAssure avant qu'il ait terminé, des erreurs de fonctionnement du système pourront se produire.

L'**Assistant Configuration de l'appliance AppAssure** vous guide au cours des étapes suivantes pour configurer le logiciel sur l'appliance :

- [Configuration de l'interface réseau](#)
- [Configuration des paramètres de nom d'hôte et de domaine](#)
- [Configuration des paramètres SNMP](#)

Une fois que vous avez terminé l'installation à l'aide de l'Assistant, la console Core démarre automatiquement.


Configuration de l'interface réseau

Pour configurer les interfaces réseau disponibles :

1. À l'écran **Bienvenue à l'Assistant Configuration de l'appliance AppAssure**, cliquez sur **Suivant**.

La page d'**interfaces réseau** affiche les interfaces réseau connectées disponibles.

2. Sélectionnez les interfaces réseau à configurer.

 **REMARQUE** : L'**Assistant Configuration de l'appliance AppAssure** configure les interfaces réseau en tant que ports individuels (sans association). Pour optimiser les performances d'ingestion, vous pouvez créer un canal d'ingestion de plus grande taille en regroupant les cartes réseau (NIC). Cependant, cela doit être fait après la configuration initiale de l'appliance.

3. Le cas échéant, connectez des interfaces réseau supplémentaires et cliquez sur **Actualiser**.
Les interfaces réseau connectées disponibles s'affichent.
4. Cliquez sur **Suivant**.
La page **Configurer l'interface réseau sélectionnée** s'affiche.
5. Sélectionnez le protocole internet approprié pour l'interface sélectionnée.
Sélectionnez **IPv4** ou **IPv6**.


Les détails du réseau s'affichent en fonction du protocole Internet sélectionné.

6. Pour attribuer les détails du protocole Internet, effectuez l'une des actions suivantes :
 - Pour attribuer automatiquement les détails du protocole Internet sélectionné, sélectionnez **Obtenir une adresse IPV4 automatiquement**.
 - Pour attribuer automatiquement la connexion réseau, sélectionnez **Utiliser l'adresse IPv4 automatiquement** et saisissez les détails suivants :
 - **Adresse IPv4** ou **Adresse IPv6**
 - **Masque de sous-réseau** pour IPv4 et **Longueur de préfixe de sous-réseau** pour IPv6
 - **Passerelle par défaut**
7. Pour attribuer les détails du serveur DNS, effectuez l'une des actions suivantes :
 - Pour attribuer automatiquement l'adresse du serveur DNS, sélectionnez **Obtenir l'adresse du serveur DNS automatiquement**.
 - Pour attribuer le serveur DNS manuellement, sélectionnez **Utiliser l'adresse de serveur DNS suivante** et saisissez les détails suivants :
 - **Serveur DNS préféré**
 - **Autre serveur DNS**
8. Cliquez sur **Suivant**.
La page **Configurer les paramètres de nom d'hôte et de domaine** s'affiche.

Pour en savoir plus sur l'association des cartes réseau, voir [Association des cartes réseau](#).


Configuration des paramètres de nom d'hôte et de domaine

Vous devez attribuer un nom d'hôte à l'appliance. Il vous est recommandé de modifier le nom d'hôte avant de lancer des sauvegardes. Par défaut, le nom d'hôte est le nom du système tel qu'il est attribué par le système d'exploitation.

 **REMARQUE** : Si vous prévoyez de modifier le nom d'hôte, il vous est recommandé de le faire à ce stade. La modification du nom d'hôte après l'exécution de l'**Assistant Configuration de l'appliance AppAssure** exige la réalisation de plusieurs étapes.

Pour configurer les paramètres de nom d'hôte et de domaine :


1. Dans la boîte de dialogue **Configurer les paramètres de nom d'hôte et de domaine**, dans le champ **Nouveau nom d'hôte**, entrez un nom d'hôte approprié.
2. Si vous ne souhaitez pas connecter votre appliance à un domaine, sélectionnez **Non** sous **Souhaitez-vous que l'appliance rejoigne un domaine ?**.

 **REMARQUE** : Si votre DL1300 est installé avec Microsoft Windows Server 2012 édition Foundation, l'option Joindre un domaine sera désactivée.

Par défaut, **Oui** est sélectionné.


3. Si vous souhaitez connecter l'appliance à un domaine, saisissez les détails suivants :

- **Nom de domaine**
- **Nom d'utilisateur de domaine**

 **REMARQUE** : L'utilisateur de domaine doit avoir des droits d'administrateur local.

- **Mot de passe d'utilisateur de domaine**

4. Cliquez sur **Suivant**.

 **REMARQUE** : La modification du nom d'hôte ou du domaine exige un redémarrage de la machine. Après le redémarrage, l'**Assistant Configuration de l'appliance AppAssure** est lancé automatiquement. Si l'appliance est connectée à un domaine, après le redémarrage, vous devez vous connecter en tant qu'utilisateur de domaine doté de droits d'administrateur sur l'appliance.


La page **Configurer les paramètres SNMP** s'affiche.

Configuration des paramètres SNMP

Simple Network Management Protocol (SNMP) est un protocole de gestion de réseau utilisé couramment qui permet des fonctions de gestion compatibles avec SNMP telles que la détection de périphériques, la surveillance et la génération d'événements. SNMP fournit une gestion de réseau du protocole TCP/IP.

Pour configurer des alertes SNMP pour l'appliance :

1. Sur la page **Configurer les paramètres SNMP**, sélectionnez **Configurer SNMP sur cette appliance**.

 **REMARQUE** : Désélectionnez **Configurer SNMP sur cette appliance** si vous ne souhaitez pas configurer des détails et alertes SNMP sur l'appliance et passez à l'étape 6.

2. Dans **Communautés**, saisissez un ou plusieurs noms de communauté SNMP.

Utilisez des virgules pour séparer plusieurs noms de communauté.

3. Dans **Accepter les paquets SNMP de ces hôtes**, saisissez les noms des hôtes avec lesquels l'appliance peut communiquer.

Séparez les noms d'hôte par des virgules ou laissez ce champ vide pour permettre la communication avec tous les hôtes.

4. Pour configurer les alertes SNMP, saisissez le **Nom de communauté** et les **Destinations d'interruptions** des alertes SNMP et cliquez sur **Ajouter**.

Répétez cette étape pour ajouter des adresses SNMP supplémentaires.

5. Pour supprimer une adresse SNMP configurée, sélectionnez l'adresse SNMP appropriée dans **Adresses SNMP configurées** et cliquez sur **Supprimer**.

6. Cliquez sur **Suivant**.

La page **Merci** s'affiche.

7. Pour achever la configuration, cliquez sur **Suivant**.

8. Cliquez sur **Quitter** dans la page **Configuration terminée**.

La console Core s'ouvre dans votre navigateur Web par défaut.


Utilitaire de récupération et de mise à jour


L'utilitaire RUU (Utilitaire de récupération et de mise à jour) est un programme d'installation tout-en-un permettant de récupérer et de mettre à jour le logiciel des appliances DL (DL1000, DL1300, DL4000 et DL4300). Il comprend le logiciel AppAssure Core et les composants spécifiques de l'appliance.


RUU se compose de versions mises à jour des rôles et fonctionnalités de Windows Server, ASP .NET MVC3, le fournisseur LSI, les applications DL, et les logiciels OpenManage Server Administrator et AppAssure Core. En outre, l'utilitaire RUU (Utilitaire de récupération et de mise à jour) met également à jour le contenu de la RASR (Rapid Appliance Self Recovery/Récupération automatique rapide de l'appliance).

Pour télécharger la version la plus récente de l'utilitaire RUU :

1. rendez-vous sur le portail de licences sous Téléchargements, puis téléchargez le programme d'installation de l'utilitaire RUU ou rendez-vous sur **support.dell.com**.
2. Exécutez le programme d'installation de l'utilitaire RUU.

 **REMARQUE** : Il se peut que votre système redémarre au cours du processus de mise à jour de l'utilitaire RUU.

 **REMARQUE** : Si vous utilisez le RUU n° 184 et que votre appliance DL possède une version de Core AppAssure inférieure (antérieure) à 5.4.3.106, le core est mis à niveau vers AppAssure Core 5.4.3.106 .

 **REMARQUE** : Si vous effectuez une mise à niveau vers RUU n° 184, vous risquez de commencer à voir apparaître des incohérences lors de l'exécution future de sauvegardes Windows déjà planifiées (via RASR), ou il vous sera peut-être impossible de créer une stratégie de sauvegarde Windows. Ces erreurs se produisent en raison du manque d'espace à l'emplacement du stockage de vos sauvegardes Windows.

Autres causes potentielles de ces échecs :

1. mise à niveau vers Rapid Recovery (Récupération rapide), en particulier si un niveau de cache de déduplication supérieur au minimum est utilisé.
2. Installation ou mise à jour ou des logiciels (par exemple, Outlook) sur l'appliance.
3. Installation des mises à jour Windows.
4. Ajout/agrandissement des fichiers de données (telles que la cache de déduplication).
5. Combinaisons des éléments précédents.

Restauration automatique rapide de l'appliance


RASR (Rapid Appliance Self Recovery) est un processus de restauration sur système nu dans lequel les lecteurs du système d'exploitation et les lecteurs de données sont utilisés pour restaurer les paramètres définis en usine.

Création de la clé USB RASR

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** : Veillez à utiliser la fonction Windows d'éjection de lecteur pour préparer la clé USB au retrait. Sinon, le contenu de la clé USB pourrait être endommagé et la clé USB ne fonctionnerait pas comme prévu.

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

Exécution du 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 clé USB RASR](#).

Les étapes suivantes vous aident à effectuer la réinitialisation usine.

Pour effectuer la restauration RASR :

1. Insérez la clé USB RASR créée.
2. Redémarrez l'appliance et sélectionnez **Gestionnaire d'amorçage (F11)**.
3. Dans le **menu principal du Gestionnaire d'amorçage**, sélectionnez le **menu d'amorçage du BIOS direct**.
4. Dans le **menu d'amorçage du gestionnaire d'amorçage**, sélectionnez le lecteur USB relié.
5. Sélectionnez votre configuration de clavier.
6. Cliquez sur **Dépanner** → **Récupération automatique de l'appliance**
7. Sélectionnez le système d'exploitation cible (SE).
RASR démarre, et l'écran d'accueil s'affiche.
8. Cliquez sur **Suivant**.
L'écran de vérification **Conditions** s'affiche.

 **REMARQUE** : Veillez à ce que tous les matériels et les autres spécifications soient vérifiés avant d'exécuter RASR.

9. Cliquez sur **Suivant**.
L'écran de **sélection du mode de restauration** s'affiche avec trois options :
 - **Restauration du système**
 - **Assistant de récupération Windows**
 - **Restauration des paramètres définis en usine**
10. Sélectionnez l'option **Restaurer les paramètres définis en usine**.
This option will recover the operating system disk from the factory image.
11. Cliquez sur **Suivant**.

Le message d'avertissement suivant s'affiche dans une boîte de dialogue : This operation will recover the operating system. All OS disk data will be overwritten.

12. Cliquez sur **Oui**.


Le disque du système d'exploitation commence la restauration du système d'exploitation d'origine.

13. A la fin de la réinitialisation usine, dans l'écran **RASR terminée**, cliquez sur **Terminer**.

Configuration de votre Dell DL1300


Présentation de la configuration


La configuration inclut des tâches telles que la configuration de navigateurs pour accéder à Console Core DL1300, la gestion des licences et la configuration des alertes et notifications. Après avoir terminé la configuration du Core, vous pouvez protéger les agents et effectuer la restauration.


 **REMARQUE** : Lorsque vous utilisez l'appliance de sauvegarde sur disque DL1300, il est recommandé d'utiliser l'onglet **Appliance** pour configurer le Core.

Configuration de navigateurs pour accéder à Core Console DL1300

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

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

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

 **REMARQUE** : Vérifiez que l'option Configuration de sécurité renforcée d'Internet Explorer est activée lorsque vous accédez à la console Web Core en local ou à distance. Pour activer la configuration de sécurité renforcée dans Internet Explorer, ouvrez **Gestionnaire de serveur** → **Serveur local** → **Configuration de sécurité renforcée d'Internet Explorer**. Lorsque cette dernière option s'affiche, vérifiez qu'elle est **activée**.

Modification des paramètres de navigateur dans Internet Explorer et Chrome

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

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

8. Faites défiler la liste jusqu'à **Multimédia**, puis sélectionnez **Lire les animations dans les pages Web**.
9. Faites défiler l'écran jusqu'à **Sécurité**, sélectionnez **Activer l'authentification Windows intégrée**, puis cliquez sur **OK**.

Configuration des paramètres de navigateur dans Firefox

Pour modifier les paramètres de navigateur dans 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 le Core ; par exemple : *Adresse IP,nom d'hôte*.
4. Redémarrez Firefox.

Accès à la Core Console DL1300

Assurez-vous de mettre à jour les sites de confiance de la façon discutée dans la rubrique [Mise à jour des sites de confiance dans Internet Explorer](#) , puis configurez vos navigateurs de la façon discutée dans la rubrique [Configuration de navigateurs pour accéder à Core Console DL1300](#). Après avoir mis à jour les sites de confiance dans Internet Explorer et configuré vos navigateurs, effectuez l'une des tâches suivantes pour accéder à la console Core :

- Connectez-vous localement à votre serveur Core, puis double-cliquez sur l'icône **Console Core**.
- 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 **Ajouter** .
8. Sous **Ajouter ce site Web à la zone**, entrez **about:blank**.
9. Cliquez sur **Ajouter**.
10. Cliquez sur **Fermer**, puis sur **OK**.

Gestion des licences

Vous pouvez gérer les licences DL1300 directement à partir de la Core Console. Depuis la console, vous pouvez modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au portail des licences depuis la page de gestion des licences dans Core Console ou vous pouvez accéder au portail de licences, à <https://licenseportal.com>.

La page Licences contient les informations suivantes :

- Type de licence
- État de licence
- Détails du référentiel
- Réplication des cores maîtres (entrants)
- Réplication des cores secondaires (sortants)
- Cumuls simultanés
- Stratégie de rétention de cumul
- Clés de cryptage
- Exportations de disque de secours virtuels
- Vérifications de montabilité
- Troncatures de journal Exchange
- Troncature de journal SQL
- Intervalle minimal d'instantané

Contacteur 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 **Contacteur maintenant**.

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 section **Détails de la licence**, cliquez sur **Modifier la licence**.
La boîte de dialogue **Modifier la licence** s'affiche.
3. Mettez à jour la nouvelle clé de licence. Pour mettre à jour la clé de licence :
 - sélectionnez la clé de licence appropriée à l'aide de l'onglet **Parcourir** dans la boîte de dialogue **Envoyer le fichier de licence**.
Pour télécharger la licence appropriée :
 1. accédez à www.rapidrecovery.licenseportal.com.

2. Dans le menu déroulant **Logiciel**, dans le coin supérieur gauche de la page, sélectionnez **Appliance**.
Toutes les licences disponibles et les informations correspondantes s'affichent.
3. Dans la colonne **Actions**, cliquez sur l'icône de téléchargement.
La licence est téléchargé sur votre système.
 - Entrez la clé de licence dans le champ `Entrer la clé de licence`.
4. Cliquez sur **Continue** (Continuer).
La licence est mise à jour sur votre système.

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 `regedit`.
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 Microsoft 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 système d'exploitation (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** et **Ajouter**. Le catalan est 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.


Cryptage de données d'instantanés d'agent

Le core peut crypter les données d'instantané d'un agent dans le référentiel. Au lieu de crypter tout le référentiel, le DL1300 permet de spécifier une clé de cryptage au cours de la protection d'un agent dans un référentiel, ce qui permet de réutiliser les clés pour différents agents.

Pour crypter les données d'instantanés d'agent :


1. À partir du Core, cliquez sur **Configuration** → **Gérer** → **Sécurité**.
2. Cliquez sur **Actions**, puis sélectionnez **Ajouter une clé de cryptage**.
La page **Créer une clé de cryptage** s'affiche.
3. Saisissez les informations suivantes :

Champ	Description
Nom	Entrez un nom pour la clé de cryptage.
Commentaire	Entrez un commentaire concernant la clé de cryptage. Il sert à fournir des détails supplémentaires sur la clé de cryptage.
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.

 **REMARQUE** : Il est recommandé d'enregistrer la phrase de passe de cryptage. En effet, si vous la perdez, les données seront inaccessibles. Pour en savoir plus, voir le chapitre relatif à la gestion de la sécurité dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300).

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

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

 **REMARQUE** : Vous devez également configurer les paramètres de groupe de notification, notamment activer l'option **Notifier par e-mail**, avant l'envoi de messages d'alerte par e-mail. Pour en savoir plus sur la façon de spécifier des événements afin de recevoir des alertes par e-mail, voir la rubrique relative à la configuration des groupes de notification pour les événements système dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

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

1. Depuis le Core, sélectionnez l'onglet **Configuration**.
2. Depuis l'option **Gérer**, sélectionnez **Événements**.
3. Dans le volet **Paramètres SMTP d'e-mail**, cliquez sur **Modifier**.

La boîte de dialogue **Modifier la configuration des notifications par e-mail** s'affiche.

4. Sélectionnez **Activer les notifications par e-mail**, puis entrez des informations détaillées pour le serveur de messagerie de la façon décrite ci-dessous :

Zone de texte	Description
Serveur SMTP	Entrez le nom du serveur de messagerie que le modèle de notification par e-mail doit utiliser. Selon la convention de nommage, le nom inclut le nom d'hôte, le domaine et le suffixe, par exemple, smtp.gmail.com .
Port	Entrez un numéro de port qui identifiera le port d'un serveur de messagerie, par exemple, le port 587 pour Gmail. La valeur par défaut est 25.
Délai (secondes)	Entrez une valeur pour spécifier la durée de la tentative de connexion avant l'expiration du délai. Cette valeur s'utilise pour établir le temps en secondes avant la survenue de l'expiration d'un délai lors de tentatives de connexion au serveur d'e-mail. La valeur par défaut est de 30 secondes.
TLS	Sélectionnez cette option si le serveur de messagerie utilise une connexion sécurisée telle que TLS(Transport Layer Security) ou SSL (Secure Sockets Layer).
Nom d'utilisateur	Entrez un nom d'utilisateur pour le serveur de messagerie.
Mot de passe	Entrez un mot de passe pour le serveur de messagerie.
De	Entrez une adresse d'expéditeur qui servira à préciser l'adresse à laquelle le modèle de notification par e-mail sera retourné, par exemple, noreply@localhost.com .

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>.

Email (E-mail) Entrez les informations de corps du modèle qui décrivent l'événement, le moment où il s'est produit et sa gravité.

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

Préparation de la protection de vos serveurs

Présentation

Pour protéger vos données avec DL1300, vous devez ajouter les stations de travail et les serveurs à protéger dans Core console ; par exemple, votre serveur Exchange, SQL ou Linux, etc.

Dans la console Core, vous pouvez identifier la machine où l'agent est installé et spécifier les volumes à protéger (un espace de stockage Microsoft Windows, par exemple). Vous pouvez définir des planifications de protection, ajouter des mesures de sécurité supplémentaires comme le cryptage et bien plus encore. Pour en savoir plus sur l'accès à la console Core pour protéger les stations de travail et serveurs, voir « [Protection des machines](#) ».

Protection des machines

Après avoir configuré l'appliance et le Core, vérifiez que vous pouvez vous connecter aux machines que vous prévoyez de sauvegarder.

Pour protéger une machine

1. Naviguez jusqu'à la console Core, puis sélectionnez l'onglet **Machines**.
2. Dans le menu déroulant **Actions**, cliquez sur **Protéger la machiner**.
La boîte de dialogue **Connecter** s'affiche.
3. Dans la boîte de dialogue **Connecter**, entrez les informations de la machine à laquelle vous souhaitez vous connecter comme décrit dans le tableau suivant.

Hôte	Le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
Port	Le numéro du port sur lequel le Core communique avec l'agent sur la machine.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, administrateur.
Mot de passe	Le mot de passe utilisé pour se connecter à cette machine

4. Cliquez sur **Connecter**.
5. Si vous recevez un message d'erreur, l'appliance ne peut pas se connecter à la machine pour la sauvegarder. Pour résoudre le problème :
 - a. Vérifiez la connectivité réseau.
 - b. Vérifiez les paramètres du pare-feu.
 - c. Vérifiez que les services AppAssure et RPC sont en cours d'exécution.
 - d. Vérifiez les Recherches de service de nom de domaine (le cas échéant).

Vérification de la connectivité du réseau

Pour vérifier la connectivité réseau :

1. Ouvrez une interface de ligne de commande sur le système client auquel vous tentez de vous connecter.
2. Exécutez la commande **ipconfig** et notez l'adresse IP du client.
3. Ouvrez une interface de ligne de commande sur l'appliance.
4. Exécutez la commande **ping <adresse IP du client>**.
5. En fonction du résultat, effectuez l'une des actions suivantes :
 - Si le client ne répond pas au ping, vérifiez la connectivité et les paramètres réseau du serveur.
 - Si le client répond, vérifiez que les paramètres du pare-feu permettent aux composants DL1300 de s'exécuter.

Vérification des paramètres du pare-feu

Si le client est correctement connecté au réseau mais est invisible pour la console Core, vérifiez le pare-feu pour vous assurer que les communications entrantes et sortantes nécessaires sont autorisées.

Pour vérifier les paramètres de pare-feu du Core et de tous les clients qu'il sauvegarde :

1. Sur l'appliance DL1300, cliquez sur **Démarrer** → **Panneau de configuration**.
2. Dans le **Panneau de configuration**, cliquez sur **Système et sécurité**, sous **Pare-feu Windows** cliquez sur **Vérifier l'état du pare-feu**.
3. Cliquez sur **Paramètres avancés**.
4. Dans l'écran **Pare-feu Windows avec Sécurité avancée**, cliquez sur **Règles entrantes**.
5. Vérifiez que le Core et les ports indiquent **Oui** dans la colonne **Activé**.
6. Si la règle n'est pas activée, effectuez un clic droit sur le Core et sélectionnez **Activer la règle**.
7. Cliquez sur **Règles sortantes** et vérifiez les mêmes éléments pour le Core.

Vérification de la résolution DNS

Si l'ordinateur que vous tentez de sauvegarder utilise DNS, vérifiez que les recherches avant et arrière de DNS sont correctes.

Pour vous assurer que les recherches arrière sont correctes :

1. Sur l'appliance, accédez aux hôtes **C:\Windows\system32\drivers\etc**.
2. Saisissez l'adresse IP de chaque client sauvegardé sur DL1300.

Association de cartes réseau

Par défaut, les cartes réseau (NIC) de l'appliance DL1300 ne sont pas liées, ce qui affecte les performances du système. Il vous est recommandé d'associer les cartes réseau dans une interface unique. L'association des cartes réseau exige :


- Une réinstallation de Broadcom Advanced Control Suite
- Création de l'association NIC

Réinstallation de Broadcom Advanced Configuration Suite



Pour réinstaller Broadcom Advanced Configuration Suite :

1. Allez à **C:\Install\BroadcomAdvanced** et double-cliquez sur **Configuration**
L'**Assistant InstallShield** s'affiche.
2. Cliquez sur **Suivant**.
3. Cliquez sur **Modifier, Ajouter ou Supprimer**.
La fenêtre **Configuration personnalisée** s'affiche.
4. Cliquez sur **Fournisseur CIM**, puis sélectionnez **Cette fonction sera installée sur le disque dur local**.
5. Cliquez sur **BASP**, puis sélectionnez **Cette fonction sera installée sur le disque dur local**.
6. Cliquez sur **Suivant**.
7. Cliquez sur **Installer**.
8. Cliquez sur **Terminer**.

Création de l'association NIC

 **REMARQUE** : Il est conseillé de **ne pas** utiliser l'interface native de regroupement en équipes de Windows 2012 Server. Cet algorithme est optimisé pour le trafic sortant, pas pour le trafic entrant. Ses performances sont médiocres avec une charge de traitement de sauvegarde, même si l'association comprend davantage de ports réseau.

Pour associer les NIC :

1. Allez sur **Démarrer** → **Rechercher** → **Broadcom Advanced Control Suite**.
 **REMARQUE** : Ne sélectionnez que des cartes réseau Broadcom lorsque vous utilisez Broadcom Advanced Control Suite.
2. Dans **Broadcom Advanced Control Suite**, sélectionnez **Associations** → **Aller à la vue Association**.
3. Dans la **Liste d'hôtes** à gauche, effectuez un clic droit sur le nom d'hôte de l'appliance DL1300 et sélectionnez **Créer une association**.
La fenêtre **Assistant Association Broadcom** s'affiche.
4. Cliquez sur **Suivant**.
5. Saisissez un nom pour l'association, puis cliquez sur **Suivant**.
6. Sélectionnez le **Type d'association** et cliquez sur **Suivant**.
7. Sélectionnez une carte que vous souhaitez inclure à l'association et cliquez sur **Ajouter**.
8. Répétez ces étapes pour toutes les cartes faisant partie de l'association.
9. Lorsque toutes les cartes sont sélectionnées pour une association, cliquez sur **Suivant**.
10. Si l'association échoue, sélectionnez une carte réseau de secours si vous voulez une carte réseau qui peut être utilisée comme NIC par défaut.
11. Indiquez si vous souhaitez configurer **LiveLink** et cliquez sur **Suivant**.
12. Sélectionnez **Ignorer la gestion du VLAN** et cliquez sur **Suivant**.
13. Sélectionnez **Confirmer les modifications du système** et cliquez sur **Terminer**.
14. Cliquez sur **Oui** lorsque l'on vous avertit que la connexion réseau est interrompue.
 **REMARQUE** : La création de l'association de cartes réseau (NIC) peut prendre environ cinq minutes.

Réglage de flux simultanés

AppAssure est configuré par défaut pour autoriser trois flux simultanés vers l'appliance. Il est recommandé qu'il y ait un flux de plus que de machines (agents) que vous sauvegardez. Par exemple, si vous sauvegardez six agents, le nombre de **Transferts simultanés maximaux** doit être défini sur sept.

Pour modifier le nombre de flux simultanés :

1. Sélectionnez l'onglet **Configuration** puis cliquez sur **Paramètres**.
2. Sélectionnez **Modifier** dans **File d'attente de transferts**.
3. Modifiez le nombre de **Transferts simultanés maximaux** à un nombre qui dépasse le nombre de clients que vous sauvegardez d'au moins un.

Installation des agents sur les clients

L'agent AppAssure doit être installé sur chaque client sauvegardé par l'appliance AppAssure. La console AppAssure Core vous permet de déployer des agents sur des machines. Le déploiement d'agents sur des machines exige une préconfiguration des paramètres pour qu'un type unique d'agent à envoyer aux clients soit sélectionné. Cette méthode fonctionne bien si tous les clients utilisent le même système d'exploitation. Cependant, s'il existe plusieurs versions de systèmes d'exploitation, il peut être plus facile d'installer les agents sur les machines.

Vous pouvez également déployer le logiciel agent sur l'ordinateur agent au cours du processus de protection d'un ordinateur. Cette option est disponible pour les ordinateurs sur lesquels le logiciel Agent n'a pas encore été installé. Pour en savoir plus sur le déploiement du logiciel Agent tout en protégeant un ordinateur, voir le document *Dell DL1300 Appliance User's Guide* sur (**Guide de l'utilisateur de l'appliance Dell DL1300**) disponible sur Dell.com/support/home.


Installation à distance des agents (pousser)


Pour installer des agents à distance (pousser) :

1. Si le client exécute une version du système d'exploitation antérieure à Windows Server 2012, vérifiez que l'infrastructure Microsoft .NET 4 est installée sur le client :
 - a. Sur l'appliance, démarrez le **Windows Server Manager** (Gestionnaire de serveurs Windows).
 - b. Cliquez sur **Configuration** → **Services**.
 - c. Vérifiez que l'infrastructure Microsoft .NET s'affiche dans la liste de services.
Si elle n'est pas installée, vous pouvez en installer une copie depuis **microsoft.com**.
2. Vérifiez ou modifiez le chemin d'accès aux progiciels d'installation de l'agent :
 - a. Dans la console AppAssure Core, cliquez sur l'onglet **Configuration**, puis cliquez sur **Paramètres** dans le panneau de gauche.
 - b. Dans la zone **Paramètres de déploiement**, cliquez sur **Modifier**.
 - c. Saisissez les informations suivantes sur l'emplacement de l'agent :

Champ	Description
Nom du programme d'installation de l'agent	Spécifie le chemin exact au dossier\fichier de l'agent.


Champ	Description
Adresse du Core	Spécifie l'adresse IP de l'appliance exécutant l'AppAssure Core.

 **REMARQUE** : Par défaut, le champ **Adresse de Core** est vide. Le champ **Adresse de Core** n'exige aucune adresse IP car les fichiers d'installation sont installés sur l'appliance.

- d. Cliquez sur **OK**.
- Cliquez sur l'onglet **Outils**, puis cliquez sur **Déploiement en masse** dans le volet de gauche.
 -  **REMARQUE** : Si un agent est déjà installé sur le client, le programme d'installation vérifie la version de l'agent. Si l'agent que vous cherchez à pousser est plus récent que la version installée, le programme d'installation propose la mise à niveau de l'agent. Si la version actuelle de l'agent est installée sur l'hôte, le déploiement en masse lance la protection entre AppAssure Core et l'agent.
 - Dans la liste de clients, sélectionnez tous les clients et cliquez sur **Vérifier** pour vous assurer que l'ordinateur est actif et que l'agent peut être déployé.
 - Lorsque la colonne **Message** confirme que la machine est prête, cliquez sur **Déployer**.
 - Pour surveiller l'état du déploiement, sélectionnez l'onglet **Événements**.
Suite au déploiement de l'agent, une sauvegarde du client démarre automatiquement.

Déploiement du logiciel de l'agent lors de la protection d'une machine

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 :

- Accédez à la boîte de dialogue **Protéger une machine** → **Connecter**, après avoir entré les paramètres de connexion appropriés dans la boîte de dialogue.
- Cliquez sur **Connexion**.
La boîte de dialogue **Déployer l'agent** s'affiche.
- Cliquez sur **Oui** pour déployer à distance le logiciel d'agent sur l'ordinateur.
La boîte de dialogue **Déployer l'agent** s'affiche.
- Entrez les paramètres de connexion et de protection comme suit :
 - Nom d'hôte** : indique le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
 - Port** : indique le numéro du port sur lequel le Core communique avec l'agent sur l'ordinateur. La valeur par défaut est 8006.
 - Nom d'utilisateur** : indique le nom d'utilisateur utilisé pour établir la connexion à cet ordinateur, par exemple, administrateur.
 - Mot de passe** : indique le mot de passe utilisé pour se connecter à cet ordinateur.
 - Nom d'affichage** : précise pour la machine un nom qui s'affiche dans la console Core. Ce nom peut être identique au nom d'hôte.
 - Protéger la machine après l'installation** : si vous sélectionnez cette option, le DL1300 peut prendre un instantané de base des données dès que vous ajoutez la machine aux éléments à

protéger. Cette option est sélectionnée par défaut. Si vous la désélectionnez, vous devez forcer manuellement la prise d'un instantané lorsque vous êtes prêt à démarrer la protection des données. Pour en savoir plus sur le forçage manuel d'un instantané, voir la section relative au forçage d'un instantané dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

- **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.

5. 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.

Installation des agents Microsoft Windows sur le client

Pour installer les agents :

1. Vérifiez que l'infrastructure Microsoft .NET 4 est installée sur le client :
 - a. Sur l'appliance, démarrez le **Windows Server Manager** (Gestionnaire de serveurs Windows).
 - b. Cliquez sur **Configuration** → **Services**.
 - c. Vérifiez que l'infrastructure Microsoft .NET s'affiche dans la liste de services.
Si elle n'est pas installée, vous pouvez en obtenir une copie sur le site microsoft.com.
2. Installez l'agent :
 - a. Sur l'appliance AppAssure, partagez le répertoire **C:\install\AppAssure** avec le(s) client(s) que vous comptez sauvegarder.
 - b. Sur le système client, adressez un lecteur à **C:\install\AppAssure** sur l'appliance AppAssure.
 - c. Sur le système client, ouvrez le répertoire **C:\install\AppAssure** et double-cliquez sur l'agent correct du système client pour démarrer l'installation.


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

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

Pour ajouter un agent :

1. Dans l'écran d'**Accueil du portail de licences d'AppAssure 5**, sélectionnez un groupe, puis cliquez sur **Télécharger un agent**.
La boîte de dialogue **Télécharger un agent** s'affiche.
2. Cliquez sur **Télécharger**, en regard de la version du programme d'installation à télécharger.
Choisissez parmi les options suivantes :
 - Programme d'installation Windows 32 bits
 - Programme d'installation Windows 64 bits
 - Programme d'installation Red Hat Enterprise Linux 6.3 32 bits


- Programme d'installation Red Hat Enterprise Linux 6.3 64 bits
- Programme d'installation CentOS 6.3, 6.4 32 bits
- Programme d'installation CentOS 6.3, 6.4 64 bits
- Programme d'installation Ubuntu 12.04 LTS, 13.04 32 bits
- Programme d'installation Ubuntu 12.04 LTS, 13.04 64 bits
- Programme d'installation SUSE Linux Enterprise Server 11 SP2 32 bits
- Programme d'installation SUSE Linux Enterprise Server 11 SP2, SP3 64 bits
- Microsoft Hyper-V Server 2012

 **REMARQUE** : Dell prend en charge les distributions Linux ci-dessus et a testé les versions de noyau publiées.

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


Le fichier **Agent** se télécharge.

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

 **REMARQUE** : Pour en savoir plus sur l'ajout d'agents à l'aide de la machine Core, voir la section relative au déploiement d'un agent (Installation en mode Push) dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur [Dell.com/support/home](https://dell.com/support/home).

Installation d'agents sur des ordinateurs Linux

Téléchargez le programme d'installation 32 bits ou 64 bits propre à la distribution utilisée sur chaque serveur Linux à protéger avec le Core. Vous pouvez télécharger les programmes d'installation depuis le portail de licences, à l'adresse <https://licenseportal.com>. Pour en savoir plus, voir « [Ajout d'un agent à l'aide du portail de licences](#) ».

 **REMARQUE** : La sécurité liée à la protection d'un ordinateur est basée sur le Pluggable Authentication Module (PAM) sous Linux. Suite à l'authentification d'un utilisateur à l'aide de **libpam**, l'utilisateur est autorisé à protéger l'ordinateur uniquement si celui-ci appartient à l'un des groupes suivants :

- sudo
- admin
- appassure
- wheel

Pour en savoir plus sur la protection d'un ordinateur, voir la section relative à la protection d'un ordinateur dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur [Dell.com/support/home](https://dell.com/support/home).

Les instructions d'installation diffèrent en fonction de la distribution Linux que vous utilisez. Pour en savoir plus sur l'installation de l'agent Linux sur votre distribution, voir la section suivante :

- [Installation de l'agent sur Ubuntu](#)
- [Installation de l'agent sur Red Hat Enterprise Linux et CentOS](#)
- [Installation de l'agent sur SUSE Linux Enterprise Server](#)

 **REMARQUE** : L'installation de l'agent Linux contourne toutes les règles de pare-feu qui n'ont pas été appliquées au moyen de UFW, Yast2 ou **system-config-firewall**.

Si vous avez ajouté manuellement des règles de pare-feu, vous devez ajouter manuellement des ports AppAssure après l'installation. Une sauvegarde des règles existantes sera écrite dans **/var/lib/appassure/backup.fwl**.

Vous devez ajouter des exceptions de pare-feu sur tous les serveurs exécutant l'agent, pour les ports TCP 8006 et 8009, afin que le Core puisse accéder aux agents.

Emplacement des fichiers de l'agent Linux

Les fichiers de l'agent Linux se trouvent dans les répertoires suivants de toutes les distributions :

Composant	Emplacement/Chemin
mono	<code>/opt/appassure/mono</code>
agent	<code>/opt/appassure/aagent</code>
aamount	<code>/opt/appassure/amount</code>
aavdisk et aavdctl	<code>/usr/bin</code>
fichiers de configuration de aavdisk	<code>/etc/appassure/aavdisk.conf</code>
wrappers pour aamount et agent	<ul style="list-style-type: none"><code>/usr/bin/aamount</code><code>/usr/bin/aagent</code>
scripts d'exécution automatique pour aavdisk et agent	<ul style="list-style-type: none"><code>/etc/init.d/appassure-agent</code><code>/etc/init.d/appassure-vdisk</code>

Dépendances de l'agent

Les dépendances suivantes sont requises et installées dans le cadre du progiciel du programme d'installation de l'agent :

Pour Ubuntu	Dépendance
L'appassure-vss exige	<code>dkms, gcc, make, linux-headers-`uname-r`</code>
L'appassure-aavdisk exige	<code>libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3</code>
L'appassure-mono exige	<code>libc6 (>=2.7-18)</code>

Pour Red Hat Enterprise Linux et CentOS

Dépendance


Le nbd-dkms exige	dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`
L'appassure-vss exige	dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`
L'appassure-aavdisk exige	nbd-dkms, libblkid, pam, pcre
L'appassure-mono exige	glibc >=2.11

Pour SUSE Linux Enterprise Server

Dépendance

Le nbd-dkms exige	dkms, gcc, make, kernel-syms
L'appassure-vss exige	dkms, kernel-syms, gcc, make
L'appassure-aavdisk exige	libblkid1, pam, pcre
L'appassure-mono exige	glibc >=2.11


Installation de l'agent sur Ubuntu

 **REMARQUE** : Avant d'effectuer ces étapes, assurez-vous d'avoir téléchargé le progiciel du programme d'installation spécifique à Ubuntu dans **/home/system directory**.

Pour installer l'agent sous Ubuntu :

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent, saisissez la commande suivante :
`chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

Le fichier devient exécutable.

 **REMARQUE** : Pour les environnements 32 bits, le programme d'installation est nommé `appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh`


3. Pour extraire et installer l'agent, saisissez la commande suivante :
`/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

L'agent Linux démarre son processus d'extraction et d'installation. Tout progiciel ou fichier manquant requis par l'agent est téléchargé et installé automatiquement dans le cadre du script.

 **REMARQUE** : Pour en savoir plus sur les fichiers dont l'agent a besoin, voir « [Dépendances de l'agent](#) ».


Une fois le programme d'installation terminé, l'agent Ubuntu est installé sur votre machine. Pour en savoir plus sur la protection de cette machine avec le Core, voir la rubrique relative à la protection des stations de travail et des serveurs dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

Installation de l'agent sur Red Hat Enterprise Linux et CentOS

 **REMARQUE** : Avant d'effectuer ces étapes, assurez-vous d'avoir téléchargé le progiciel d'installation Red Hat ou CentOS dans **/home/system directory**. Les étapes suivantes sont identiques pour les environnements 32 bits et 64 bits.

Pour installer un agent sur Red Hat Enterprise Linux et CentOS :

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent, saisissez la commande suivante :
`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

 **REMARQUE** : Pour les environnements 32 bits, le programme d'installation est nommé `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`.

Le fichier devient exécutable.


3. Pour extraire et installer l'agent, saisissez la commande suivante :
`/appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

L'agent Linux démarre son processus d'extraction et d'installation. Tout progiciel ou fichier manquant requis par l'agent est téléchargé et installé automatiquement dans le cadre du script.

Pour en savoir plus sur les fichiers dont l'agent a besoin, voir « [Dépendances de l'agent](#) ».

Une fois le programme d'installation terminé, l'agent s'exécute sur votre machine. Pour en savoir plus sur la protection de cette machine avec le Core, voir la rubrique relative à la protection des stations de travail et des serveurs dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

Installation de l'agent sur SUSE Linux Enterprise Server

 **REMARQUE** : Avant d'effectuer ces étapes, assurez-vous d'avoir téléchargé le progiciel d'installation SUSE Linux Enterprise Server (SLES) dans le **/home/system directory**. Les étapes suivantes sont identiques pour les environnements 32 bits et 64 bits.

Pour installer l'agent sur SLES :

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent DL1300, saisissez la commande suivante :
`chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.



REMARQUE : Pour les environnements 32 bits, le programme d'installation est nommé `appassureinstaller__sles_i386_5.x.x.xxxxx.sh`

Le fichier devient exécutable.

3. Pour extraire et installer l'agent DL1300, saisissez la commande suivante :

`/appassure-installer_sles_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

L'agent Linux démarre son processus d'extraction et d'installation. Tout progiciel ou fichier manquant requis par l'agent est téléchargé et installé automatiquement dans le cadre du script.

Pour en savoir plus sur les fichiers dont l'agent a besoin, voir « [Dépendances de l'agent](#) ».

4. Lorsque vous êtes invité à installer les nouveaux progiciels, tapez `y` et appuyez sur <Entrée>.
Le système termine le processus d'installation.

Une fois le programme d'installation terminé, l'agent s'exécute sur votre ordinateur. Pour savoir comment protéger cet ordinateur à l'aide du Core, voir la section relative à la protection des stations de travail et serveurs dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home

Scénarios d'utilisation courants

Cette section montre les cas d'utilisation les plus courants du DL1300, et fournit une présentation de haut niveau des informations et procédures nécessaires pour chaque scénario. Le cas échéant, des références à des informations supplémentaires sont fournies.

Protection des machines

La technologie de réplication et de sauvegarde AppAssure offre une protection avancée pour vos machines virtuelles ou serveurs, tout en offrant une grande flexibilité dans la restauration des applications et des données. Lorsqu'une machine est protégée, des instantanés de données complets et incrémentiels sont capturés et stockés dans le référentiel. Le processus de protection AppAssure exploite deux technologies principales : les instantanés et l'agent intelligent Dell DL1300 qui sont décrits ci-dessous.

Instantanés


L'agent AppAssure pour Windows utilise Microsoft VSS (Volume Shadow copy Service, service de copie fantôme de volume) pour figer et mettre au repos les données d'application sur disque, afin de capturer une sauvegarde cohérente avec le système de fichiers et avec l'application. Pendant la création d'un instantané, le module d'écriture VSS du serveur cible interdit l'écriture de contenu sur le disque. Au cours de ce processus de blocage de l'écriture du contenu sur disque, toutes les opérations d'E/S sur disque sont mises en file d'attente et reprennent uniquement lorsque l'instantané a été capturé, tandis que les opérations déjà en cours sont terminées et que tous les fichiers ouverts sont fermés. Pour en savoir plus, voir la rubrique « [Processus d'instantané](#) ».

Agents intelligents DL1300

L'agent intelligent est installé sur les machines protégées par le Core DL1300. L'agent intelligent effectue le suivi des modifications apportées aux blocs du volume de disque et prend un instantané des blocs modifiés selon l'intervalle de protection prédéfini. L'approche incrémentielle à base d'instantanés de niveau bloc empêche la copie répétée des mêmes données de la machine protégée vers le Core. Lorsque l'instantané est prêt, il est rapidement transféré vers le Core à l'aide connexions par socket multithreads intelligentes. Pour en savoir plus, voir la rubrique [Agent intelligent Dell DL1300](#).

Déploiement d'agents intelligents

Vous devez installer le programme d'installation de l'agent AppAssure sur toutes les machines de votre environnement protégées par le DL1300.

 **REMARQUE** : Ce document fournit un résumé de ces procédures. Pour en savoir plus ou obtenir des instructions spécifiques pour les agents Linux, voir le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300).

Étape 1 : Obtention du logiciel d'agent


Vous pouvez obtenir le logiciel d'agent intelligent avec l'une des méthodes suivantes :

- **Téléchargement depuis le Core AppAssure** : connectez-vous à la console Core et téléchargez le logiciel sur la machine d'agent. Sélectionnez **Téléchargements** dans l'onglet **Outils**, puis téléchargez le programme d'installation Web du composant Agent.
- **Téléchargement depuis le portail de licences AppAssure** : si vous avez inscrit votre logiciel dans le portail de licences logicielles Dell, vous pouvez vous connecter à ce portail et télécharger le logiciel sur la machine d'agent.
- **Déploiement du logiciel d'agent lors de la protection d'une machine** : vous pouvez déployer le logiciel d'agent sur la machine à protéger à l'aide de l'**Assistant Protéger une machine**.
- **Utilisation de la fonction Déploiement en masse** : si le Core est installé, vous pouvez déployer le logiciel d'agent sur plusieurs machines à l'aide de la fonction **Déploiement en masse**, accessible dans l'onglet **Outils** de la console Core.


Étape 2 : Installation du logiciel d'agent

Lancez le programme d'installation en suivant la procédure décrite ci-après pour installer le logiciel sur chaque machine à protéger dans le Core. Pour installer le logiciel d'agent sur des machines Windows :


1. Depuis la machine à protéger, double-cliquez sur le fichier du programme d'installation de l'agent.
2. Dans la page d'**Accueil**, cliquez sur **Suivant** pour poursuivre l'installation.
3. Dans l'écran **Contrat de licence**, sélectionnez **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.

 **REMARQUE** : Le programme d'installation de l'agent vérifie l'existence des fichiers prérequis. Si ces fichiers n'existent pas, le programme d'installation de l'agent identifie les fichiers nécessaires et affiche les résultats ; par exemple, « Types CLR Microsoft System pour SQL Server 2008 R2 (x64) ».

4. Cliquez sur **Installer les prérequis**.
5. Une fois les fichiers prérequis installés, cliquez sur **Suivant**.
6. Dans l'écran **Options d'installation**, passez en revue les options choisies. Si nécessaire, modifiez-les comme indiqué ci-dessous :
 - a. Dans le champ **Dossier de destination**, vérifiez le dossier de destination choisi pour l'installation. Pour modifier cet emplacement, procédez comme suit :
 - Cliquez sur l'icône de dossier.
 - Dans la boîte de dialogue **Rechercher le dossier de destination**, sélectionnez le nouvel emplacement. Cliquez sur **OK**.
 - b. Dans le champ **Numéro de port**, entrez le numéro de port à utiliser pour les communications entre l'agent et le Core.


 **REMARQUE** : La valeur par défaut est 8006. Si vous avez changé le numéro de port, notez-le au cas où vous devriez ajuster les paramètres de configuration ultérieurement.

7. Vérifiez les options d'installation et cliquez sur **Installer**. Une fois l'installation terminée, la page **Terminé** s'affiche.
8. Sélectionnez l'une des options suivantes, puis cliquez sur **Terminer** : Oui, je veux redémarrer mon ordinateur maintenant ou Non, je redémarrerai mon ordinateur plus tard.

 **REMARQUE** : Vous devez redémarrer votre système avant d'utiliser le logiciel d'agent.


Configuration des tâches de protection

Lorsque vous ajoutez une protection, vous devez définir des informations de connexion, telles que l'adresse IP et le port. Vous devez aussi fournir des informations d'identification pour la machine à protéger. (Facultatif) Vous pouvez fournir le nom d'affichage à utiliser dans la console Core à la place de l'adresse IP. Vous définissez également la planification de protection de la machine.

 **REMARQUE** : Ce document fournit un résumé de ces procédures. Pour en savoir plus, voir le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

Protection d'une machine

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

 **REMARQUE** : Vous devez avoir installé le logiciel d'agent AppAssure sur la machine pour pouvoir la protéger. Vous pouvez choisir d'installer l'agent avant de réaliser cette procédure, ou de le déployer pendant que vous définissez la protection dans la boîte de dialogue **Connexion**. Pour installer le logiciel d'agent pendant le processus de protection de la machine, voir la rubrique relative au déploiement du logiciel d'agent lors de la protection d'un agent dans le manuel « *Dell DL1300 Appliance User's Guide* » (Guide de l'utilisateur de l'appliance Dell DL1300).

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 la rubrique relative à la protection de plusieurs machines dans le manuel « *Dell DL1300 Appliance User's Guide* » (Guide de l'utilisateur de l'appliance Dell DL1300).

Pour protéger une machine

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 de boutons.
L'**Assistant Protection d'une machine** s'affiche.
3. Dans la page **Accueil**, 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 pas voir la page **Accueil** de l'**Assistant Protection d'une machine** à l'avenir, sélectionnez l'option **Ignorer cette page d'accueil à la prochaine ouverture de l'Assistant**.
4. Cliquez sur **Suivant**.
5. Dans la page **Connexion**, entrez les informations concernant la machine à 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 l'AppAssure Core communique avec l'agent sur la machine. Le numéro de port par défaut est 8006.

Zone de texte Description

Nom d'utilisateur Le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, administrateur.

Mot de passe Le mot de passe utilisé pour se connecter à cette machine

6. Cliquez sur **Suivant**. Si la page **Protection** apparaît ensuite dans l'**Assistant Protection d'une 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, accédez à l'option **Paramètres de planification** et sélectionnez **Protection par défaut (instantanés toutes les 3 heures de tous les volumes)**. Avec la planification de protection par défaut, le Core prend des instantanés de la machine d'agent toutes les 3 heures. Ces instantanés peuvent être capturés toutes les heures (valeur minimale). Pour modifier les paramètres de protection, à tout moment après avoir fermé l'Assistant, notamment choisir les volumes à protéger, accédez à l'onglet Résumé de la machine d'agent.
- 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 l'option Typique dans l'**Assistant Protection d'une machine** et choisi la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine spécifiée.
- Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (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.
- 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 d'une machine** et choisi la protection personnalisée, cliquez sur **Suivant** et passez à l'étape 10 pour choisir les volumes à protéger.

10. Dans **Volumes de protection**, sélectionnez les volumes de la machine d'agent que vous souhaitez protéger. Si la liste contient des volumes que vous ne voulez pas inclure dans la protection, cliquez dans la colonne de cases à cocher pour effacer la sélection. Cliquez ensuite sur **Suivant**.

 **REMARQUE** : 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. (Facultatif) Pour activer le 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 sur la machine d'agent concernée. Vous pourrez modifier ultérieurement ces paramètres dans l'onglet Configuration de la console Core AppAssure 5.



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 cryptage.
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 (à savoir un instantané de toutes les données des volumes protégés) est transférée vers le référentiel sur l'AppAssure Core en fonction de l'horaire que vous avez défini, sauf si vous avez demandé la suspension initiale de la protection.

Restauration de données

Avec le DL1300, les données sont protégées sur les machines Windows et Linux. Les sauvegardes des machines protégées sont enregistrées sur le Core sous forme de points de restauration qui peuvent servir à restaurer vos données. Il est possible de restaurer des volumes entiers, remplacés à partir d'un point de restauration sur les machines cibles. Pour restaurer les données à partir des points de restauration, vous pouvez choisir l'une des méthodes suivantes :

- Restauration de fichiers et de dossiers
- Restauration de volumes de données à l'aide de Live Recovery
- Restauration sans système d'exploitation à l'aide d'Universal Recovery

Restauration de répertoires ou de fichiers

Vous pouvez utiliser l'Explorateur Windows pour copier et coller des fichiers et répertoires à partir d'un point de restauration monté vers une machine Windows. Cette fonction peut être utile lorsque vous souhaitez distribuer une partie seulement d'un point de restauration à vos utilisateurs. Lorsque vous


copiez des fichiers et répertoires, les autorisations d'accès de l'utilisateur qui effectue l'opération de copie sont utilisées et appliquées à ces répertoires et fichiers.

Pour restaurer un répertoire ou un fichier à l'aide de l'Explorateur Windows :


1. Montez le point de restauration qui contient les données à restaurer. Pour en savoir plus, voir la rubrique relative au montage d'un point de restauration pour une machine Windows dans le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300).
2. Dans l'Explorateur Windows, naviguez vers le point de restauration monté, puis sélectionnez les fichiers et répertoires à restaurer. Faites un clic droit et sélectionnez **Copier**.
3. Dans l'Explorateur Windows, accédez à l'emplacement de la machine où restaurer les données. Effectuez un clic droit et sélectionnez **Coller**.

Restauration de volumes


Dans la console Core, vous pouvez restaurer des volumes entiers à partir d'un point de restauration d'un volume non système, en remplaçant les volumes sur la machine de destination.

 **REMARQUE** : La procédure suivante est une présentation simplifiée du processus de restauration. Pour consulter des informations ou des procédures détaillées sur les autres options de restauration, voir la rubrique relative à la restauration de volumes à partir d'un point de restauration » dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300).

Pour restaurer des volumes à partir d'un point de restauration :

1. Dans la console Core, cliquez sur l'onglet **Restaurer**.
L'**Assistant Restaurer une machine** s'affiche.
2. Dans la page **Machines protégées**, sélectionnez la machine protégée dont vous souhaitez restaurer les données, puis cliquez sur **Suivant**.
 **REMARQUE** : Le logiciel d'agent doit être installé sur la machine protégée et cette machine doit contenir les points de restauration que vous prévoyez d'utiliser pour 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 d'agent.
 **REMARQUE** : Si nécessaire, utilisez les boutons de navigation au bas de la page pour afficher d'autres points de restauration. Vous pouvez aussi limiter la quantité de points de restauration affichés dans la page Points de restauration de l'Assistant, en filtrant l'affichage sur la base du volume (si cette option est définie) 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 sur laquelle restaurer les données, comme suit :
 - Si vous voulez restaurer les données du point de restauration sélectionné sur la même machine d'agent (par exemple, Machine1) et que les volumes à restaurer n'incluent pas le volume système, sélectionnez **Restaurer sur une machine protégée (volumes non système uniquement)**, vérifiez que la machine de destination (Machine1) est sélectionnée, puis cliquez sur **Suivant**. La page Mappage des volumes s'affiche. Passez à l'étape 6.
 - Pour restaurer les données du point de restauration sélectionné sur une autre machine protégée (par exemple, pour remplacer le contenu de Machine2 par les données de Machine1), sélectionnez **Restaurer sur une machine protégée (volumes non système uniquement)**, sélectionnez la machine de destination dans la liste (par exemple, Machine2), puis cliquez sur **Suivant**. La page Mappage des volumes s'affiche. Passez à l'étape 6.

- Pour effectuer la restauration à partir d'un point de restauration sur un volume système (par exemple, le lecteur C de la machine d'agent Machine1), vous devez effectuer une restauration sans système d'exploitation (BMR).
6. Sur la page Mappage des volumes, pour chaque volume du point de restauration à restaurer, sélectionnez le volume de destination approprié. Pour ne pas restaurer un volume particulier, dans la colonne Volumes, sélectionnez **Ne pas restaurer**.
 7. Sélectionnez **Afficher les options avancées**, puis procédez comme suit :
 - Pour restaurer les données sur des machines Windows, vous pouvez sélectionner **Live Recovery** (Restauration en direct) pour utiliser cette fonction.
Avec la technologie de restauration instantanée Live Recovery d'AppAssure 5, vous pouvez récupérer ou restaurer immédiatement les données sur vos machines physiques ou virtuelles à partir des points de restauration stockés des machines Windows, y compris les espaces de stockage Microsoft Windows. Live Recovery n'est pas disponible pour les machines Linux.
 - Pour forcer le démontage, sélectionnez **Forcer le démontage**.
Si vous ne forcez pas le démontage avant la restauration des données, la restauration peut échouer avec l'erreur « Volume en cours d'utilisation ».

La machine d'agent, si elle est démarrée sur le CD d'amorçage, affiche l'interface Universal Recovery Console (URC). Cet environnement est utilisé pour restaurer le lecteur système ou les volumes sélectionnés directement depuis le Core. Notez l'adresse IP et les informations d'identification de la clé d'authentification dans l'URC ; ces données sont actualisées chaque fois que vous démarrez à partir du CD d'amorçage.

8. Si les volumes à restaurer contiennent des bases de données SQL ou Microsoft Exchange, la page **Démonter les bases de données** vous invite à démonter ces bases. (Facultatif) 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**.
9. Cliquez sur **OK** pour confirmer le message d'état indiquant que le processus de restauration a commencé.
10. Pour surveiller l'avancement de votre action de restauration, dans la console Core, cliquez sur **Événements**.

Restauration sans système d'exploitation (BMR)

AppAssure offre la possibilité d'effectuer une restauration sans système d'exploitation (BMR) de vos machines Windows ou Linux. Le processus BMR permet de restaurer la configuration logicielle complète d'un système spécifique. Nous utilisons l'expression « sans système d'exploitation », car l'opération de restauration non seulement restaure les données à partir du serveur, mais également reformate le disque dur, et réinstalle le système d'exploitation et toutes les applications logicielles. Pour effectuer une restauration sans système d'exploitation (BMR), vous spécifiez un point de restauration provenant d'une machine protégée, et restaurez (rollback) les données sur la machine physique ou virtuelle indiquée. Les autres situations où vous pouvez choisir la restauration BMR sont la mise à niveau matérielle ou le remplacement d'un serveur.

Il est possible d'exécuter une restauration sans système d'exploitation (BMR) pour des machines physiques ou virtuelles. Par ailleurs, AppAssure vous permet d'effectuer une restauration BMR que les matériels source et cible soient identiques ou différents.

Conditions requises pour l'exécution d'une restauration BMR d'une machine Windows

Avant de démarrer une restauration sans système d'exploitation d'une machine Windows, vous devez vous assurer que les conditions et critères suivants existent :

- **Sauvegardes de la machine à restaurer** : vous devez disposer d'un AppAssure Core fonctionnel contenant les points de restauration du serveur protégé à restaurer.
- **Matériel à restaurer (nouveau ou ancien, similaire ou non)** : la machine cible doit respecter la configuration requise pour l'installation de l'agent.
- **Image multimédia et logiciels** : vous devez disposer d'un CD/DVD vierge et d'un logiciel de gravure de CD, ou de logiciels pour créer une image ISO. Si vous gérez les machines à distance avec un logiciel informatique en réseau virtuel comme UltraVNC, vous devez disposer de la visionneuse VNC.
- **Pilotes de stockage et pilotes de carte réseau compatibles** : pour la restauration sur un matériel différent, vous devez disposer de pilotes de stockage et de pilotes de carte réseau compatibles Windows 7 PE (32 bits) pour la machine cible, y compris les pilotes RAID, AHCI et de jeu de puces pour le système d'exploitation cible, le cas échéant.
- **Espace disque et partitions de stockage, selon les besoins** : vérifiez 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 avoir une capacité supérieure ou égale à celle de la partition source d'origine.
- **Partitions compatibles** : les systèmes d'exploitation Windows 8 et Windows Server 2012 amorcés sur des partitions FAT32 EFI peuvent faire l'objet d'une protection ou d'une restauration, de même que les volumes Resilient File System (ReFS). Les partitions UEFI sont considérées comme de simples volumes FAT32. Les transferts incrémentiels sont entièrement pris en charge et protégés. AppAssure 5 prend en charge les systèmes UEFI pour la restauration sans système d'exploitation (BMR), y compris le partitionnement automatique des disques GPT.

Stratégie d'exécution d'une restauration sans système d'exploitation d'une machine Windows

 **REMARQUE** : Voici les étapes de base de la restauration sans système d'exploitation (BMR). Pour en savoir plus sur chaque étape, voir le document *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300).

Pour effectuer une BMR d'une machine 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. Adressez les volumes.
6. Lancez la restauration.
7. Surveillez l'avancement.

Réplication de points de restauration

La réplication est un processus consistant à copier des points de restauration et à transférer ces points vers un emplacement secondaire à des fins de récupération après sinistre. Ce processus exige une

relation de paire source-cible entre deux Cores. Le Core source copie les points de restauration des agents protégés, puis les transmet en continu en mode asynchrone à un Core cible situé sur un site distant de récupération après sinistre. L'emplacement hors site peut être un centre de données appartenant à l'entreprise (Core autogéré), le site d'un fournisseur tiers de services gérés (MSP) ou un emplacement dans le Cloud. Si vous effectuez 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 de commentaires automatiques.


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

Configuration de votre environnement

Si la bande passante entre le Core source et le Core cible ne peut pas gérer le transfert des points de restauration stockés, la réplication commence par la création de la valeur de départ du Core cible avec des images de base et des points de restauration provenant des serveurs sélectionnés protégés sur le Core source. Le processus de création de la valeur de départ peut être réalisé à n'importe quel moment, que ce soit lors du transfert initial des données à utiliser comme base pour la réplication planifiée récurrente, ou bien pour la répétition de la réplication pour une machine précédemment répliquée dont la réplication a été suspendue ou supprimée. Dans ce cas, l'option Créer une chaîne de RP vous permet de copier les points de restauration non encore répliqués pour un lecteur de départ.

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

- **Vitesse de modification** : la vitesse de modification est la vitesse à laquelle la quantité de données protégées s'accumule. La vitesse dépend de la quantité de données qui change sur les volumes protégés et de l'intervalle de protection de ces volumes. Si un ensemble de blocs change dans le volume, la réduction de l'intervalle de protection réduit la vitesse de modification.
- **Bande passante** : la bande passante est la vitesse de transfert disponible entre le Core source et le Core cible. Il est crucial que la bande passante soit supérieure à la vitesse de modification pour que la réplication suive le rythme des points de restauration créés par les instantanés. Étant donné la quantité de données transmises de Core à Core, plusieurs flux parallèles peuvent être nécessaires pour réaliser ces transferts à des vitesses filaires atteignant le débit d'une connexion 1 Gbit Ethernet.

 **REMARQUE** : La bande passante spécifiée par l'ISP est la bande passante totale disponible. La bande passante sortante est partagée par tous les périphériques sur le réseau. Assurez-vous qu'il y ait suffisamment de bande passante libre pour que la réplication corresponde à la vitesse de modification.

- **Nombre d'agents** : il est important de prendre en compte le nombre d'agents protégés par chaque Core source et le nombre que vous planifiez de répliquer vers la cible. Le DL1300 permet d'effectuer

la réplication pour un seul serveur protégé à la fois, ce qui permet de répliquer certains serveurs uniquement. Si tous les serveurs protégés doivent être répliqués, l'opération affecte considérablement la vitesse de modification, en particulier si la bande passante entre les Cores source et cible est insuffisante pour la quantité et la taille des points de restauration que vous répliquez.

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


La vitesse de modification maximale pour les types de connexion WAN est affichée dans le tableau ci-dessous, avec des exemples de la bande passante par gigaoctet nécessaire pour une vitesse de modification correcte.

Tableau 2. Vitesse de modification maximale pour des types de connexion WAN.

Large bande	Bande passante	Vitesse de modification maximale
DSL	768 Kbits/s et plus	330 Mo par heure
Câble	1 Mbit/s et plus	429 Mo par heure
T1	1,5 Mbits/s et plus	644 Mo par heure
Fibre	20 Mbit/s et plus	8,38 Go par heure

Pour des résultats optimaux, suivez les recommandations du tableau ci-dessus. Si une liaison échoue pendant le transfert des données, la réplication reprend à partir du point où le transfert précédent a échoué, une fois la liaison restaurée et opérationnelle.

Étapes de configuration de la réplication

 **REMARQUE** : Les informations ci-dessous présentent de manière générale les étapes nécessaires pour effectuer la réplication. Pour consulter les procédures complètes, consultez le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur dell.com/support/home.

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 d'agent, surveiller et gérer la réplication et effectuer des restaurations. La réplication avec AppAssure inclut les opérations suivantes :

- **Configuration de la réplication autogérée** : pour en savoir plus sur la réplication vers un Core cible autogéré, voir la rubrique relative à la réplication vers un Core cible autogéré dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Configuration de la réplication tierce** : pour en savoir plus sur la réplication vers un Core cible tiers, voir la rubrique relative au processus de réplication vers un Core cible tiers dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Réplication d'un agent existant** : pour en savoir plus sur la réplication d'un agent déjà protégé par le Core source, voir la rubrique relative à l'ajout d'une machine à une réplication existante, dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Consommation du lecteur de départ** : pour en savoir plus sur la consommation des données de lecteur de départ sur le Core cible, voir la rubrique relative à la consommation du lecteur de départ


sur un Core cible dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home

- **Définition de la priorité de réplication d'un agent** : pour en savoir plus sur la définition des priorités de réplication des agents, voir la rubrique relative à la définition de la priorité de réplication d'un agent dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home
- **Définition de la planification de réplication d'un agent** : pour en savoir plus sur la définition d'une planification de réplication, voir la rubrique relative à la planification de la réplication dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Surveillance de la réplication si nécessaire** : pour en savoir plus sur la surveillance de la réplication, voir la rubrique relative à la surveillance de la réplication dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Gestion des paramètres de réplication à la demande** : pour en savoir plus sur la gestion des paramètres de réplication, voir la rubrique relative à la gestion des paramètres de réplication » dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.
- **Restauration des données répliquées en cas de sinistre ou de perte de données** : pour en savoir plus sur la restauration des données répliquées, voir la rubrique relative à la restauration des données répliquées dans le manuel *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur Dell.com/support/home.

Utilisation de disques virtuels de secours

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

Lorsque vous exportez les données vers une machine virtuelle, toutes les données de sauvegarde d'un point de restauration, ainsi que les paramètres définis pour la planification de protection de votre machine sont exportés. Vous pouvez également créer un « disque de secours virtuel » en exportant en continu les données protégées de votre machine protégée vers une machine virtuelle.

 **REMARQUE** : Seule la configuration du DL1300 de 3 To avec 2 machines virtuelles et de 4 To avec 2 machines virtuelles prend en charge l'exportation ponctuelle et l'exportation en continu sur les VM de disque de secours virtuel.

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 DL1300 de 3 To avec 2 machines virtuelles et de 4 To avec 2 machines virtuelles prennent en charge l'exportation ponctuelle et l'exportation en continu sur les VM de 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** .

Gestion des points de restauration

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

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 3. 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 d'abord ajouter ce compte à Core Console. Voir la rubrique relative à l'ajout d'un compte Cloud dans le document <i>Dell DL1300 Appliance User's Guide</i> (Guide de l'utilisateur de l'appliance Dell DL1300).
	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 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	<p>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 :</p> <ul style="list-style-type: none">• 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. <p> 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.</p>
Action de recyclage	<p>Sélectionnez l'une des options d'action de recyclage suivantes :</p> <ul style="list-style-type: none">• 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	<p>Entrez toutes les informations supplémentaires dont la capture est nécessaire pour l'archive. Le commentaire s'affiche si vous importez l'archive ultérieurement.</p>
Utiliser un format compatible	<p>Sélectionnez cette option pour archiver vos données dans un format compatible avec les versions précédentes des Cores.</p> <p> REMARQUE : Le nouveau format offre de meilleures performances, mais n'est pas compatible avec les anciens Cores.</p>

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**.

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, voir la rubrique relative à l'ajout d'un compte Cloud dans le manuel « *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible sur **Dell.com/support/home** ».
- Archivez vos données et exportez-les vers votre compte Cloud. Pour en savoir plus, voir la rubrique relative à la création d'une archive dans le manuel « *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible) disponible sur **Dell.com/support/home** ».
- Restaurez les données archivées en les important depuis l'emplacement de Cloud. Pour en savoir plus, voir la rubrique relative à l'importation d'une archive dans le manuel « *Dell DL1300 Appliance User's Guide* (Guide de l'utilisateur de l'appliance Dell DL1300) disponible) disponible sur **Dell.com/support/home** ».

Obtention d'aide

Recherche de documentation et de mises à jour logicielles

Des liens d'accès direct à la documentation de l'appliance DL1300 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**.

Contacteur Dell

 **REMARQUE** : Si vous ne disposez pas d'une connexion Internet, les informations de contact figurent sur la facture d'achat, le bordereau de colisage, la facture le catalogue des produits Dell.

Dell fournit plusieurs options de service et de support en ligne et par téléphone. Si vous ne disposez pas d'une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, facture ou catalogue de produits Dell. La disponibilité des produits varie selon le pays et le produit. Il se peut que certains services ne soient pas disponibles dans votre région.

Commentaires sur la documentation

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