Appliance Dell DL1000

Guide de déploiement

DELL EMC

Remarques, précautions et avertissements

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

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 - 09

Rév. A03

Table des matières

1 Présentation de votre DL1000 Dell 5
Technologies de base du DL1000 5
Récupération en direct 5
Récupération universelle 5
Déduplication globale réelle 6
Cryptage 6
Fonctions de protection des données du Dell DL1000 6
Dell DL1000 Core 6
Agent intelligent Dell DL1000 7
Processus d'instantané 7
Réplication : site de reprise après sinistre ou fournisseur de services 7
Récupération 8
Recovery-as-a-Service 8
Virtualisation et cloud 8
Architecture de déploiement du Dell DL1000 8
Autres informations utiles 10

2 Installer votre DL1000 Dell 11
Introduction 11
Configurations disponibles 11
Présentation de l'installation 11
Spécifications d'installation 12
Configuration réseau requise 12
Infrastructure de réseau conseillée 12
Configuration du matériel 12
Installation de l'appliance DL1000 dans un rack 13
Utilisation du système sans rack 13
Câblage de l'appliance 13
Branchement du bras de maintien des câbles (en option) 14
Mise sous tension de l'appliance DL1000 14
Configuration initiale du logiciel 14
Assistant de configuration de l'appliance AppAssure 14
Assistant de configuration de l'appliance DL 17
Rapid Appliance Self Recovery 22
Création de la clé USB RASR 22
Exécution du RASR 23
Utilitaire de récupération et de mise à jour 24

3 Configuration de votre Dell DL1000 25
Présentation de la configuration 25
Rétablissement des paramètres par défaut du système d'exploitation 25
Configuration de navigateurs pour accéder à Core Console DL1000 25

Modification des paramètres de navigateur dans Internet Explorer et Chrome 26
Configuration des paramètres de navigateur dans Firefox..... 26
Accès à la Core Console DL1000..... 26
Mise à jour des sites de confiance dans Internet Explorer..... 27
Cryptage de données d'instantanés d'agent..... 27
Configuration d'un serveur de messagerie et d'un modèle de notification par courrier électronique 27
Réglage du nombre de flux..... 28

4 Préparation de la protection de vos serveurs..... 29
Présentation..... 29
Installation des agents sur les clients..... 29
Déploiement du logiciel de l'agent lors de la protection d'un agent..... 29
Installation du logiciel Rapid Recovery Agent sur des machines Windows..... 30
Déployer le logiciel Rapid Recovery Agent sur une ou plusieurs machines..... 32
À propos de l'installation du logiciel Agent sur des machines Linux..... 34
Emplacement des fichiers de l'agent Linux..... 36
Dépendances de l'agent..... 37
Installation sur Debian ou Ubuntu du logiciel Rapid Recovery Agent..... 37
Installation du logiciel Rapid Recovery Agent sur SUSE Linux Enterprise Server..... 38
Installation de l'agent sur Red Hat Enterprise Linux et CentOS..... 39
Installer le logiciel Agent sur des machines Linux hors ligne..... 39
Installer le logiciel Agent sur des machines Windows Server Core Edition..... 40
Configuration de Rapid Recovery Agent sur une machine Linux..... 41
Protection d'une machine..... 42
Vérification de la connectivité du réseau..... 45
Vérification des paramètres du pare-feu..... 45
Vérification de la résolution DNS..... 45
Association de cartes réseau..... 46

5 Obtention d'aide..... 48
Où trouver la documentation et les mises à jour du logiciel..... 48
Documentation..... 48
Mises à jour logicielles..... 48
Contacter Dell..... 48
Commentaires sur la documentation..... 48

1

Présentation de votre DL1000 Dell

Votre Dell DL1000 combine la sauvegarde et la réplication dans un produit de protection unifiée des données. Elle 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 chiffrement et la réplication intégrés à une infrastructure privée ou publique du cloud. Les applications et données de serveur peuvent être restaurées en quelques minutes à des fins de conservation des données (DR) et de conformité.

Votre DL1000 prend en charge les environnements à plusieurs hyperviseurs sur les clouds privés et publics VMware vSphere, Oracle VirtualBox et Microsoft Hyper-V.

Sujets :

- Technologies de base du DL1000
- Fonctions de protection des données du Dell DL1000
- Architecture de déploiement du Dell DL1000
- Autres informations utiles

Technologies de base du DL1000

Votre appliance combine les technologies suivantes :

- Récupération en direct
- Récupération universelle
- Déduplication globale réelle
- Chiffrement

Récupération en direct

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

Récupération universelle

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

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

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

Déduplication globale réelle

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

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

Figure 1. Diagramme de la déduplication globale réelle

Cryptage

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

Fonctions de protection des données du Dell DL1000

Dell DL1000 Core

Le Core est le composant central de l'architecture de déploiement DL1000. Il stocke et gère les sauvegardes de machine et fournit des services pour la sauvegarde, la récupération, la conservation, la réplication, l'archivage et la gestion. Le Core est un ordinateur adressable 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 DL1000

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

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

Processus d'instantané

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

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

Réplication : site de reprise après sinistre ou fournisseur de services

La réplication est le processus qui consiste à copier des points de restauration depuis un core Rapid Recovery et à les envoyer vers un autre core Rapid Recovery dans un emplacement distinct où ils pourront être récupérés dans le cadre d'une reprise 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.

Récupération

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 DL1000 permet de réaliser une restauration à l'aide de Verified Recovery, Récupération universelle ou Récupération en direct.

Recovery-as-a-Service

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

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

Virtualisation et cloud

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

DL1000 peut exporter n'importe quelle machine protégée ou répliquée vers des versions sous licence de VMware ou Hyper-V. Dans le cas d'exportations continues, la machine virtuelle est mise à jour de façon incrémentielle après chaque instantané. Les mises à jour incrémentielles sont rapides et fournissent des clones de secours prêts à être mis sous tension en un seul clic. Les exportations de machine virtuelle prises en charge sont les suivantes :

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

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

Architecture de déploiement du Dell DL1000

L'architecture de déploiement du DL1000 est constituée de composants locaux et distants. Les composants distants peuvent être facultatifs pour les environnements qui n'ont pas besoin d'utiliser un site de récupération après sinistre ou un fournisseur de services gérés (MSP) pour effectuer la restauration hors site. Un déploiement local de base comprend un serveur de sauvegarde appelé core, et une ou plusieurs machines protégées dénommées agents. Le composant hors site est activé à l'aide de la réplication, pour fournir des

fonctionnalités de restauration complète sur le site de reprise après sinistre. Le core DL1000 utilise des images de base et des instantanés incrémentiels pour compiler les points de restauration des agents protégés.

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

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

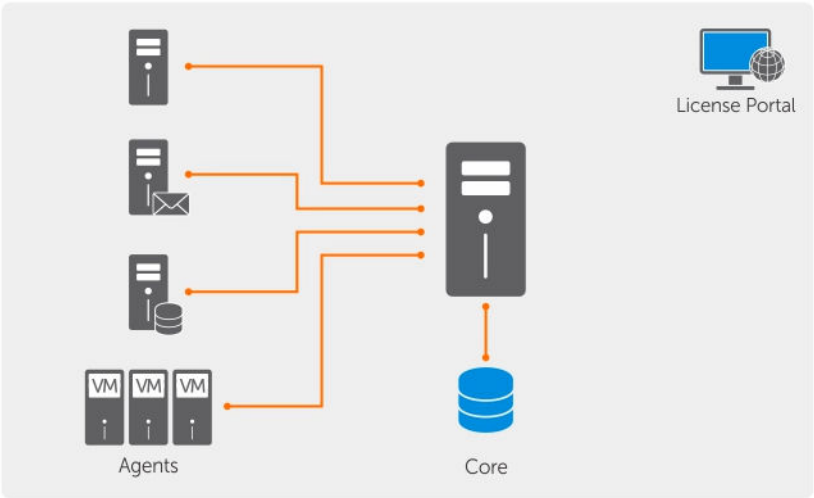

Figure 2. Architecture de déploiement Dell DL1000

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

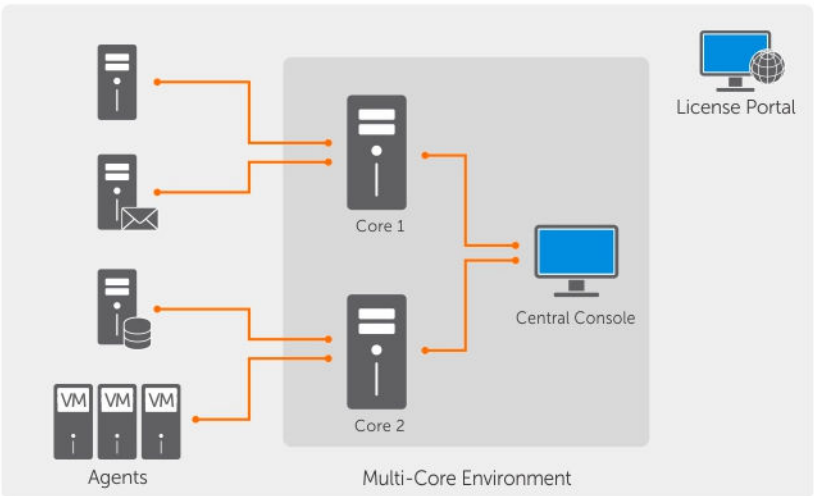

Figure 3. Architecture de déploiement de plusieurs cores DL1000

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 DL1000.
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.

2

Installer votre DL1000 Dell

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
1 To sans aucune VM	Lecteur de 2 To avec une partition logicielle/un système d'exploitation de 200 Go et un espace de référentiel utilisable de 1 To
2 To sans aucune VM	Lecteur de 3 To avec une partition logicielle/un système d'exploitation de 200 Go et un espace de référentiel utilisable de 2 To
3 To sans aucune VM	Lecteur de 4 To avec une partition logicielle/un système d'exploitation de 200 Go et un espace de référentiel utilisable de 3 To
3 To avec 2 machines virtuelles	Lecteur de 4 To avec une partition logicielle/un système d'exploitation de 200 Go, une partition de 300 Go pour le stockage de VM et un espace de référentiel utilisable de 3 To

Chaque configuration inclut également les matériels et logiciels suivants :

- Système Dell DL1000
- Contrôleurs RAID Dell PowerEdge (PERC)
- Logiciel Dell AppAssure

Présentation de l'installation

L'installation du DL1000 comprend l'installation des services Rapid Recovery Core et Rapid Recovery Agent sur les systèmes à protéger. Si d'autres cores sont configurés, vous devez installer les services de console de gestion centrale Rapid Recovery.

Pour installer le DL1000, procédez comme suit :

1 Procurez-vous la clé de licence permanente. Dans la console Core, vous pouvez gérer directement vos licences DL1000, modifier la clé de licence et contacter le serveur de licences. Vous pouvez également accéder au portail de licences Rapid Recovery depuis la page de Gestion des licences de la console Core.

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 de configuration de l'appliance DL).

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

Il y a une dizaine d'années, l'infrastructure standard des réseaux dorsaux offrait des vitesses de 100 mégabits par seconde. Les exigences en matière de trafic réseau et d'entrées/sorties ont augmenté régulièrement et substantiellement. De ce fait, les standards des réseaux dorsaux ont dû augmenter pour répondre à la demande. Les réseaux dorsaux modernes prennent en charge des vitesses comme le Gigabit Ethernet (GbE), qui transfère des trames Ethernet à 1 gigabit par seconde, ou le 10 GbE, qui est dix fois plus rapide.

Pour l'exécution de Rapid Recovery, Dell nécessite au minimum une infrastructure réseau 1GbE pour des performances efficaces. Dell recommande des réseaux 10GbE pour les environnements robustes. Les réseaux 10GbE sont également recommandés pour la protection de serveurs de grands volumes (5 To ou plus).

Si la machine core comporte plusieurs cartes d'interface réseau (NIC) prenant en charge l'association de cartes réseau NIC (regroupement de plusieurs cartes réseau physiques en un même NIC logique) et si les commutateurs du réseau le permettent, l'association de cartes réseau NIC sur le core peut générer des performances supplémentaires. Dès lors, l'association sur des machines protégées de cartes réseau pouvant être regroupées dans une association peut également augmenter les performances générales.

Si le core utilise iSCSI ou NAS (Network Attached Storage), Dell recommande d'utiliser des cartes réseau (NIC) distinctes pour le stockage et pour le trafic réseau.

Utilisez des câbles réseau d'une valeur nominale appropriée pour obtenir la bande passante prévue. Dell recommande de tester régulièrement les performances de votre réseau et d'ajuster votre matériel en conséquence.

Ces suggestions concernent des besoins réseaux classiques pour toutes les activités d'une entreprise, en sus des fonctionnalités de sauvegarde, de réplication et de récupération fournies par Rapid Recovery.

Configuration du matériel.

L'appliance est livrée avec un seul système DL1000. Avant de configurer le matériel de l'appliance, voir le manuel DL1000 de votre système, livré avec l'appliance. Déballez et configurez le matériel de l'appliance DL1000.

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 DL1000 :

1 Montez le système DL1000 en rack et câblez-le.
2 Mettez le système DL1000 sous tension.

Installation de l'appliance DL1000 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 DL1000 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 DL1000 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.

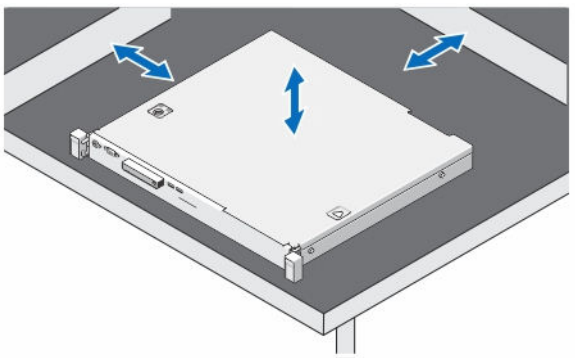

Figure 4. Utilisation du système sans rack

Câblage de l'appliance

Localisez le document *Dell DL1000 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 DL1000.

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 DL1000

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 DL1000 – Guide de mise en route* 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 de 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**.

   Après avoir entré le mot de passe, l'écran **Appuyez sur Ctrl+Alt+Suppr pour vous connecter** s'affiche.
6. Connectez-vous en utilisant le mot de passe d'administrateur modifié.

   L'écran **Sélectionner la langue de l'appliance** s'affiche.
7. Sélectionnez la langue de votre appliance à partir de la liste des langues prises en charge.

   L'écran **EULA** s'affiche.
8. Pour accepter le CLUF, cliquez sur le bouton **CLUF**.

   REMARQUE : Vous ne pourrez continuer à exécuter l'Assistant de configuration de l'appliance AppAssure que si vous acceptez le CLUF. Sinon, l'appliance vous déconnectera immédiatement.

L'écran d'accueil de l'**Assistant de 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 de 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 de configuration de l'appliance DL** 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
- Provisionnement du stockage

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 DL1000 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.

Provisionnement du stockage

Pour effectuer le provisionnement de disque pour tout le stockage disponible afin de créer un nouveau référentiel AppAssure :

1 Dans la page **Provisionnement**, cliquez sur **Suivant.**
L'écran **Provisionnement** affiche la capacité de stockage disponible pour le provisionnement. Cette capacité est utilisée pour créer un nouveau référentiel AppAssure.

> **REMARQUE : Dans le cas du système de configuration DL1000 3 To (2 VM), vous pouvez allouer de l'espace disque aux VM de secours.**

Le provisionnement de disque de votre système est terminé et un nouveau référentiel a été créé.
2 Cliquez sur **Suivant**.
L'écran**Configuration terminé** s'affiche, cliquez sur **Quitter**.

Assistant de configuration de l'appliance DL

> **REMARQUE : L'Assistant de configuration du serveur DL s'affiche uniquement lorsque vous mettez à niveau votre appliance à l'aide du dernier utilitaire RUU.**

> **PRÉCAUTION : Vous devez avoir effectué toutes les étapes de l'Assistant de configuration de l'appliance DL 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 DL 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 de configuration de l'appliance DL avant qu'il ait terminé, des erreurs de fonctionnement du système risquent de se produire.**

L'Assistant de configuration de l'appliance DL vous guide au cours des étapes suivantes pour configurer le logiciel sur l'appliance :

- Configuration de l'interface réseau
- Enregistrement et paramétrage de l'hôte
- Alertes et surveillance
- Accès et gestion
- Configuration des sauvegardes Windows
- Provisionnement du stockage
- Configuration des options de mise à jour et stratégie de conservation

> **REMARQUE : Après avoir terminé la configuration de l'appliance, vous pouvez soit ignorer l'Assistant, soit continuer à exécuter la protection de la machine, la réplication, les exportations de machines virtuelles et/ou de secours. Si vous choisissez d'ignorer l'Assistant, la console Core démarre automatiquement et vous pourrez effectuer ultérieurement la protection de la machine, la réplication et les exportations de machines virtuelles.**

Pour plus d'informations sur la manière d'effectuer la protection de la machine, la réplication et les exportations de machines virtuelles, voir *Rapid Recovery sur appliances DL – Guide d'utilisation* sur **site www.dell.com/support/home**.

Configuration de l'interface réseau

Pour configurer les interfaces réseau disponibles :

1 Dans l'écran **Bienvenue dans l'Assistant de configuration de l'appliance DL**, cliquez sur **Suivant**.
La fenêtre **Contrat de licence** s'affiche.

2 Pour accepter le contrat, cliquez sur **J'accepte le contrat de licence**, puis cliquez sur **Suivant**.
La page **Paramètres réseau** affiche les interfaces réseau connectées disponibles.

3 Si nécessaire, connectez des interfaces réseau supplémentaires et cliquez sur **Actualiser**.
Les interfaces réseau connectées disponibles s'affichent.

4 Sélectionnez les interfaces réseau appropriées adaptées à votre environnement.
Vous avez le choix entre IPV4 et IPV6.

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

5 Pour activer IPV4, sélectionnez **Activer une interface IPv4**.
   a Pour attribuer les détails du protocole Internet de l'interface IPv4, effectuez l'une des actions suivantes :
      - Pour attribuer automatiquement les détails du protocole Internet sélectionné, sélectionnez **Obtenir une adresse IPV4 automatiquement**.
      - Pour attribuer manuellement la connexion réseau, sélectionnez **Définir manuellement l'adresse IPv4** et entrez les détails suivants :
         - **Adresse IPv4**
         - **Masque de sous-réseau**
         - **Passerelle par défaut**

6 Pour activer IPV6, sélectionnez **Activer une interface IPv6**
   a Pour attribuer les détails du protocole Internet de l'interface IPv6, effectuez l'une des actions suivantes :
   - Pour attribuer automatiquement les détails du protocole Internet sélectionné, sélectionnez **Obtenir une adresse IPV6 automatiquement**.
   - Pour attribuer manuellement la connexion réseau, sélectionnez **Définir manuellement l'adresse IPv6** et entrez les détails suivants :
      - **Adresse IPv6**
      - **Longueur du préfixe de sous-réseau**
      - **Passerelle par défaut**

7 Pour activer l'association de cartes réseau NIC, sélectionnez **Activer l'association de cartes réseau NIC**.
Pour en savoir plus sur l'association des cartes réseau NIC, voir Association des cartes réseau.

8 Cliquez sur **Suivant**.
La page **Enregistrement** s'affiche.

Enregistrement et paramétrage de l'hôte

Enregistrez votre appliance avec la clé de licence appropriée afin de bénéficier des fonctionnalités en rapport. Il 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 est recommandé de le faire à ce stade. La modification du nom d'hôte après l'exécution de l'Assistant Configuration de l'appliance DL exige la réalisation de plusieurs étapes.

1 Dans la page **Enregistrement**, vous devez sélectionner l'une des options ci-dessous :
   - **Enregistrer maintenant** – Pour enregistrer votre appliance avec la licence achetée. Saisissez les détails suivants : numéro de licence dans la zone de texte `Numéro de licence` et une adresse e-mail valide dans la zone de texte `Adresse e-mail`.

- **Utiliser la licence d'évaluation** – Pour enregistrer votre appliance avec la licence d'évaluation. La licence d'évaluation expire au bout de 30 jours. Afin de pouvoir continuer à utiliser le produit sans interruption, n'attendez pas la fin de cette période pour enregistrer votre appliance.

2 Cliquez sur **Suivant**.

La page **Paramètres de l'hôte** s'affiche.

3 Par défaut, le nom d'hôte de l'appliance est affiché dans la zone de texte `Nom d'hôte`. Pour modifier le nom d'hôte de votre appliance, entrez un `nom approprié` dans la zone de texte **Nom d'hôte**.

4 Si vous voulez joindre votre appliance à un domaine, cochez la case **Joindre ce système à un domaine** et spécifiez les informations suivantes :

Sinon, passez à l'étape 5.

REMARQUE : Joindre un système à un domaine n'est pas possible sur Windows Server 2012 R2 Foundation Edition. Dans ce cas, la case Joindre ce système à un domaine est désactivée.

Zone de texte	Description
Adresse de domaine	Adresse du domaine auquel vous souhaitez ajouter votre système
Administrateur de domaine	Administrateur de domaine
Mot de passe	Mot de passe

5 Cliquez sur **Suivant**.

La page **Alertes et surveillance** s'affiche.

Alertes et surveillance

Pour activer des alertes concernant des modifications intervenant sur les matériels et les logiciels, vous avez deux possibilités : SNMP et SMTP. SNMP (Simple Network Management Protocol) est un protocole de gestion réseau courant qui permet des fonctionnalités d'administration (détection de périphériques, surveillance et génération d'événements). SNMP fournit une gestion réseau du protocole TCP/IP. Vous pouvez utiliser SNMP (Simple Network Management Protocol) ou SMTP (Simple Mail Transfer Protocol) pour définir des alertes et la surveillance de votre appliance.
Pour recevoir des notifications, configurez ici les options :

REMARQUE : Il est recommandé de configurer des alertes. Vous avez également la possibilité d'ignorer la configuration des alertes. Pour cela, passez directement à l'étape 3.

1 Vous avez le choix parmi les options suivantes pour activer des alertes :
   - Pour activer des alertes système SNMP, sélectionnez **Activer des alertes système SNMP**.
     1 Dans `Communauté SNMP`, saisissez un ou plusieurs noms de communautés SNMP. Utilisez des virgules pour séparer plusieurs noms de communautés.
     2 Dans `Destinations des interruptions SNMP`, entrez des destinations d'interruptions et cliquez sur **Ajouter**.
   - Pour activer des alertes logicielles SNMP, sélectionnez **Activer des alertes système SNMP**.
     1 Dans `Communauté SNMP`, saisissez un ou plusieurs noms de communautés SNMP. Utilisez des virgules pour séparer plusieurs noms de communautés.
     2 Dans `Destinations des interruptions SNMP`, entrez des destinations d'interruptions et cliquez sur **Ajouter**.
2 Pour définir des alertes logicielles via e-mail, sélectionnez **Notifier par e-mail** et entrez une adresse e-mail valide.
3 Cliquez sur **Suivant**.

La page `Accès et gestion` s'affiche.

Accès et gestion

Pour accéder à votre appliance et la gérer, vous devez configurer les paramètres d'accès et de gestion.

Pour configurer les paramètres d'accès et de gestion de votre appliance, procédez comme suit :

1 Dans la page **Accès et gestion**, sélectionnez ou désélectionnez les options suivantes pour accéder à votre appliance et la gérer via les éléments suivants :
   - Activer le Bureau à distance
   - Activer le pare-feu Windows
   - Activer la sécurité renforcée d'Internet Explorer
   - Activer Windows Update
   - Utiliser un serveur proxy
2 Si vous sélectionnez **Utiliser un serveur proxy**, entrez l'adresse du proxy dans la zone de texte `Adresse de proxy` et le numéro de port dans la zone de texte `Port`.
3 **REMARQUE : Si vous souhaitez utilisez les options par défaut des paramètres d'accès et de gestion, cliquez sur le bouton Rétablir les paramètres par défaut.**

   Cliquez sur **Suivant**.

   La page **Options de sauvegarde de la configuration de l'appliance** s'affiche.

Configuration des sauvegardes Windows

REMARQUE : Tous les divers DL, à l'exception de DL1000, prennent en charge la fonction Windows de sauvegardes.

Options de sauvegarde de la configuration de l'appliance vous permet de définir la fréquence à laquelle la configuration de l'appliance est sauvegardée. Les données des sauvegardes Windows aident à récupérer les paramètres de configuration de vos appliances en cas de défaillance.

1 Dans les **options de sauvegarde de la configuration de l'appliance**, sélectionnez **Effectuer une sauvegarde de la configuration de l'appliance**.

   Vous avez le choix entre les options suivantes : Tous les jours, Toutes les semaines et Tous les mois.
2 Pour définir la fréquence des sauvegardes Windows, sélectionnez l'une des options suivantes :

Option	Description
Tous les jours	Sauvegarde vos paramètres de configuration tous les jours à partir de 00h01
Toutes les semaines	Sauvegarde vos paramètres de configuration toutes les semaines à partir de chaque dimanche à 00h01
Tous les mois	Sauvegarde vos paramètres de configuration tous les mois en commençant à partir de chaque dimanche à 00h01

3 Cliquez sur **Suivant**.

   La page **Provisionnement du stockage** s'affiche.

Provisionnement du stockage

Votre appliance vous permet de provisionner son stockage interne pour créer des disques virtuels (VD) hébergeant des référentiels et des disques virtuels de secours, des archives ou servant à d'autres fins.

1 Dans la page **Provisionnement du stockage**, sélectionnez les options de configuration suivantes pour votre stockage.

   Le `nom du référentiel` s'affiche par défaut en tant que **référentiel 1**.

REMARQUE : La taille du référentiel dépend de la licence appliquée lors de l'enregistrement de votre appliance.

- Si vous avez appliqué une licence d'évaluation lors de l'enregistrement de votre appliance, il n'y a pas de restriction dans la taille du référentiel.
- Si, lors de l'enregistrement de votre appliance, vous avez appliqué une licence achetée, la taille du référentiel correspond au modèle. Par exemple : Sur une appliance DL1000 de 1 To, un référentiel de 1 To est créé.

2 Sélectionnez **Allouer une partie de votre stockage pour les disques virtuels de secours, les archives, ou à d'autres fins**.

3 En déplaçant le curseur, allouez le pourcentage de l'espace de stockage qui est disponible après la création du référentiel. Vous pouvez également spécifier la taille exacte dans la zone de texte `Taille`.

Il sera créé un disque virtuel de la capacité spécifiée pour l'hébergement de machines virtuelles de secours, d'archives ou d'autres finalités.

4 Cliquez sur **Suivant**.

Le référentiel initial est créé ainsi que les VD destinés à héberger des VM ou des disques à d'autres fins.

La page **Stratégie de conservation** s'affiche.

Configuration des options de mise à jour et stratégie de conservation

Les politiques de conservation imposent des périodes de stockage des sauvegardes sur des supports à court terme (rapide et onéreux). Il peut arriver que certaines exigences techniques et commerciales exigent une conservation étendue de ces sauvegardes. Cependant, l'utilisation de stockage coûte très cher. Dans votre appliance, les stratégies de conservation peuvent être personnalisées pour spécifier la durée pendant laquelle un point de restauration de sauvegarde est conservé. Au fur et à mesure que les points de restauration arrivent en fin de leur période de conservation, les points de restauration parviennent à expiration et sont supprimés du pool de conservation.

REMARQUE : Si la restriction de licence de la stratégie de conservation est l'option par défaut, la stratégie de conservation ne peut pas être configurée pour une conservation des données de plus de trois mois. Si vous tentez de le faire, un message d'erreur s'affichera.

1 Les options suivantes vous permettent de définir la période pendant laquelle sont stockés les instantanés de sauvegarde des machines protégées. Elles vous permettent également de modifier le processus de rollup de fusion et de suppression des anciennes sauvegardes. La page **Stratégie de conservation** affiche les options suivantes :

Tableau 2. Options de planification pour la stratégie de conservation par défaut

Zone de texte	Description
Conserver tous les points de restauration pendant n [période de conservation]	Indique la période de conservation des points de restauration. Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. La valeur par défaut est de 3 jours. Vous avez le choix entre jours, semaines, mois ou années
...puis gardez un point de restauration par heure pour n [période de conservation]	fournit un niveau de conservation plus granulaire. Il s'utilise en tant que bloc de construction avec le paramétrage principal pour mieux définir la durée de conservation des points de restauration. Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. La valeur par défaut est de 2 jours. Vous avez le choix entre jours, semaines, mois ou années
...puis gardez un point de restauration par jour pour n [période de conservation]	Fournit un niveau de conservation plus granulaire. Il s'utilise en tant que bloc de construction avec le paramétrage principal pour mieux définir la durée de conservation des points de restauration. Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. La valeur par défaut est de 4 j. Vous avez le choix entre jours, semaines, mois ou années

Zone de texte	Description
...puis gardez un point de restauration par semaine pour n [période de conservation]	Fournit un niveau de conservation plus granulaire. Il s'utilise en tant que bloc de construction avec le paramétrage principal pour mieux définir la durée de conservation des points de restauration. Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. La valeur par défaut est de 3 semaines. Vous avez le choix entre semaines, mois ou années
...puis gardez un point de restauration par mois pour n [période de conservation]	Fournit un niveau de conservation plus granulaire. Il s'utilise en tant que bloc de construction avec le paramétrage principal pour mieux définir la durée de conservation des points de restauration. Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. La valeur par défaut est de 2 mois. Vous avez le choix entre mois ou années
...puis gardez un point de restauration par an pour n [période de conservation]	Entrez un nombre représentant la période de conservation, puis sélectionnez une période de temps. Vous avez le choix entre années

2 Cliquez sur **Suivant**.

La fenêtre **Options de mise à jour** s'affiche.

3 Pour vérifier l'existence de mises à jour du logiciel de l'appliance, sélectionnez l'option **Rechercher des mises à jour du logiciel de l'appliance**.

Si une mise à jour existe, elle est téléchargée et installée.

4 Pour permettre des mises à jour de Rapid Recovery Core, sélectionnez **Permettre des mises à jour de Rapid Recovery Core**, puis sélectionnez l'une des options ci-dessous :

- Notifier de mises à jour, mais ne pas les installer automatiquement
- Installer automatiquement les mises à jour

5 Cliquez sur **Terminer**.

Les paramètres sont appliqués.

Rapid Appliance Self Recovery

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

Création de la clé USB RASR

Pour créer une clé USB RASR :

1 Allez à l'onglet **Appliance**.

2 Dans le volet de navigation de gauche, sélectionnez **Appliance** > **Sauvegarde**.

La fenêtre **Créer un lecteur USB RASR** s'affiche.

REMARQUE : Insérez une clé USB 16 Go ou plus, avant de tenter de créer la clé RASR.

3 Après avoir inséré une clé USB de 16 Go ou plus, cliquez sur **Créer un lecteur USB RASR maintenant**.

Un message de **vérification de conditions** s'affiche.

Une fois les prérequis vérifiés, la fenêtre **Créer un lecteur USB RASR** affiche la taille minimale requise pour créer le lecteur USB et la **liste des chemins cible possible.**.

4 Sélectionnez la cible et cliquez sur **Créer**.

Une boîte de dialogue de confirmation s'affiche.

5 Cliquez sur **Oui**.

La clé de lecteur USB RASR est créée.

6 **REMARQUE : Veillez à utiliser la fonction Windows d'éjection de lecteur pour préparer le retrait de la clé USB. Sinon, le contenu de celle-ci risque d'être endommagé et la clé USB risque de ne pas fonctionner comme prévu.**

Retirez la clé USB RASR créée pour chaque appliance DL, étiquetez-la et rangez-la en vue d'une utilisation ultérieure.

Exécution du RASR

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

REMARQUE : Assurez-vous que vous disposez des derniers RUU disponibles et accessibles sur votre appliance.

.

REMARQUE : Pour savoir comment effectuer une récupération du système à l'aide de RASR, reportez-vous au document *Récupérer une appliance Dell™ DL de sauvegarde et de récupération à l'aide de RASR (Rapid Appliance Self Recovery)* sur Dell.com/support/home.

Pour effectuer une réinitialisation des paramètres d'usine :

1 Insérez la clé USB RASR créée.
2 Redémarrez l'appliance et sélectionnez **Gestionnaire d'amorçage (F11)**.
3 Dans le **menu principal du Gestionnaire d'amorçage**, sélectionnez le **menu d'amorçage ponctuel du BIOS**.
4 Dans le **menu d'amorçage du gestionnaire d'amorçage**, sélectionnez le lecteur USB relié.
5 Sélectionnez votre configuration de clavier.
6 Cliquez sur **Dépanner** > **Rapid Appliance Self Recovery**
7 Sélectionnez le système d'exploitation cible (SE).

RASR démarre, et l'écran d'**accueil** s'affiche.

8 Cliquez sur **Suivant**.

L'écran de vérification **Conditions** s'affiche.

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

9 Cliquez sur **Suivant**.

L'écran de **sélection du mode de restauration** s'affiche avec trois options :

- **Restauration du système**
- **Assistant de récupération Windows**
- **Restauration des paramètres définis en usine**

10 Sélectionnez l'option **Restaurer les paramètres définis en usine** .

This option will recover the operating system disk from the factory image.

11 Cliquez sur **Suivant**.

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

12 Cliquez sur **Oui**.

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

13 La page **RASR terminé** s'affiche à la fin de la récupération. Cliquez sur **Terminer**.
14 Démarrez le système après la restauration.
15 **REMARQUE : Ne continuez que si vous voyez l' Assistant de configuration d'appliance AppAssure ; sinon, passez à l'étape 17.**

Attendez que l'Assistant de configuration de l'appliance AppAssure ait fini de se charger. Vous devez le fermer. Fermez l'assistant à l'aide du Gestionnaire des tâches de Windows.

16 Exécutez le fichier **launchRUU.exe** dans le package RUU. Laissez-vous guider par les instructions qui s'affichent et sélectionnez l'option permettant de poursuivre l'installation de RUU.

17 L'**Assistant de configuration de l'appliance DL** se lance et vous guide dans la restauration.

Votre appliance fonctionne normalement à présent.

Utilitaire de récupération et de mise à jour

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

RUU se compose de versions mises à jour des rôles et fonctionnalités de Windows Server, .Net 4.5.2, un fournisseur LSI, les applications DL et les logiciels OpenManage Server Administrator et Rapid Recovery Core. En outre, l'utilitaire met également à jour le contenu de RASR (Rapid Appliance Self Recovery).

REMARQUE : Si vous utilisez actuellement l'une des versions AppAssure Core, la version 6.0.2.144 (ou antérieure) de Rapid Recovery Core, RUU force la mise à jour vers la version la plus récente disponible dans la charge utile. Il n'est pas possible d'ignorer cette mise à jour et celle-ci n'est pas réversible. Si vous ne souhaitez pas effectuer la mise à niveau du logiciel Core, n'exécutez pas RUU.

Pour installer la version la plus récente de RUU :

1 Allez sur le portail de licences sous la section Téléchargements ou sur **support.dell.com** et téléchargez le programme d'installation de RUU.

2 Pour lancer RUU, exécutez le fichier **launchRUU.exe** dans le package RUU.

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

3

Configuration de votre Dell DL1000

Présentation de la configuration

Après avoir exécuté l'Assistant de configuration de l'appliance DL, procédez comme suit pour vérifier que votre appliance de sauvegarde et les serveurs sauvegardés par celle-ci sont bien configurés.

La configuration inclut des tâches comme la configuration des navigateurs pour accéder à distance à la console Core DL1000, gérer les licences et configure des alertes et des notifications. Après avoir terminé la configuration du core, vous pourrez protéger les agents et effectuer des récupérations.

REMARQUE : L'appliance est configurée avec une licence Rapid Recovery temporaire de 30 jours. Pour obtenir une clé de licence permanente, connectez-vous au portail de licences Dell Data Protection | Rapid Recovery sur www.dell.com/DLActivation. Pour plus de détails sur la modification d'une clé de licence, reportez-vous au manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation* sur dell.com/support/home.

REMARQUE : Lorsque vous utilisez l'appliance de sauvegarde sur disque DL1000, il est recommandé d'utiliser l'onglet Appliance pour configurer le core.

Rétablissement des paramètres par défaut du système d'exploitation

Pour rétablir les paramètres par défaut du système d'exploitation, effectuez les opérations suivantes :

1 Connectez-vous en tant qu'administrateur et ouvrez une fenêtre de commande.
2 Naviguez vers le site **c:\windows\system32\sysprep** et exécutez la commande **sysprep.exe/generalize/oobe/reboot**.
3 Sélectionnez :
- **English (anglais)** pour la langue
- **United States (États-Unis)** pour le pays/ la région
- **US** pour la disposition du clavier

Configuration de navigateurs pour accéder à Core Console DL1000

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 Rapid Recovery Core>* à la zone **Sites de confiance**.
4 Cliquez sur **Fermer**, sélectionnez **Sites de confiance**, puis cliquez sur **Personnaliser le niveau**.
5 Faites défiler l'affichage jusqu'à **Divers** → **Affiche un contenu mixte** et sélectionnez **Activer**.
6 Faite défiler l'affichage jusqu'au bas de l'écran vers l'entrée **Authentification utilisateur** → **Ouverture de session**, puis sélectionnez **Connexion automatique avec le nom d'utilisateur et le mot de passe actuel**.
7 Cliquez sur **OK**, puis sélectionnez l'onglet **Avancé**.
8 Faites défiler la liste jusqu'à **Multimédia**, puis sélectionnez **Lire les animations dans les pages Web**.
9 Faites défiler l'écran jusqu'à **Sécurité**, sélectionnez **Activer l'authentification Windows intégrée**, puis cliquez sur **OK**.

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 DL1000

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 DL1000. 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**.

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 DL1000 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 DL1000 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 DL1000 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**.
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**.

Réglage du nombre de flux

Par défaut, Rapid Recovery est configuré pour autoriser trois flux simultanés en direction de l'appliance. Il est recommandé de définir un nombre de flux entre 10 et 15 pour des performances optimales.

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 **maximum de transferts simultanés** en le définissant 10 et 15 pour des performances optimales, mais, si le réglage des performances ne semble pas satisfaisant, essayez de l'adapter manuellement.

4

Préparation de la protection de vos serveurs

Présentation

Pour protéger vos données avec DL1000, vous devez ajouter dans la console Core les stations de travail et les serveurs à protéger ; par exemple, votre serveur Exchange, SQL ou Linux, etc.

Dans la console Core, vous pouvez identifier la machine sur laquelle 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 chiffrement, etc. Pour en savoir plus sur l'accès à la console Core pour protéger les stations de travail et les serveurs, voir Protection d'une machine.

Sujets :

- Installation des agents sur les clients
- À propos de l'installation du logiciel Agent sur des machines Linux
- Installer le logiciel Agent sur des machines Linux hors ligne
- Protection d'une machine

Installation des agents sur les clients

L'agent Rapid Recovery doit être installé sur chaque client sauvegardé par l'appliance DL1000. La console Rapid Recovery Core vous permet de déployer des agents sur des machines. Le déploiement d'agents sur des machines nécessite 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. Mais, s'il existe plusieurs versions de systèmes d'exploitation, il peut être plus facile d'installer les agents machine par machine.

Vous pouvez également déployer le logiciel Agent sur la machine agent lors de la protection de celle-ci. Cette option est possible pour les machines sur lesquels le logiciel Agent n'a pas encore été installé. Pour en savoir plus sur le déploiement du logiciel Agent pendant la protection d'une machine, voir *Rapid Recovery sur appliances DL – G* sur **Dell.com/support/home**.

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

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

REMARQUE : Cette procédure n'est pas requise si vous avez déjà installé le logiciel Agent sur une machine que vous souhaitez protéger. Si le logiciel Agent n'est pas installé avant la protection de la machine, vous ne serez pas en mesure de sélectionner des volumes pour la protection dans le cadre de cet assistant. Dans ce cas, par défaut, tous les volumes de la machine d'agent seront inclus dans la protection. Rapid Recovery prend en charge la protection et la récupération des machines configurées avec des partitions EISA. La prise en charge est également étendue aux machines Windows 8 et 8.1 et aux machines Windows 2012 et 2012 R2 qui utilisent Windows Recovery Environment (Windows RE).

1 Effectuez l'une des opérations suivantes :
   - Si vous procédez à partir de l'Assistant de protection de machines, passez à l'étape 2 .
   - Si vous procédez à partir de la console Rapid Recovery Core, dans la barre de boutons, cliquez sur **Protéger**.

L'**Assistant de protection de machines** s'affiche.

2 Dans la page **Accueil**, sélectionnez les options d'installation appropriée :

- Si vous n'avez pas besoin de définir un référentiel ni d'établir de chiffrement, sélectionnez **Normal**.
- Si vous avez besoin de créer un référentiel ou définir un référentiel différent pour les sauvegardes de la machine sélectionnée, ou si vous souhaitez établir un chiffrement à l'aide de l'assistant, sélectionnez **Avancé (afficher les étapes facultatives)**.
- Le cas échéant, si vous ne souhaitez plus voir la page **Accueil** de l'Assistant de protection de machines à l'avenir, cochez l'option **Ignorer cette page d'accueil à la prochaine ouverture de l'Assistant**.

3 Lorsque vous êtes satisfait de vos choix dans la page d'accueil, cliquez sur **Suivant**.

La page **de connexion** s'affiche.

4 Dans la page **Connexion**, entrez les informations concernant la machine à laquelle vous souhaitez vous connecter (voir le tableau suivant), puis cliquez sur **Suivant**.

Tableau 3. Paramètres de connexion machine

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
Port	Le numéro du port sur lequel Rapid Recovery Core communique avec l'agent sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, Administrateur (ou, si la machine se trouve dans un domaine, [nom de domaine] \Administrateur).
Mot de passe	Le mot de passe utilisé pour se connecter à cette machine

Si la page **Installer l'agent** s'affiche ensuite dans l'Assistant de protection de machines, cela veut dire que Rapid Recovery ne détecte pas Rapid Recovery Agent sur la machine et qu'il va installer la version actuelle du logiciel.

5 **REMARQUE : Le logiciel Agent doit être installé sur la machine à protéger, et la machine doit être redémarrée avant de pouvoir être sauvegardée vers le core. Pour que le programme d'installation redémarre la machine protégée, sélectionnez l'option Après l'installation, redémarrer automatiquement la machine (recommandé) avant de cliquer sur Suivant.**

Cliquez sur **Suivant**.

Installation du logiciel Rapid Recovery Agent sur des machines Windows

Déployez le fichier du programme d'installation de Rapid Recovery Agent vers la machine que vous souhaitez protéger en utilisant l'une des méthodes décrites dans la rubrique « Installation du logiciel Rapid Recovery Agent » du manuel *Dell Data Protection | Rapid Recovery 6.0 – Guide d'installation et de mise à niveau*. Ensuite, lancez le programme d'installation en suivant la procédure décrite ci-dessous pour installer ou mettre à niveau le logiciel sur chaque machine Windows à protéger dans Rapid Recovery Core.

REMARQUE : Vous devez exécuter le programme d'installation avec des privilèges d'administrateur local.

1 Depuis la machine à protéger, cliquez deux fois sur l'exécutable du programme d'installation de Rapid Recovery Agent pour lancer ce programme.

Selon la configuration de votre machine, la fenêtre Contrôle de compte d'utilisateur ou la fenêtre Ouvrir un fichier – Avertissement de sécurité peut s'afficher.

2 Si le système vous demande une autorisation, confirmez que vous voulez exécuter le programme d'installation et apporter des modifications au système.

3 Si des composants .NET sont manquants ou ont besoin d'être mis à niveau, acceptez les invites à télécharger et installer .NET Framework.

4 Dans le champ Langue, sélectionnez la langue appropriée, puis cliquez sur **OK**.

5 Choisissez l'une des options suivantes :

- Si c'est la première fois que le logiciel Rapid Recovery Agent est installé sur cette machine, le programme d'installation prépare l'installation, puis l'Assistant d'installation de Rapid Recovery Agent s'affiche. Passez directement à l'étape 6.
- Si une version antérieure d'AppAssure Agent ou de Rapid Recovery Agent y est installée, il vous sera demandé si vous souhaitez effectuer une mise à niveau vers la version actuelle.

  1 Cliquez sur **Oui**.

    La page **Progression** de l'Assistant d'installation de Rapid Recovery Agent s'affiche alors. L'application est téléchargée vers le dossier de destination et une barre indique l'avancement du téléchargement. Lorsque le téléchargement est terminé, l'Assistant passe automatiquement à la page **Terminé**.

  2 Passez à l'étape 12.

6 Dans la page **Bienvenue** de l'Assistant d'installation de Rapid Recovery, cliquez sur **Suivant** pour poursuivre l'installation.

La page **Contrat de licence** s'affiche.

7 Dans la page **Contrat de licence**, cliquez sur **J'accepte les termes du contrat de licence**, puis sur **Suivant**.

La page **Prérequis** s'affiche.

8 Le programme d'installation de Rapid Recovery Agent vérifie l'existence des fichiers prérequis.

- Si ces fichiers existent, un message vous signale que tous les éléments prérequis sont installés sur la machine.
- S'ils n'existent pas, le programme d'installation de Rapid Recovery Agent identifie quels sont les fichiers nécessaires et affiche les résultats en conséquence ; par exemple, CRT 2013 (x64) ENU (code distribuable pour Microsoft Visual Studio®), ou CLR Microsoft System for SQL Server 2008 R2 (x64). Cliquez sur **Installer les prérequis**.

9 Une fois les fichiers prérequis installés, cliquez sur **Suivant**.

La page **Options avancées** s'affiche.

10 Dans la page **Options d'installation**, passez en revue les options choisies. Si nécessaire, modifiez-les comme indiqué ci-dessous.

- 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**.
- Dans le champ de texte **Numéro de port**, entrez le numéro de port à utiliser pour la communication entre le logiciel Agent sur la machine protégée et Rapid Recovery Core.

  REMARQUE : La valeur par défaut est 8006. Si vous modifiez le numéro de port, notez-le au cas où vous devriez ajuster ultérieurement les paramètres de configuration.
- Sélectionnez **Autoriser l'agent d'envoyer automatiquement des informations de diagnostic et d'utilisation à Dell Inc.** pour envoyer des informations de diagnostic et d'utilisation à Dell. Si vous ne voulez pas envoyer ces informations, désélectionnez cette option.

11 Une fois satisfait des options d'installation, cliquez sur **Installer**.

La page **Progression** s'affiche avec une barre permettant de surveiller l'avancement de l'installation.

Lorsque l'installation est terminée, la page **Terminé** s'affiche. Passez à l'étape 12.

12 Dans la page **Terminé**, si un message indique que le système doit être redémarré pour que l'installation prend effet, effectuez l'une des opérations suivantes :

- Pour redémarrer immédiatement, cochez **Oui, je veux redémarrer mon ordinateur maintenant**.
- Pour redémarrer plus tard, désélectionnez l'option **Non, je veux redémarrer mon ordinateur plus tard.**.

13 Dans la page **Terminé**, cliquez sur **Terminer**.

L'assistant d'installation se ferme et l'installation d'Agent est terminée.

Déployer le logiciel Rapid Recovery Agent sur une ou plusieurs machines

L'Assistant de déploiement du logiciel Rapid Recovery Agent peut vous faciliter la tâche pour déployer le logiciel Rapid Recovery Agent sur une ou plusieurs machines Windows.

REMARQUE : Par le passé, l'on désignait cette fonction sous le nom de « déploiement en masse ».

Lorsque vous utilisez l'Assistant de déploiement du logiciel Rapid Recovery Agent, Rapid Recovery peut détecter automatiquement les machines présentes sur un hôte et il vous permet de sélectionner les machines sur lesquelles vous voulez le déployer. Pour les machines présentes sur des domaines ou des hôtes autres qu'Active Directory, vCenter ou ESX(i), vous pouvez vous connecter manuellement à des machines individuelles en utilisant leurs adresses IP et les informations d'identification appropriées. Vous pouvez également envoyer des mises à niveau du logiciel vers des machines déjà protégées par le Rapid Recovery Core local.

Depuis la console Core, vous pouvez effectuer l'une des tâches suivantes :

- Déploiement sur des machines d'un domaine Active Directory
- Déploiement vers des machines présentes sur un hôte virtuel VMware vCenter/ESX(i)

REMARQUE : Dell recommande de limiter à 50 au maximum le nombre de machines sur lequel effectuer un déploiement simultané afin d'éviter des contraintes de ressources sur les ressources susceptible de faire échouer le déploiement.

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 votre appliance, partagez le répertoire **C:\Program Files\AppRecovery** avec le ou les clients que vous prévoyez de sauvegarder.
   b Sur le système client, mappez un lecteur vers **C:\Program Files\AppRecovery** sur l'appliance DL.
   c Sur le système client, ouvrez le répertoire **C:\Program Files\AppRecovery** et cliquez deux fois sur l'agent correspondant au système client afin de démarrer l'installation.

Déploiement sur des machines d'un domaine Active Directory

Cette procédure permet de déployer simultanément le logiciel Rapid Recovery Agent sur une ou plusieurs machines d'un même domaine Active Directory.
Avant de commencer cette procédure, munissez-vous des informations de domaine et des identifiants pour le serveur Active Directory.

1 Sur la console Rapid Recovery Core, cliquez sur le menu déroulant **Protéger**, puis sur **Déployer le logiciel Agent**.
   L'Assistant de déploiement du logiciel Agent s'ouvre.
2 Dans la page **Connexion** de l'assistant, dans la liste déroulante **Source**, sélectionnez **Active Directory**.
3 Entrez les informations de domaine et les identifiants comme dans le tableau suivant.

Tableau 4. Informations de domaine et identifiants

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP du domaine Active Directory.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter au domaine ; par exemple, Administrateur ou, si la machine se trouve dans un domaine, [nom de domaine] \Administrateur).
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à ce domaine.

4 Cliquez sur **Suivant**.

5 Dans la page **Machines**, sélectionnez les machines vers lesquelles vous souhaitez déployer le logiciel Rapid Recovery Agent.

6 Si vous le souhaitez, pour redémarrer automatiquement les machines protégées après l'installation d'Agent, sélectionnez **Après l'installation d'Agent, redémarrer automatiquement les machines (recommandé)**.

7 Cliquez sur **Terminer**.

Le système vérifie automatiquement chacune des machines que vous avez sélectionnées.

Si Rapid Recovery détecte des problèmes pendant la vérification automatique, l'Assistant passe à une page d'avertissements, dans laquelle vous pouvez effacer des machines de la sélection et les vérifier manuellement. Si les machines que vous avez ajoutées réussissent la vérification automatique, elles apparaissent dans le volet Déployer Agent sur les machines.

8 Si, malgré la page d'avertissements, vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel Rapid Recovery Agent se déploie sur les machines spécifiées. Ces machines ne sont pas encore protégés. Pour les protéger, reportez-vous à la rubrique « Protection de plusieurs machines dans le domaine Active Directory » du manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation*.

Déploiement vers des machines présentes sur un hôte virtuel VMware vCenter/ESX(i)

Cette procédure permet de déployer simultanément le logiciel Rapid Recovery Agent sur une ou plusieurs machines d'un même hôte virtuel VMware vCenter/ESX(i).
Avant de démarrer cette procédure, munissez-vous des informations suivantes :

- les identifiants pour l'hôte virtuel VMware VCenter/ESX(i)
- l'emplacement de l'hôte
- les identifiants de connexion pour chacune des machines à protéger

REMARQUE : Les outils VMware doivent être installés sur toutes les machines virtuelles ; sinon, Rapid Recovery serait dans l'incapacité de détecter le nom d'hôte de la machine virtuelle sur laquelle effectuer le déploiement. Au lieu du nom d'hôte, Rapid Recovery utilise le nom de la machine virtuelle, ce qui peut entraîner des problèmes si le nom d'hôte est différent de celui de la machine virtuelle.

1 Sur la console Rapid Recovery Core, cliquez sur le menu déroulant **Protéger**, puis sur **Déployer le logiciel Agent**.

L'**Assistant de déploiement du logiciel Agent** s'ouvre.

2 Dans la page **Connexion** de l'assistant, dans la liste déroulante **Source**, sélectionnez **vCenter/ESX(i)**.

3 Entrez les informations d'hôte et les identifiants comme dans le tableau suivant.

Tableau 5. Paramètres de connexion VCenter/ESX(i)

Zone de texte	Description
Hôte	Le nom ou l'adresse IP du serveur VMware vCenter ou de l'hôte virtuel ESX(i).
Port	Le port utilisé pour se connecter à l'hôte virtuel. Le paramètre par défaut est 443.

Zone de texte	Description
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à l'hôte virtuel ; par exemple, Administrateur ou, si la machine se trouve dans un domaine, [nom de domaine] \Administrateur).
Mot de passe	Le mot de passe sécurisé utilisé pour se connecter à cet hôte virtuel.

4 Cliquez sur **Suivant**.

5 Dans la page **Machines** de l'assistant, sélectionnez l'une des options suivantes dans le menu déroulant :

- Hôtes et clusters
- Machines virtuelles et modèles

6 Développez la liste de machines, puis sélectionnez les machines virtuelles vers lesquelles vous souhaitez déployer le logiciel.

Une notification s'affiche si Rapid Recovery détecte qu'une machine est hors ligne ou que les outils VMware ne sont pas installés.

7 Si vous souhaitez redémarrer les machines automatiquement une fois le déploiement effectué, sélectionnez **Après l'installation d'Agent, redémarrer automatiquement les machines (recommandé)**.

8 Cliquez sur **Suivant**.

Rapid Recovery vérifie automatiquement chacune des machines que vous avez sélectionnées.

9 Dans la page **Réglages** de l'assistant, entrez les identifiants pour chaque machine dans le format suivant : `hostname::username::password`.

REMARQUE : Entrez une machine par ligne.

10 Cliquez sur **Terminer**.

Le système vérifie automatiquement chacune des machines que vous avez sélectionnées.

Si Rapid Recovery détecte des problèmes pendant la vérification automatique, l'Assistant passe à une page d'avertissements, dans laquelle vous pouvez effacer des machines de la sélection et les vérifier manuellement. Si les machines que vous avez ajoutées réussissent la vérification automatique, elles apparaissent dans le volet Déployer Agent sur les machines.

11 Si, malgré la page d'avertissements, vous êtes satisfait de vos sélections, cliquez à nouveau sur **Terminer**.

Le logiciel Rapid Recovery Agent se déploie vers les machines spécifiées.

À propos de l'installation du logiciel Agent sur des machines Linux

Utilisez les conseils suivants lorsque vous installez le logiciel Agent sur des machines Linux que vous souhaitez protéger. Une fois l'installation terminée, configurez l'agent, comme expliqué dans la rubrique « Configuration de Rapid Recovery Agent sur une machine Linux » du *Dell Data Protection | Rapid Recovery 6.0 – Guide d'installation et de mise à niveau*.

PRÉCAUTION : Après avoir configuré le logiciel Agent que vous venez d'installer sur une machine Linux, redémarrez cette dernière. Le redémarrage garantit que la version du pilote du noyau utilisée pour protéger votre machine est la bonne version.

La méthode pour l'installation et le retrait du logiciel Agent sur des machines Linux a changé. À partir de la version 6.0.1, les facteurs suivants s'appliquent :

- Un seul ensemble d'instructions s'applique aux installations d'Agent sur une machine Linux accédant à Internet. L'on parle alors d'installation en ligne. Au lieu d'utiliser des scripts shell, l'on utilise des gestionnaires de packages pour installer ou retirer le logiciel Rapid Recovery d'un référentiel référencé sur la machine Linux.

  REMARQUE : Le référentiel sert à préparer les fichiers pertinents pour les gestionnaires de packages. Ce référentiel n'a rien à voir avec le référentiel Rapid Recovery.

- Si vous installez l'agent sur une machine Linux sans accès à Internet (une machine isolée, par exemple, ou une machine autonome sécurisée), l'on parle alors d'installation hors ligne. Pour ce processus, vous devrez d'abord télécharger un package d'installation depuis une machine Linux accédant à Internet, puis vous devrez déplacer ces fichiers d'installation vers l'ordinateur sécurisé.

Les différentes distributions Linux prises en charge utilisant différents gestionnaires de packages pour l'installation en ligne, la procédure à suivre pour l'installation, la mise à niveau ou le retrait d'Agent sur des systèmes d'exploitation Linux pris en charge dépendent du

gestionnaires de packages utilisé. Les gestionnaires de packages et les distributions Linux qu'ils prennent en charge sont décrits dans le tableau suivant.

Tableau 6. Les gestionnaires de packages et les distributions Linux qu'ils prennent en charge

Gestionnaire de packages	Distribution Linux
yum	Le gestionnaire de packages yum prend en charge les distributions Linux basées sur Red Hat Enterprise Linux (RHEL) : RHEL, CentOS et Oracle Linux.
zypper	SUSE Linux Enterprise Server (SLES) versions 11, 12
apt	Distributions Linux basées sur Debian : Debian 7 ou 8 et Ubuntu 12.04 et versions ultérieures.

Pour chaque machine Linux que vous configurez, vous devez configurer votre référentiel local de logiciels pour que ce dernier pointe vers l'emplacement où le gestionnaire de packages se procure les fichiers d'installation de Dell Rapid Recovery.

REMARQUE : Ce processus est représenté par les étapes 1 à 4 de chacune des procédures d'installation. Lors des mises à niveau des futures éditions de Rapid Recovery Agent sur une machine Linux où le référentiel à l'espace configuré, vous n'aurez plus besoin de reconfigurer votre référentiel de logiciels.

Après que vous aurez configuré un référentiel de logiciels sur votre machine Linux, le gestionnaire de packages sera en mesure de récupérer et installer les packages nécessaires pour l'installation ou le retrait de Rapid Recovery Agent et de ses composants : aamount (maintenant appelé local mount), aavdisk (maintenant appelé rapidrecovery-vdisk), et Mono (un ensemble d'outils open source conformes Ecma et compatibles avec .NET Framework, servant au portage du logiciel Agent sur les plates-formes Linux).

Pour chaque gestionnaire de packages, vous pouvez exécuter en ligne de commande la commande appropriée au gestionnaire pour déterminer si ce dernier est configuré pour télécharger des packages Rapid Recovery. Ces commandes sont répertoriées dans le tableau suivant.

Tableau 7. Commande permettant d'afficher la configuration des référentiels dans les divers gestionnaires de packages

Gestionnaire de packages	Commande affichant la liste des référentiels configurés
yum	yum replolist
zypper	zypper repos
apt	ls /etc/apt/sources.list.d

Les versions précédentes du logiciel AppAssure Agent doivent être complètement retirées d'une machine Linux avant d'installer la version de Rapid Recovery Agent et de protéger la machine Linux avec Rapid Recovery Core. Cela est vrai pour les deux types d'installations : en ligne ou hors ligne. Le retrait d'AppAssure Agent passe par l'utilisation de scripts shell. Les instructions de désinstallation peuvent varier selon la distribution Linux utilisée. Pour en savoir plus sur la désinstallation d'AppAssure Agent à partir d'une machine Linux, reportez-vous à la rubrique « Désinstallation du logiciel AppAssure Agent à partir d'une machine Linux » du *Dell Data Protection | Rapid Recovery 6.0 – Guide d'installation et de mise à niveau*.

REMARQUE : Le retrait du nouveau logiciel Rapid Recovery Agent utilise le gestionnaire de packages de pour chaque distribution. Par conséquent, en cas de désinstallation d'une version de Rapid Recovery Agent, reportez-vous à la procédure appropriée sous la rubrique reportez-vous à la rubrique « Désinstallation du logiciel AppAssure Agent à partir d'une machine Linux » du *Dell Data Protection | Rapid Recovery 6.0 – Guide d'installation et de mise à niveau*.

Si vous installez Rapid Recovery Agent sur une machine Linux sur laquelle AppAssure Agent n'a jamais été installé, utilisez le tableau précédent pour déterminer quel est le gestionnaire de packages approprié. Puis, appliquez la procédure d'installation appropriée.

Après avoir configuré le logiciel Agent que vous venez d'installer sur une machine Linux, vous devrez redémarrer cette dernière. Le redémarrage garantit que la version du pilote du noyau utilisée pour protéger votre machine est la bonne version.

Ainsi, le processus d'installation lorsque vous effectuez une mise à niveau à partir d'AppAssure vers Rapid Recovery implique les actions suivantes :

- retirer le logiciel AppAssure Agent (non requis pour les installations de première fois)
- déterminer le gestionnaire de packages correspondant à votre distribution Linux
- appliquer la procédure à suivre pour l'installation de Rapid Recovery Agent sur la machine Linux, y compris la configuration du référentiel de logiciels (étapes 1 à 4 de la procédure d'installation)
- exécuter l'utilitaire de configuration pour définir le port, configurer les utilisateurs, ajouter des exclusions de pare-feu, installer le module de noyau, et démarrer le service Agent
- redémarrer la machine Linux

Les instructions pour l'installation du logiciel Agent sur une machine Linux diffèrent légèrement selon la distribution Linux utilisée. Pour plus d'informations sur la préparation et l'installation du logiciel Agent sur une machine Linux connectée à Internet, reportez-vous à la rubrique appropriée. Vous avez le choix entre les sections suivantes :

- Installation sur Debian ou Ubuntu du logiciel Rapid Recovery Agent
- Installation du logiciel Rapid Recovery Agent sur SUSE Linux Enterprise Server

Pour plus d'informations sur la préparation et l'installation du logiciel Agent sur une machine Linux non connectée à Internet, reportez-vous à la rubrique :

- Installer le logiciel Agent sur des machines Linux hors ligne

Avant de commencer l'installation du logiciel Agent, reportez-vous aux rubriques du *Dell Data Protection | Rapid Recovery 6.0 – Guide d'installation et de mise à niveau* : Télécharger la distribution Linux ; À propos de la sécurité, Emplacement des fichiers Agent Linux ; Dépendances Agent ; Informations pour les scripts Linux.

Emplacement des fichiers de l'agent Linux

Il existe plusieurs fichiers requis pour prendre en charge le logiciel Agent Rapid Recovery sur une machine Linux. Pour toutes les distributions Linux prises en charge, ces fichiers se trouvent dans les répertoires suivants :

- mono :
  `/opt/apprecovery/mono`
- agent :
  `/opt/apprecovery/agent`
- Montage local :
  `/opt/apprecovery/local_mount`
- rapidrecovery-vdisk et aavdctl :
  `/usr/bin/aavdisk`
- Fichiers de configuration pour rapidrecovery-vdisk :
  `/etc/apprecovery/aavdisk.conf`
- Wrappers pour Agent et local_mount
  `/usr/bin/agent`
  `/usr/bin/local_mount`
- scripts d'exécution automatique pour Agent et rapidrecovery-vdisk :
  `/etc/init.d/rapidrecovery-agent`
  `/etc/init.d/rapidrecovery-vdisk`

Dépendances de l'agent

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

- Pour Debian et Ubuntu :
  - rapidrecovery-agent exige les éléments suivants :

    ```
    dkms, gcc, make, linux-headers-`uname-r`
                    libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
    ```

  - rapidrecovery-mono exige les éléments suivants :

    ```
    libc6 (>=2.7-18)
    ```

- Pour Red Hat Enterprise Linux, CentOS et Oracle Linux :
  - nbd-dkms exige

    ```
    dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`
    ```

  - rapidrecovery-agent exige les éléments suivants :

    ```
    dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`,
                    nbd-dkms, libblkid, pam, pcre
    ```

  - rapidrecovery-mono exige les éléments suivants :

    ```
    glibc >=2.11
    ```

- Pour SUSE Linux Enterprise Server
  - nbd-dkms exige

    ```
    dkms, gcc, make, kernel-syms
    ```

  - rapidrecovery-agent exige les éléments suivants :

    ```
    dkms, kernel-syms, gcc, make, libblkid1, pam, pcre
    ```

  - rapidrecovery-mono exige les éléments suivants :

    ```
    glibc >= 2.11
    ```

Installation sur Debian ou Ubuntu du logiciel Rapid Recovery Agent

Le fichier .deb de Rapid Recovery Agent est une archive contenant des informations de référentiel spécifiques au gestionnaire de packages apt. Procédez comme suit pour installer Rapid Recovery Agent sur des machines Debian ou Ubuntu machines dans le cadre d'une installation en ligne.

REMARQUE : Cette procédure s'applique à une machine Linux qui est connectée à Internet. Pour une installation hors ligne de Rapid Recovery Agent sur une machine Linux, voir Installer le logiciel Agent sur des machines Linux hors ligne.

1 Ouvrez une session de terminal avec accès root.

2 Déterminez votre répertoire de travail actuel en entrant PWD et en appuyant sur **Entrée**. Pour notre exemple, nous supposerons que votre répertoire est **/home/rapidrecovery/**.

3 Téléchargez vers votre répertoire de travail actuel le fichier .deb d'installation de Rapid Recovery approprié depuis le portail de licences depuis https://licenseportal.com.

Pour plus d'informations sur le portail de licences, voir le manuel *Portail des licences Dell Data Protection | Rapid Recovery – Guide d'utilisation*.

4 Pour établir une connexion persistante entre votre machine Linux et le référentiel Dell distant où se trouvent stockés le logiciel et les composants Rapid Recovery, tapez la commande suivante :

```
dpkg -i <.deb installation file you downloaded>
```

Par exemple, si le fichier du programme d'installation est nommé rapidrecovery-repo-6.0.2.999 .deb dans le répertoire **/home/rapidrecovery/**, tapez la commande suivante, puis appuyez sur **Entrée** :

```
dpkg -i rapidrecovery-repo-6.0.2.999.deb
```

Tous les packages ou fichiers requis par l'agent et qui sont manquants seront téléchargés depuis le référentiel distant et installés automatiquement dans le cadre du script.

REMARQUE : Pour plus d'informations sur les dépendances pour une installation sur machine Linux, voir . Dépendances de l'agent.

5 Installez Rapid Recovery Agent en invoquant le gestionnaire de packages apt, en mettant à jour le gestionnaire de référentiel. Tapez la commande suivante, puis appuyez sur **Entrée** :

```
apt-get update
```

6 Demandez au gestionnaire de packages d'installer le logiciel Rapid Recovery Agent. Tapez la commande suivante, puis appuyez sur **Entrée** :

```
apt-get install rapidrecovery-agent
```

7 Le gestionnaire de packages se prépare à installer tous les fichiers dépendants. Si le système vous invite à confirmer l'installation de fichiers non signés, entrez **y**, puis appuyez sur **Entrée**.

Les fichiers Rapid Recovery Agent sont installés.

Installation du logiciel Rapid Recovery Agent sur SUSE Linux Enterprise Server

Le fichier .rpm de Rapid Recovery Agent est une archive contenant des informations de référentiel pour SUSE Linux Enterprise Server (SLES) . Cette distribution utilise le gestionnaire de packages zypper. Procédez comme suit pour installer Rapid Recovery Agent sur SLES.

REMARQUE : Cette procédure s'applique à une machine Linux qui est connectée à Internet. Pour une installation hors ligne de Rapid Recovery Agent sur une machine Linux, voir Installer le logiciel Agent sur des machines Linux hors ligne.

1 Ouvrez une session de terminal avec accès root.

2 Déterminez votre répertoire de travail actuel en entrant PWD et en appuyant sur **Entrée**. Pour notre exemple, nous supposerons que votre répertoire est **/home/rapidrecovery/**.

3 Téléchargez vers votre répertoire de travail actuel le fichier .rpm d'installation de Rapid Recovery Agent approprié depuis le portail de licences (https://licenseportal.com).

Pour plus d'informations sur le portail de licences, voir le manuel *Portail des licences Dell Data Protection | Rapid Recovery – Guide d'utilisation*.

4 Pour établir une connexion persistante entre votre machine Linux et le référentiel Dell distant où se trouvent stockés le logiciel et les composants Rapid Recovery, tapez la commande suivante :

```
rpm -ivh <.rpm installation file you downloaded>
```

Par exemple, si le fichier du programme d'installation est nommé rapidrecovery-repo-6.0.2.999.rpm dans le répertoire **/home/rapidrecovery/**, tapez la commande suivante, puis appuyez sur **Entrée** :

```
rpm -ivh rapidrecovery-repo-6.0.2.999.rpm
```

Tous les packages ou fichiers requis par l'agent et qui sont manquants seront téléchargés depuis le référentiel distant et installés automatiquement dans le cadre du script.

REMARQUE : Pour plus d'informations sur les dépendances pour une installation sur machine Linux, voir Dépendances de l'agent.

5 Installez Rapid Recovery Agent en invoquant le gestionnaire de packages zypper, en mettant à jour le gestionnaire de référentiel. Tapez la commande suivante, puis appuyez sur **Entrée** :

```
apt-get update
```

6 Demandez au gestionnaire de packages d'installer le logiciel Rapid Recovery Agent. Tapez la commande suivante, puis appuyez sur **Entrée** :

```
apt-get install rapidrecovery-agent
```

7 Le gestionnaire de packages se prépare à installer tous les fichiers dépendants. Si le système vous invite à confirmer l'installation de fichiers non signés, entrez **y** , puis appuyez sur **Entrée**.

Les fichiers Rapid Recovery Agent sont installés.

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 requis par l'agent, voir Dépendances de l'agent.

Une fois l'installation terminée, l'agent s'exécute sur votre machine. Pour en savoir plus sur la protection de cette machine avec le core, voir la rubrique « Protection des stations de travail et des serveurs » dans le manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation* sur **Dell.com/support/home**.

Installer le logiciel Agent sur des machines Linux hors ligne

Cette tâche nécessite d'accéder à une machine Linux en ligne, à un support de stockage amovible et à la machine Linux hors ligne, qui est la destination finale. Si AppAssure Agent est installé sur la machine Linux hors ligne, vous devez d'abord le désinstaller avant d'installer Rapid Recovery Agent. Pour plus d'informations, reportez-vous à la section « Désinstallation du logiciel AppAssure Agent sur une machine Linux » du manuel *Dell Data Protection | Rapid Recovery – Guide d'installation et de mise à niveau*.

Pour une installation du logiciel Agent sur des machines Linux qui n'ont pas accès à Internet, procédez comme suit. Une fois l'installation terminée, configurez l'agent, comme expliqué dans la rubrique Configuration de Rapid Recovery Agent sur une machine Linux.

REMARQUE : En cas d'installation sur plusieurs distributions Linux, exécutez cette procédure une fois pour chaque distribution.

1 À partir d'une machine Linux ayant accès à Internet, ouvrez une fenêtre de terminal et tapez la commande suivante :

```
wget http://s3.amazonaws.com/repolinux/6.0.2/packages-downloader.sh
```

Le script de shell se télécharge vers votre répertoire courant.

2 Exécutez le script de script de shell à l'aide de la commande suivante :

```
bash packages-downloader.sh
```

Le script s'exécute et vous invite à choisir une distribution Linux et une architecture spécifiques.

3 Entrez l'index du package d'installation souhaité et appuyez sur **Entrée**.

Par exemple, pour obtenir un package d'installation pour Red Hat Enterprise Linux 7, entrez 3, puis appuyez sur **Entrée**.

Le programme d'installation approprié est extrait vers le répertoire **~/rapidrecovery.packages/**.

REMARQUE : Les caractères ~/ représentent votre répertoire personnel.

4 Copiez les packages Rapid Recovery Agent vers un support amovible. L'emplacement spécifique de votre support amovible peut varier selon la distribution Linux. Tapez la commande suivante et appuyez sur **Entrée** :

```
cp -R ~/rapidrecovery.packages/ <your_removable_media>
```

Par exemple, si vous utilisez un lecteur USB amovible qui est monté à l'emplacement /media/USB drive-1, tapez la commande suivante et appuyez sur **Entrée** :

```
cp -R ~/rapidrecovery.packages /media/USB-drive-1
```

Tous les fichiers nécessaires sont copiés vers le support amovible.

5 Apportez le support amovible à la machine Linux hors ligne et montez le lecteur.

6 À partir du périphérique monté, copiez les données vers votre répertoire personnel ou vers un autre emplacement de votre choix. Par exemple, tapez la commande suivante et appuyez sur **Entrée** :

```
cp -R /media/USB-drive-1 ~/rapidrecovery.packages
```

7 Allez au répertoire Rapid Recovery. Par exemple, tapez la commande suivante et appuyez sur **Entrée** :

```
cd ~/rapidrecovery.packages
```

8 Exécutez l'installation d'Agent avec des privilèges root. Cette commande varie selon la distribution Linux utilisée.

- Pour Red Hat, SLES, Oracle et CentOS, tapez la commande suivante et appuyez sur **Entrée** :

  ```
  sudo rpm -i *.rpm
  ```

- Pour Debian et Ubuntu, tapez la commande suivante et appuyez sur **Entrée** :

  ```
  sudo dpkg -i *.deb
  ```

Le gestionnaire de packages local exécute l'installation de Rapid Recovery Agent.

Une fois l'installation terminée, configurez l'agent, comme expliqué dans la rubrique Configuration de Rapid Recovery Agent sur une machine Linux.

PRÉCAUTION : Après avoir configuré le logiciel Agent que vous venez d'installer sur une machine Linux, vous devrez redémarrer cette dernière. Le redémarrage garantit que la version du pilote du noyau utilisée pour protéger votre machine est la bonne version.

Installer le logiciel Agent sur des machines Windows Server Core Edition

Procédez comme suit pour installer le logiciel Agent sur une machine Windows Server Core.

REMARQUE : La procédure suivante installe le logiciel Agent en mode console. Pour une installation en mode silencieux, faites suivre le nom de fichier du programme d'installation de `/silent` sur la ligne de commande. Par exemple, `Agent-X64-6.X.X.xxxxx.exe /silent`.

1 Téléchargez le fichier du programme d'installation de Rapid Recovery Agent depuis le Portail des licences Dell Data Protection | Rapid Recovery ou depuis Rapid Recovery Core.

2 À partir d'une invite de commande, accédez au répertoire contenant le fichier du programme d'installation de Rapid Recovery Agent et entrez le nom de ce fichier pour commencer l'installation :

```
Agent-X64-6.x.x.xxxxx.exe
```

Le programme installe le logiciel Agent et affiche l'avancement de l'installation dans la console. Une fois l'opération terminée, les nouvelles installations déclenchent un redémarrage automatique de la machine, alors que les mises à niveau d'Agent peuvent ne pas nécessiter un redémarrage de la machine.

Configuration de Rapid Recovery Agent sur une machine Linux

Après avoir installé Rapid Recovery Agent sur une machine Linux, exécutez l'utilitaire de configuration de Rapid Recovery. Cet utilitaire compilera et installera le module noyau sur la machine Linux que vous souhaitez protéger sur votre core.

L'utilitaire de configuration propose plusieurs options de configuration et offre des conseils aux différents stades numérotés de la procédure lorsqu'il détecte votre configuration spécifique.

Procédez comme suit pour configurer Rapid Recovery Agent sur une machine Linux. Certaines options de configuration peuvent varier en fonction de la distribution Linux que vous installez.

1 Ouvrez une session de terminal avec accès root.

2 Lancez l'utilitaire de configuration en tapant la commande suivante, puis appuyez sur Entrée :

```
sudo /usr/bin/rapidrecovery-config
```

L'utilitaire de configuration démarre et affiche une liste d'options de configuration, chacune portant un numéro d'index permettant d'entrer dans la configuration appropriée.

3 En tapant la commande suivante, configurez le port pour cette machine protégée, puis appuyez sur Entrée. Le port par défaut est 8006.

```
1 <agent_port>
```

Par exemple, si vous utilisez le port par défaut, entrez la commande suivante :

```
1 8006
```

4 Configurez les utilisateurs disponibles pour la protection, en tapant la commande suivante, puis appuyez sur Entrée :

```
1 <user_names_separated_by_comma>
```

Par exemple, si vous utilisez des noms d'utilisateur michael, administrateur et test_user1, tapez la commande suivante :

```
2 michael,administrator,test_user1
```

5 Configurez des règles de pare-feu pour sélectionner un gestionnaire de configuration de pare-feu. Cela va créer les exceptions de pare-feu pour le port désigné en 1.

Si l'utilitaire détecte un ou plusieurs gestionnaires de configuration de pare-feu (comme lokkit ou firewalld), chacun de ces gestionnaires sera répertorié dans l'utilitaire à la ligne 3. Sélectionnez le gestionnaire approprié manager et entrez-le, en commençant par le numéro de commande (3), puis appuyez sur Entrée :

```
3 <firewall_configuration>
```

Par exemple, si vous utilisez firewalld, tapez la commande suivante :

```
3 firewalld
```

6 À partir de l'utilitaire, interrogez la liste des modules de noyau compatibles en entrant le numéro de commande, puis appuyez sur Entrée :

```
4
```

Un sous-shell renvoie la liste de tous les modules de noyau compatibles pour l'installation. Exemple :

```
Searching for all available for installation kernels.
This might take a while, depending on the Internet connection speed.
Kernels compatible for module installation:
 0 - linux-image-3.16.0.23-generic
 1 - linux-image-3.16.0.31-generic
```

```
 2 - linux-image-3.16.0.33-generic
 3 - linux-image-3.16.0.34-generic
Input indices of the kernel modules you wish to install, delimited by space; use 'all' to
install into all supported kernels, or 'q' to quit.
```

7 Configurez le module de noyau Rapid Recovery approprié.

Par exemple, pour entrer les modules de noyau pour 3.16.0-23 et 3.16.0-34, entrez `1 4` et appuyez sur Entrée.

Pour entrer tous les modules de noyau, entrez `all` et appuyez sur Entrée.

8 Après avoir configuré le logiciel Agent que vous venez d'installer, redémarrez la machine. Le redémarrage garantit que la version du pilote du noyau utilisée pour protéger votre machine est la bonne version.

Après avoir terminé ce processus, le référentiel local a été configuré sur cette machine Linux. Le logiciel Agent est installé et le module de noyau est chargé.

Lors de la prochaine étape, vous protégerez la machine sur le core Rapid Recovery.

Protection d'une machine

Si vous avez déjà installé le logiciel Rapid Recovery Agent sur la machine à protéger, mais que vous n'avez pas encore redémarré celle-ci, faites-le maintenant.

Cette rubrique explique comment démarrer la protection des données sur la machine que vous spécifiez à l'aide de l'Assistant de protection de machines.

Lorsque vous ajoutez une protection, vous devez définir des informations de connexion (adresse IP et port). Vous devez également fournir les identifiants de connexion à la machine à protéger. Facultativement, vous pouvez fournir le nom qui s'affichera dans la console Core à la place de l'adresse IP. Dans ce cas, vous ne verrez pas l'adresse IP de la machine protégée lorsque vous afficherez ses détails de la console Core. Vous définirez également la planification de protection de la machine.

Le workflow de l'assistant de protection peut varier légèrement en fonction de votre environnement. Par exemple, si le logiciel Rapid Recovery Agent est installé sur la machine à protéger, vous ne serez pas invité à l'installer à partir de l'assistant. De même, si un référentiel existe déjà sur le core, vous ne serez pas invité à en créer un.

1 Effectuez l'une des opérations suivantes :

- Si vous procédez à partir de l'Assistant de protection de machines, passez à l'étape 2.
- Si vous procédez à partir de la console Rapid Recovery Core, dans la barre de boutons, cliquez sur **Protéger**.

L'**Assistant de protection de machines** s'affiche.

2 Dans la page **Accueil**, sélectionnez les options d'installation appropriée :

- Si vous n'avez pas besoin de définir un référentiel ni d'établir de chiffrement, sélectionnez **Normal**.
- Si vous avez besoin de créer un référentiel ou définir un référentiel différent pour les sauvegardes de la machine sélectionnée, ou si vous souhaitez établir un chiffrement à l'aide de l'assistant, sélectionnez **Avancé (afficher les étapes facultatives)**.
- Le cas échéant, si vous ne souhaitez plus voir la page **Accueil** de l'Assistant de protection de machines à l'avenir, cochez l'option **Ignorer cette page d'accueil à la prochaine ouverture de l'Assistant**.

3 Lorsque vous êtes satisfait de vos choix dans la page d'accueil, cliquez sur **Suivant**.

La page **de connexion** s'affiche.

4 Dans la page **Connexion**, entrez les informations concernant la machine à laquelle vous souhaitez vous connecter (voir le tableau suivant), puis cliquez sur **Suivant**.

Tableau 8. Paramètres de connexion machine

Zone de texte	Description
Hôte	Le nom d'hôte ou l'adresse IP de l'ordinateur que vous souhaitez protéger.
Port	Le numéro du port sur lequel Rapid Recovery Core communique avec l'agent sur la machine. Le numéro de port par défaut est 8006.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter à cette machine ; par exemple, Administrateur (ou, si la machine se trouve dans un domaine, [nom de domaine] \Administrateur).
Mot de passe	Le mot de passe utilisé pour se connecter à cette machine

Si la page **Installer l'agent** s'affiche ensuite dans l'Assistant de protection de machines, cela veut dire que Rapid Recovery ne détecte pas Rapid Recovery Agent sur la machine et qu'il va installer la version actuelle du logiciel. Allez à l'étape 7.

Si la page **Mettre à niveau Agent** s'affiche ensuite dans l'assistant, cela veut dire qu'il existe une ancienne version du logiciel Agent sur la machine à protéger.

REMARQUE : Le logiciel Agent doit être installé sur la machine à protéger, et la machine doit être redémarrée avant de pouvoir être sauvegardée vers le core. Pour que le programme d'installation redémarre la machine protégée, sélectionnez l'option Après l'installation, redémarrer automatiquement la machine (recommandé) avant de cliquer sur Suivant.

5 Dans la page **Mettre à niveau Agent**, effectuez l'une des actions suivantes :

- Pour déployer la nouvelle version du logiciel Agent (correspondant la version de Rapid Recovery Core), sélectionnez **Mettre à niveau Agent vers la dernière version du logiciel**.
- Pour continuer la protection de la machine sans mise à jour de la version du logiciel Agent, désélectionnez l'option **Mettre à niveau Agent vers la dernière version du logiciel**.

6 Cliquez sur **Suivant**.

7 Si vous le désirez, dans la page **Protection**, si vous voulez que, pour la machine protégée, s'affiche dans la console Rapid Recovery Core un autre nom que son adresse IP, dans le champ **Nom d'affichage**, entrez ce nom dans la boîte de dialogue.

Vous pouvez entrer un maximum de 64 caractères. N'utilisez pas les caractères spéciaux décrits dans la rubrique « Caractères interdits » du manuel *Rapid Recovery sur appliances DL – Guide d'utilisation*. En outre, ne faites pas commencer le nom d'affichage par l'une des combinaisons de caractères décrites dans la rubrique « Expressions interdites » du manuel *Rapid Recovery sur appliances DL – Guide d'utilisation*.

8 Sélectionnez la planification de protection appropriée expliquée ci-dessous :

- Pour utiliser la planification de protection par défaut, accédez à l'option Paramètres de planification, sélectionnez **Protection par défaut**.

Avec la planification de protection par défaut, le Core prend une fois par heure des instantanés de tous les volumes sur la machine protégée. Pour modifier les paramètres de protection à tout moment après avoir fermé l'Assistant, y compris pour le choix des volumes à protéger, accédez à la page Résumé de la machine protégée.

- Pour définir une planification de protection différente dans l'option Paramètres de planification, sélectionnez **Protection personnalisée**.

9 Effectuez la configuration comme suit :

- Si vous avez sélectionné une configuration standard dans l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Terminer** pour confirmer vos choix, fermer l'Assistant et protéger la machine spécifiée.

  Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.
- Si vous avez sélectionné une configuration standard pour l'Assistant de protection de machines et défini une protection personnalisée, cliquez sur **Suivant** pour configurer une planification de protection personnalisée. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à la section « Création de planifications de protection personnalisées » dans le manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation*.

- Si vous avez sélectionné la configuration Avancée pour l'Assistant de protection de machines et choisi la protection par défaut, cliquez sur **Suivant** et passez à l'étape 14 pour afficher les options de référentiel et de chiffrement.
- Si vous avez sélectionné la configuration Avancée pour l'Assistant de protection de machines et spécifié la protection personnalisée, cliquez sur **Suivant** et passez à l'étape 11 pour choisir les volumes à protéger.

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

REMARQUE : En règle générale, il est recommandé de protéger, au minimum, le volume réservé au système et le volume contenant le système d'exploitation (généralement le lecteur C).

11 Dans la page **Planification de la protection**, définissez une planification de protection personnalisée et cliquez sur **Suivant**. Pour plus de détails sur la définition d'une planification de protection personnalisée, reportez-vous à la section « Création de planifications de protection personnalisées » dans le manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation*.

Si le référentiel est déjà configuré, et que vous avez sélectionné l'option Avancé à l'étape 1, la page Chiffrement s'affiche. Passez à l'étape 13.

12 Si vous le souhaitez, dans la page **Chiffrement**, pour activer le chiffrement, sélectionnez **Activer le chiffrement**.

Les champs de clé de chiffrement apparaissent dans la page **Chiffrement**.

REMARQUE : Si vous l'activez, le chiffrement sera appliqué aux données de tous les volumes protégés de cette machine. Vous pouvez modifier ultérieurement les paramètres de chiffrement à partir de la console Rapid Recovery Core. Pour plus d'informations sur le chiffrement, reportez-vous à la rubrique « Comprendre les clés de chiffrement » dans le manuel *Rapid Recovery 6.0 sur appliances DL – Guide d'utilisation* sur www.dell.com/support/home.

PRÉCAUTION : Rapid Recovery utilise le chiffrement AES 256 bits en mode CBC (Cipher Block Chaining) avec des clés de 256 bits. Bien que l'utilisation du chiffrement soit facultative, Dell vous recommande vivement de créer une clé de chiffrement et de protéger la phrase de passe que vous définissez. Stockez cette phrase de passe en un endroit sûr, car elle est d'une importance capitale pour la restauration des données. Sans la phrase de passe, la récupération des données est impossible.

13 Dans la page **Chiffrement**, sélectionnez l'une des options suivantes :

- Si vous souhaitez chiffrer cette machine protégée à l'aide d'une clé de chiffrement qui est déjà définie dans ce core Rapid Recovery, sélectionnez **Chiffrer les données à l'aide d'une clé de chiffrement**, puis sélectionnez la clé appropriée dans le menu déroulant. Passez à l'étape suivante.
- Si vous souhaitez ajouter au core une nouvelle clé de chiffrement et appliquer cette clé à cette machine protégée, entrez les informations décrites dans le tableau suivant.

Tableau 9. Paramètres de clé de chiffrement

Zone de texte	Description
Nom	Entrez un nom pour la clé de chiffrement. Les noms de clés de chiffrement doivent contenir entre 1 et 130 caractères alphanumériques. Vous ne pouvez pas inclure de caractères spéciaux (barre oblique inverse, barre oblique normale, barre verticale, deux-points, astérisque, guillemets, point d'interrogation, parenthèse ouvrante ou fermante, et commercial ou dièse). Ces informations apparaissent dans le champ Description lorsqu'on affiche les clés de chiffrement depuis la console Core.
Description	Entrez un commentaire pour la clé de chiffrement. Ces informations s'affichent dans le champ Description lors de l'affichage des clés de chiffrement dans la console Core.
Phrase de passe	Entrez la phrase de passe utilisée pour contrôler l'accès. La bonne pratique consiste à éviter d'utiliser les caractères spéciaux mentionnés ci-dessus. Notez la phrase de passe dans un endroit sûr. Le support Dell ne peut pas récupérer de phrase de passe. Une fois que vous avez créé une clé de chiffrement et que vous l'avez appliquée à une ou plusieurs machines protégées, vous ne pourrez pas restaurer les données si vous perdez la phrase de passe.

Zone de texte	Description
Confirmer la phrase de passe	Entrez de nouveau la phrase de passe que vous venez de saisir.

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

Lorsque vous ajoutez pour la première fois la protection à une machine, une image de base (un instantané de toutes les données présentes dans les volumes protégés) se transfère vers le référentiel sur le core Rapid Recovery conformément à la planification que vous avez définie, sauf si vous avez demandé la suspension initiale de la protection.

15 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 Rapid Recovery et RPC sont bien 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 DL1000 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 DL1000, 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 DL1000.

Association de cartes réseau

Par défaut, les cartes réseau (NIC) de l'appliance DL1000 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 DL1000 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.

5

Obtention d'aide

Où trouver la documentation et les mises à jour du logiciel

Il existe dans la console Rapid Recovery Core des liens directs vers la documentation et les mises à jour du logiciel Rapid Recovery et de l'appliance DL1000.

Documentation

Pour accéder au lien de documentation :

1 dans la console Core, 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 console Core, cliquez sur l'onglet **Appliance** .

2 Dans le volet de gauche, accédez au lien**Appliance** > **Mises à jour de logiciel**.

Contacter Dell

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

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

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.