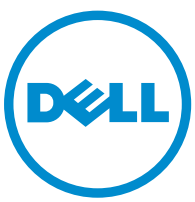
Appliance Dell DL4300
Guide de déploiement



Remarques, précautions et avertissements

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

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

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

2016 - 05

Rév. A02

Table des matières

1

Configuration de l’appliance DL4300

Introduction

L’appliance Dell DL4300 représente la nouvelle génération d'appliances de protection de sauvegarde sur disque effectuée par le logiciel Dell AppAssure. L'appliance permet :

- des fonctions de stockage adaptables pour la prise en charge d'entreprises de toutes tailles
- 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
- la configuration potentielle de Fibre Channel

Termes utilisés dans ce document

Le tableau suivant présente les termes utilisés dans ce document pour faire référence à divers composants matériels et logiciels de l'appliance DL4300.

Tableau 1. Composants matériels et logiciels de l’appliance DL4300

Composant	Terme utilisé
Appliance DL4300	Serveur
Boîtier de stockage Dell Storage MD1400	Boîtier de stockage
Logiciel Dell AppAssure	AppAssure

Configurations disponibles

L'appliance DL est disponible en deux configurations : Édition Standard et Édition Capacité élevée.

Tableau 2. Configurations de la capacité de DL4300 Édition Standard

Capacité	Configuration matérielle
5 To	12 disques de 1 To, 4 disques internes de 1 To
10 à 20 To	12 disques de 2 To, 4 disques internes de 2 To
30 à 40 To	12 disques de 4 To, 4 disques internes de 4 To
50 à 60 T0	12 disques de 6 To, 4 disques internes de 6 To

Tableau 3. Configurations de la capacité de DL4300 Édition High Capacity

Capacité	Configuration matérielle
40 To, 50 To, 60 To, 70 To, 80 To, 90 To, 100 To, 110 To et 120 To	12 disques de 6 To, 4 disques internes de 6 To

REMARQUE : Un stockage supplémentaire peut être ajouté par le biais des étagères d'extension (Dell Storage MD1400). Un stockage supplémentaire peut être ajouté à n'importe quel modèle, toutefois, l'édition Standard Edition a une capacité maximale de 60 To et l'édition High Capacity Edition dispose d'une capacité maximale de 120 To. Les deux éditions supportent un maximum de quatre étagères d'extension.

Chaque configuration inclut également les matériels et logiciels suivants :

- Système Dell DL4300
- Contrôleurs RAID Dell PowerEdge (PERC)
- Un système d'exploitation préinstallé et le logiciel de gestion de stockage et du système Dell OpenManage
- logiciel AppAssure

REMARQUE : Si la configuration de votre appliance n'inclut pas les boîtiers de stockage Dell Storage MD1400, ignorez toute référence à Dell Storage MD1400 et aux boîtiers de stockage qui figure dans ce document.

Spécifications d'installation

Configuration réseau requise

Votre appliance nécessite l'environnement réseau suivant :

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

Infrastructure de réseau conseillée

Dell conseille aux organisations d'utiliser un segment principal de 1 GbE pour obtenir de meilleures performances avec AppAssure et des réseaux de 10 GbE pour des environnements extrêmement robustes.

Configuration du matériel.

L'appliance est livrée avec un seul système DL4300. Avant de configurer le matériel de l'appliance, voir le document *Mise en route de l'appliance Dell DL4300 avec votre système* livré avec l'appliance. Déballez et configurez le matériel de l'appliance DL.

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 serveur, procédez comme suit :

1. Mettez en rack et câblez le système DL4300 et les boîtiers de stockage.
2. Mettez sous tension les boîtiers de stockage puis le système DL4300.

Installation du serveur dans un rack

Si votre système comprend un kit de rails, localisez les *Instructions d'installation en rack* livrées avec le kit du rack. Suivez les instructions d'installation des rails dans l'unité de rack, le système et le boîtier de stockage du rack.

Réglage du commutateur de configuration du boîtier de stockage

Réglez le mode de stockage de chaque boîtier de stockage sur le mode unifié, tel que présenté dans les figures suivantes.

REMARQUE : Le commutateur de configuration doit être défini préalablement à la mise sous tension du boîtier de stockage. Si le mode de configuration est modifié, une fois le boîtier de stockage mis sous tension, les modifications ne seront prises en compte qu'au cycle d'alimentation suivant du système. Pour en savoir plus, voir *Dell Storage MD1400 Enclosures Hardware Owner's Manual (Manuel du propriétaire du matériel Dell Storage MD1400 Enclosures)* disponible à l'adresse **Dell.com/support/home**.

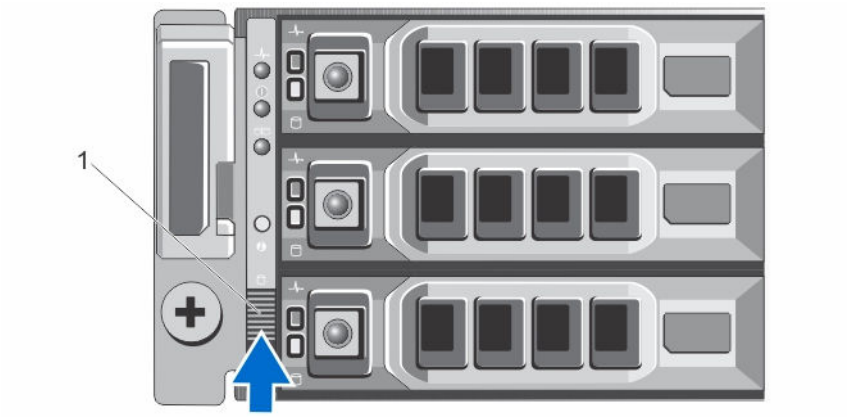


Figure 1. Réglage du commutateur de configuration d'un boîtier de stockage PowerVault MD1400

1. commutateur de configuration

Connexion des boîtiers de stockage au système

Connectez le câble de données du PERC (PowerEdge RAID Controller) installé sur le système Dell DL4300 au port SAS du module EMM (Enclosure Management Module) principal du boîtier de stockage.

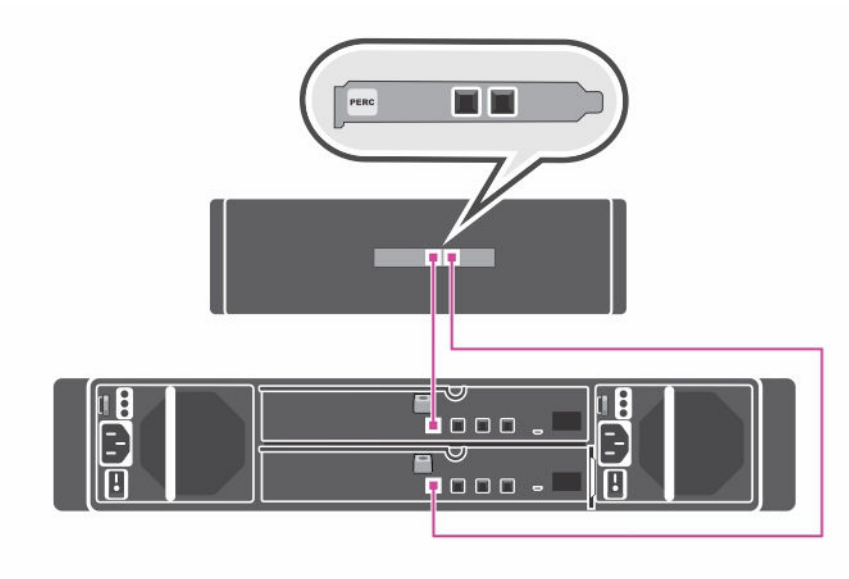


Figure 2. Connexion du système DL4300 au boîtier de stockage MD1400

Configuration à l'aide d'un port redondant

Pour une configuration à l'aide d'un port redondant :

1. Connectez l'extrémité de chaque câble SAS au port 0 et au port 1 du contrôleur PERC du système DL4300.
2. Connectez l'autre extrémité de chaque câble SAS au port 1 de chaque module EMM du boîtier de stockage MD1400.

Configuration à un seul port

Pour la configuration à un seul port :

1. Connectez une extrémité du câble SAS au port 0 du contrôleur PERC du système DL4300.
2. Connectez l'autre extrémité du câble SAS au port 1 sur le module EMM du boîtier de stockage MD1400.

Configuration multichaîne

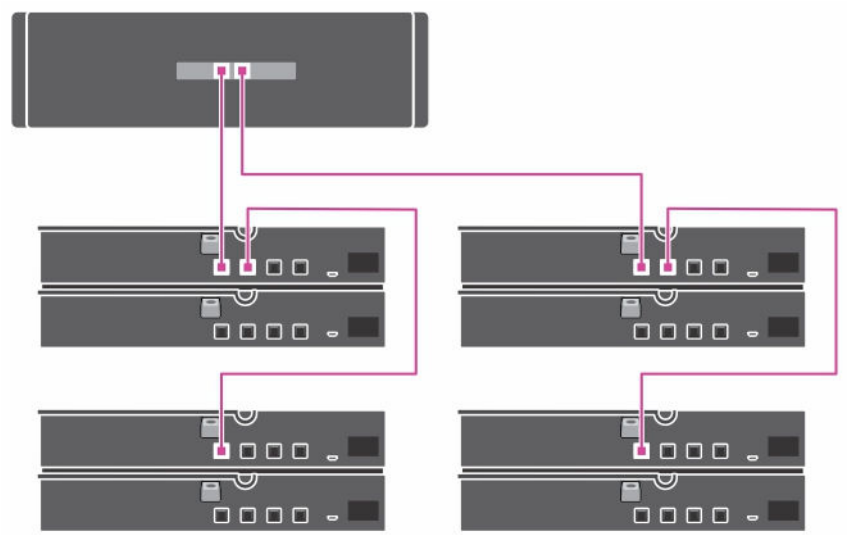


Figure 3. Configuration multichaîne

La configuration multichaîne prend en charge jusqu'à quatre boîtiers. Les deux premiers boîtiers sont connectés en série à l'un des boîtiers connectés à un seul port de la carte contrôleur. Les deux autres boîtiers sont connectés en série à l'un des boîtiers connectés au deuxième port de la carte contrôleur.

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.

Câblage de l'appliance

Localisez le document *Getting Started With Your System (Mise en route de votre système)* disponible sur **Dell.com/support/home**, livré avec votre appliance. Suivez-en les instructions pour connecter le clavier, la souris, le moniteur, les câbles d'alimentation et de réseau à votre appliance.

Mise sous tension de l'appliance

Après avoir branché l'appliance, mettez sous tension le boîtier de stockage MD1400, puis mettez sous tension le système DL4300.

REMARQUE : Il est recommandé de connecter l'appliance à un onduleur (UPS) pour assurer une fiabilité et une disponibilité maximales.

Configurations de disques de DL4300

DL4300 prend en charge des disques Nearline SAS et des disques SATA. Le système d'exploitation réside sur un disque virtuel RAID 1 (en miroir) situé dans les logements 12 et 13. Pour plus d'informations sur ces disques, voir le *Dell DL4300 Appliance Owner's Manual (Manuel du propriétaire de l'appliance Dell DL4300)* disponible à l'adresse **Dell.com/support/home**. Les lecteurs disponibles dans les emplacements 0 à 11 et 14 à 17 sont disponibles pour la configuration automatique grâce à l'Assistant Configuration de

l’appliance AppAssure (recommandé), mais peuvent également être configurés manuellement à l'aide de configurations personnalisées, le cas échéant. Les disques sont automatiquement affectés en tant que RAID 6. L’extension de la capacité à l’aide d’un boîtier de stockage MD1400 est facultative.

2

Configuration initiale du logiciel

Lorsque vous mettez sous tension l'appliance pour la première fois et que vous modifiez le mot de passe système, l'**Assistant Configuration de l'appliance AppAssure** s'exécute 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) Microsoft s'affiche sur la page **Paramètres**.
2. Pour accepter le CLUF, cliquez sur le bouton **J'accepte**.
   Une page permettant de modifier le mot de passe d'administration apparaît.
3. Cliquez sur **OK** en réponse au message vous invitant à modifier le mot de passe d'administrateur.
4. Saisissez et confirmez le nouveau mot de passe.
   Un message vous invite à confirmer la modification du mot de passe.
5. Cliquez sur **OK**.
6. À partir de l'écran **Dell readme.htm**, faites défiler la page et cliquez sur **Poursuivre/Continuer**.
7. Connectez-vous en utilisant le mot de passe d'administrateur modifié.
   L'écran **Sélectionnez la langue de appliance AppAssure** s'affiche.
8. Sélectionnez la langue de votre appliance à partir de la liste des langues prises en charge.
   L'écran d'accueil de l'**Assistant Configuration de l'appliance AppAssure** s'affiche.

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

REMARQUE : Ne fermez pas l'**Assistant Configuration de l'appliance AppAssure** tant que toutes les tâches n'ont pas été exécutées.

Assistant Configuration de l'appliance AppAssure

PRÉCAUTION : Assurez-vous de terminer 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. Ne pas effectuer de modifications via le panneau de configuration, utiliser Microsoft Windows Update, mettre à jour le logiciel AppAssure ou installer de licences tant que l'Assistant n'est pas terminé.

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

- Configuration de l'interface réseau
- Configuration des paramètres de nom d'hôte et de domaine
- Configuration des paramètres SNMP
- Création de disque(s) virtuel(s) Windows et RASR

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 équipe). 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 supplémentaires connectées 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 le regroupement de NIC, voir Regroupement de 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 comptez modifier le nom d'hôte, il vous est recommandé de le faire à ce stade. La modification du nom d'hôte suite à l'exécution de l'**Assistant Configuration de l'appliance** exige que vous effectuiez manuellement plusieurs étapes.

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

1. À la page **Configurer les paramètres de nom d'hôte et de domaine**, pour modifier le nom d'hôte de l'appliance, saisissez un nom d'hôte approprié dans le champ **Nouveau nom d'hôte**.
2. Si vous ne souhaitez pas que l'appliance rejoigne un domaine, sélectionnez **Non** dans **Souhaitez-vous que l'appliance rejoigne un domaine ?**

   Par défaut, **Oui** est sélectionné.
3. Pour joindre 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. Suite au redémarrage, l'**Assistant Configuration de l'appliance AppAssure** est lancé automatiquement. Si l'appliance est jointe à un domaine, 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. À la page **Configurer les paramètres SNMP**, sélectionnez **Configurer SNMP sur cette appliance** dans la page **Configurer les paramètres SNMP**.

   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 **Créer un/des disque(s) virtuel(s) Windows et RASR (s)** apparaît.

Création de disque(s) virtuel(s) Windows et RASR

Le système DL4300 prend en charge :

- deux lecteurs de système d'exploitation, douze disques de données et quatre disques durs internes
- possibilité de créer des numéros d'unité logique (LUN) pour le stockage des informations de restauration sur matériel sans système d'exploitation (BMR)
- possibilité de créer un espace distinct pour la sauvegarde Windows du fichier RASR.

Pour créer un/des disque(s) virtuel(s) optionnel(s) :

1. Sélectionnez les disques virtuels suivants :
   a. disque virtuel de sauvegarde Windows

      PRÉCAUTION : Si vous avez ignoré cette option dans l' AppAssure Appliance Configuration Wizard (Assistant Configuration de l'appliance AppAssure), vous ne serez pas en mesure de créer une sauvegarde Windows Server et de configurer une stratégie de sauvegarde.

      Le disque virtuel de sauvegarde Windows fournit l'espace cible nécessaire à la création des sauvegardes Windows Server. Un espace disque de 75 Go est attribué par défaut pour la sauvegarde Windows DV créée et vous ne pouvez pas augmenter la taille de la sauvegarde Windows DV. Avec le temps, la quantité de données sauvegardées peut dépasser 75 Go et si tel est le cas, vous ne serez pas en mesure d'effectuer la sauvegarde ou la configuration de la stratégie de sauvegarde sur la page de **Sauvegarde** : un message d'erreur signalant le manque de capacité s'affiche. Dans ce cas, la sauvegarde Windows peut être reconfigurée dans un partage réseau ou sur un autre volume de disque sur l'appliance DI. Pour en savoir plus, voir la section Configurer une Stratégie de sauvegarde de lecteur réseau partagé planifiée dans la section *Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)* (Récupération d'un Dell™ DL Appliance de sauvegarde et de récupération à l'aide de RASR (Rapid Appliance Self Recovery/Récupération automatique rapide de l'appliance)) disponible sur **Dell.com/supportmanuals**.
   b. disque virtuel RASR amorçable

      Le disque virtuel RASR amorçable fournit un volume de récupération redondant permettant d'exécuter une récupération RASR. Vous pouvez redémarrer le volume de récupération redondant en appuyant sur la touche <F8> pendant l'autotest de démarrage. Après le redémarrage, suivez les étapes décrites dans la section Exécution de RASR à l'aide de la clé USB RASR.
2. Cliquez sur **Suivant**.

   Un écran de remerciement s'affiche pendant que le système est en cours de configuration. Un message confirmant que la configuration est terminée apparaît.
3. Cliquez sur **Quitter**.

   La console Core est lancée automatiquement.
4. Poursuivez le processus de configuration avec Provisionnement du stockage.

Utilitaire de récupération et de mise à jour

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

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

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

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

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

REMARQUE : Si vous utilisez le RUU nº 184 et que votre appliance DL possède une version de Core AppAssure inférieure (antérieure) à 5.4.3.106, le core est mis à niveau vers AppAssure Core 5.4.3.106 .

REMARQUE : Si vous effectuez une mise à niveau vers RUU nº 184, vous risquez de commencer à voir apparaître des incohérences lors de l'exécution future de sauvegardes Windows déjà planifiées (via RASR), ou il vous sera peut-être impossible de créer une stratégie de sauvegarde Windows. Ces erreurs se produisent en raison du manque d'espace à l'emplacement du stockage de vos sauvegardes Windows.

Autres causes potentielles de ces échecs :

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

Restauration automatique rapide de l'appliance

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

- Restaurer les paramètres définis en usine
- Restaurer l'état de l'appliance, tel qu'il existait avant l'incident

Création de la clé USB RASR

Pour créer une clé USB RASR :

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

   REMARQUE : Insérez une clé USB 16 Go ou plus, avant de tenter de créer la clé RASR.
3. Après avoir inséré une clé USB de 16 Go ou plus, cliquez sur **Créer un lecteur USB RASR maintenant**.
   Un message de **vérification de conditions** s'affiche.

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

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

   Une boîte de dialogue de confirmation s'affiche.

5. Cliquez sur **Oui**.

   La clé de lecteur USB RASR est créée.

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

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

Exécution du RASR

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

Les étapes suivantes vous aident à effectuer la réinitialisation usine.

Pour restaurer l'état de l'appliance, qui existait avant l'incident et récupérer les référentiels, les points de récupération et les paramètres, reportez-vous à rubrique au document *Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)* (Restauration d'une sauvegarde Dell™ DL et restauration RASR) disponible sur **Dell.com/support/home**

.

Pour effectuer la restauration RASR :

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

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

8. Cliquez sur **Suivant**.

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

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

9. Cliquez sur **Suivant**.

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

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

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

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

11. Cliquez sur **Suivant**.

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

12. Cliquez sur **Oui**.
    Le disque du système d'exploitation commence la restauration du système d'exploitation d'origine.
13. A la fin de la réinitialisation usine, dans l'écran **RASR terminée**, cliquez sur **Terminer**.

Utilisation de la fenêtre RASR à l'aide du double module SD interne

Votre système est livré avec un double module SD interne et une carte SD de 16 Go de capacité.

Pour exécuter le RASR à l'aide du double module SD interne (IDSDM) :

1. Redémarrez l'appliance via le module IDSDM.

   PRÉCAUTION : Assurez-vous que la carte SD est insérée dans le logement 1.

   Le message suivant s'affiche :

   ```
   The secondary SD card is missing, not responding, or in write-protected mode. Do one of the following: 1) Install a SD card media in the secondary SD card reader. 2) Reseat or replace the SD card media.3) If write-protected mode is expected, then no respose action is required.
   ```

   Ignorez le message ci-dessus.
2. Pour poursuivre l'exécution du RASR à l'aide du module SD interne, effectuez les étapes 5 à 13 de la section Exécution de RASR à l'aide de la clé USB RASR.

Provisionnement du stockage

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

- Référentiels AppAssure

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

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

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

Avant de commencer à provisionner le stockage sur le disque, déterminez la quantité de stockage que vous souhaitez allouer aux machines virtuelles de secours. Vous pouvez allouer n'importe quel pourcentage de la capacité disponible restant après la création du référentiel AppAssure aux machines virtuelles hôte de secours. Par exemple, si vous utilisez Storage Resource Management (SRM), vous pouvez allouer jusqu'à 100 % de la capacité de stockage restante après la création du référentiel AppAssure. L'espace peut être alloué aux VM de secours uniquement sur les appliances provisionnées sur des machines virtuelles hôtes. À l'aide de la fonction Live Recovery d'AppAssure, vous pouvez utiliser ces machines virtuelles pour remplacer rapidement un serveur protégé par l'appliance qui serait défaillant.

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

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

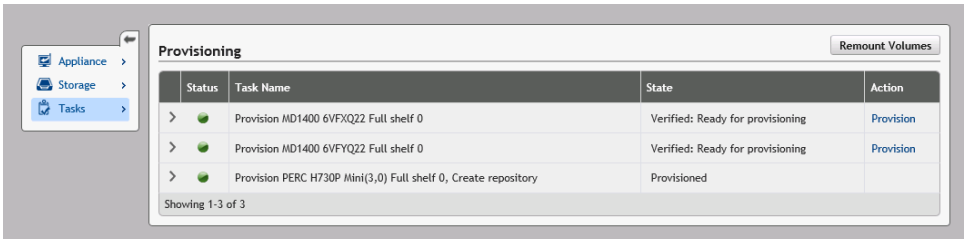
Pour effectuer le provisionnement de disque pour tout le stockage disponible :

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

   PRÉCAUTION : Avant de continuer, s'assurer que les étapes 2 à 4 sont suivies dans cette procédure.

2. REMARQUE : Provisionnement du contrôleur RAID interne pour créer le référentiel initial sur votre appliance.

   Ouvrez la fenêtre **Storage (Stockage) de provisionnement** en cliquant sur **Provision** (Fournir des infos de paramétrage) dans la colonne Action, en regard du stockage auquel vous souhaitez fournir les infos de paramétrage.
3. Dans la section **Réserve de stockage facultative** , cochez la case en regard d'**Allouer une portion du stockage aux machines virtuelles en mode Veille en cours de provisionnement ou à d'autres fins** et indiquez un pourcentage de stockage à allouer. Dans le cas contraire, le pourcentage de stockage indiqué dans la section **Réserve de stockage en option** sera pris sur tous les disques connectés.
4. Cliquez sur **Provisionner**.



   Les disques virtuels permettant d'héberger les référentiels et les machines virtuelles de secours sont créés.

Provisionnement du stockage sélectionné

Pour provisionner le stockage sélectionné :

1. Dans l'onglet **Appliance**, cliquez sur **Tâches**.
   L'écran **Tâches** affiche la capacité de stockage interne et de stockage externe disponible pour l'appliance, indique si elle est disponible pour le provisionnement ou déjà provisionnée, et précise s'il existe une condition interdisant le provisionnement automatique du stockage. Cette capacité est utilisée pour créer un référentiel AppAssure.
2. REMARQUE : Il est recommandé de provisionner le stockage interne disponible avant de procéder à une extension au boîtier externe (MD1400).

Pour provisionner uniquement une portion de l'espace disponible, cliquez sur **Provisionner** sous **Action**, en regard de l'espace de stockage à provisionner.

- Pour créer un nouveau référentiel, sélectionnez **Créer un nouveau référentiel**, puis entrez un nom pour ce référentiel.

  Par défaut, le champ de nom du référentiel contient « Référentiel 1 ». Vous pouvez choisir d'écraser ce nom.
- Pour ajouter de la capacité à un référentiel existant, sélectionnez **Étendre le référentiel existant**, puis sélectionnez l'entrée voulue dans la liste **Référentiels existants**.

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

3. Sous **Réserve de stockage facultative**, vous pouvez sélectionner l'option qui permet d'allouer une portion du stockage aux machines virtuelles de secours, puis spécifier le pourcentage de stockage à allouer à ces VM.
4. Vous pouvez choisir de désélectionner la case à cocher **Faire ceci pour une seule tâche de provisionnement si plusieurs tâches sont provisionnées simultanément** (cochée par défaut).

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

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

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

Configuration de DL4300 à l'aide du stockage Fibre Channel (en option)

L'Édition haute capacité DL4300 offre une option de stockage HBA Fibre Channel permettant de créer des référentiels à l'aide de matrices de stockage Fibre Channel.

REMARQUE : Si la configuration Fibre Channel est commandée, elle remplace l'adaptateur SAS PERC H830 à encoches.

REMARQUE : Pour plus d'informations sur les spécifications, les hypothèses et pour des informations détaillées sur les étapes suivantes, reportez-vous au livre blanc *DL4xxx : Implémentation Fibre Channel* , disponible sur **dell.com/support/home** .

Pour intégrer et configurer DL4300 à l'aide du stockage Fibre Channel :

1. connectez le HBA Fibre Channel du DL4300 à un commutateur SAN.
2. installez Qlogic ou le logiciel de gestion HBA Emulex sur tout adaptateur commandé avec le système.
3. installez le logiciel à trajet multiples de la matrice de stockage.
4. effectuez le zonage Fibre Channel.
5. créez un LUN (numéro d'unité logique) Fibre Channel qui sera affecté et utilisé comme référentiel pour DL4300.

6. montez le LUN de stockage Fibre Channel.
7. configurez le stockage Fibre Channel DL4300 comme référentiel de sauvegarde.

3

Tâches à effectuer après l'installation

Après avoir exécuté l'**Assistant Configuration de l'appliance AppAssure**, procédez comme suit pour vérifier que votre appliance de sauvegarde et les serveurs que l'appliance sauvegarde sont bien configurés.

REMARQUE : L'appliance est configurée avec une licence logicielle AppAssure temporaire de 30 jours. Pour obtenir une clé de licence permanente, connectez-vous au portail de licences Dell AppAssure à l'adresse **www.dell.com/DLActivation**. Pour en savoir plus sur la modification d'une clé de licence dans le logiciel AppAssure, voir la rubrique « Modifier une clé de licence » dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance Dell DL4000) à l'adresse **dell.com/support/home**.

Accès à la console Core

Veillez à mettre à jour les sites de confiance comme vous l'indique la rubriqueMise à jour des sites de confiance dans Internet Explorer, et à configurer vos navigateurs comme l'indique la rubrique Configuration de navigateurs pour accéder à distance à la console Core. Une fois que vous avez mis à jour les sites de confiance dans Internet Explorer et configuré vos navigateurs, effectuez l'une des opérations suivantes pour accéder à la console Core :

- connectez-vous localement au serveur AppAssure Core, puis double-cliquez sur l'icône **Core Console**.
- Ou, entrez l'une des URL suivantes dans votre navigateur Web :
  - **https://<NomDeVotreServeurCore>:8006/apprecovery/admin/core ou**
  - **https://<AdresseIPDeVotreServeurCore>:8006/apprecovery/admin/core**

Mise à jour des sites de confiance dans Internet Explorer

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

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

Configuration des navigateurs pour accéder à distance à Core Console

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

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

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

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

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

Modification des paramètres de navigateur dans Internet Explorer et Chrome

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

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

Configuration des paramètres du navigateur Mozilla Firefox

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

Pour modifier les paramètres du navigateur Mozilla Firefox :

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

La recherche doit renvoyer au moins trois résultats.

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

Examen des périodes de rétention

AppAssure définit les périodes de rétention par défaut qui déterminent la fréquence à laquelle des instantanés sont pris et la durée de rétention de ceux-ci. Les périodes de rétention doivent être basées sur les besoins de votre environnement. Par exemple, si vous sauvegardez des serveurs qui exécutent des données critiques à la mission, qui changent fréquemment et qui sont essentiels à la continuité des opérations, des instantanés doivent être pris plus fréquemment.

Pour examiner et modifier les périodes de rétention :

1. ouvrez la console AppAssure Core.
2. sélectionnez l'onglet **Configuration**, puis cliquez sur **Stratégie de rétention**.
3. réglez la stratégie de rétention en fonction des besoins de votre organisation.
4. cliquez sur **Appliquer**.

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, il vous 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 de l'AppAssure Core, cliquez sur **Configuration** → **Gérer** → **Sécurité**.
2. Cliquez sur **Actions**, puis sélectionnez **Ajouter une clé de chiffrement**.
   La page **Créer une clé de cryptage** s'affiche.
3. Saisissez les informations suivantes :

Champ	Description
Nom	Entrez un nom pour la clé de chiffrement.
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 conseillé d'enregistrer la phrase de passe de cryptage car si vous la perdez le données seront inaccessibles.

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

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

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

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

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

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

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

Zone de texte	Description
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 d'émissions

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

Pour modifier le nombre d'émissions simultanées :

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

Protection des ordinateurs et vérification de la connectivité aux clients

Après avoir configuré l'appliance DL et le Core, vérifiez que vous pouvez vous connecter aux ordinateurs que vous comptez sauvegarder.

Pour protéger un ordinateur

1. Naviguez jusqu'à la console Core, puis sélectionnez l'onglet **Machines**.
2. Dans le menu déroulant **Actions,** cliquez sur **Protéger l'ordinateur**.

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

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

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

Vérification de la connectivité du réseau

Pour vérifier la connectivité réseau :

1. Ouvrez une interface de ligne de commande sur le système client auquel vous tentez de vous connecter.
2. Exécutez la commande ipconfig et notez l'adresse IP du client.
3. Ouvrez une interface de ligne de commande sur l'appliance.
4. Exécutez la commande ping <IP address of 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 AppAssure 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 du pare-feu de l'AppAssure Core et de tout client sauvegardé par celui-ci :

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

Vérification de résolution de nom (le cas échéant)

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 AppAssure, allez aux hôtes C:\Windows\system32\drivers\etc.
2. Saisissez l'adresse IP de chaque client sauvegardé sur DL4300.

Association de cartes réseau

Par défaut, les cartes réseau (NIC) de l'appliance DL4300 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
- La création de l'association NIC

- la configuration d'un commutateur virtuel Hyper-V

Réinstallation de Broadcom Advanced Configuration Suite

Pour réinstaller Broadcom Advanced Configuration Suite (BACS) :

1. Identifiez les cartes réseau (NIC) sur votre système. Pour identifier les cartes réseau :
   a. Accédez à Dell Open Manage Server Administrator (OMSA).
   b. Sur la page principale, cliquez sur **Système → Châssis du système principal → Logements**.
2. Désinstallez les versions précédentes de pilotes Broadcom et d'applications de gestion.
3. Téléchargez les pilotes Broadcom et BACS appropriés sur votre appliance.

   Les pilotes suivants sont disponibles à l'adresse **dell.com/support**.

   - Pilote QLogic

     Cliquez sur **Serveurs, stockage et mise en réseau → Logiciel Dell DL 4300 → Pilotes et téléchargements → Catégorie → Réseau → QLogic BCM57xx et BCM57xxx** .
   - Pilote Broadcom

     Cliquez sur **Serveurs, stockage et mise en réseau → Logiciel Dell DL 4300 → Pilotes et téléchargements → Catégorie → Réseau → Mise à jour de pilote Broadcom Windows 64 bits pour les adaptateurs NetXtreme Ethernet**.
4. Terminez l'installation en passant par l'Assistant Installation.

Création de l'association NIC

REMARQUE : Il est recommandé de ne pas utiliser l'interface native d'association 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 DL4300 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 construction de l'association peut prendre environ 5 minutes.

Configuration d'un commutateur virtuel Hyper-V

Pour que les machines virtuelles de secours communiquent au sein d'un environnement de production, créez un commutateur virtuel. Pour créer un commutateur virtuel externe, voir la section *Configurer des réseaux virtuels* à l'adresse **www.technet.microsoft.com**.

4

Installation des agents sur les clients

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

Vous pouvez également déployer le logiciel agent sur l'ordinateur agent au cours du processus de protection d'un ordinateur. Cette option est disponible pour les ordinateurs sur lesquels le logiciel Agent n'a pas encore été installé. Pour en savoir plus sur le déploiement du logiciel Agent tout en protégeant un ordinateur, voir le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance Dell DL4300) à l'adresse **dell.com/support/home**.

Installation à distance des agents (pousser)

Pour installer des agents à distance (pousser) :

1. Si le client utilise une version de système d'exploitation antérieure à Windows Server 2012, vérifiez que l'infrastructure Microsoft .NET4 est installée sur le client :
   a. Sur l'appliance, démarrez le **Windows Server Manager** (Gestionnaire de serveurs Windows).
   b. Cliquez sur **Configuration** → **Services.**
   c. Vérifiez que l'infrastructure Microsoft .NET s'affiche dans la liste de services.

      Si elle n'est pas installée, vous pouvez en installer une copie depuis **microsoft.com**.
2. Vérifiez ou modifiez le chemin d'accès aux progiciels d'installation de l'agent :
   a. Dans la console AppAssure Core, cliquez sur l'onglet **Configuration**, puis cliquez sur **Paramètres** dans le panneau de gauche.
   b. Dans la zone **Paramètres de déploiement**, cliquez sur **Modifier**.
   c. Saisissez les informations suivantes sur l'emplacement de l'agent :

Champ	Description
Nom du programme d'installation de l'agent	Spécifie le chemin exact au **folder\file** de l'agent.
Adresse du Core	Spécifie l'adresse IP de l'appliance exécutant l'AppAssure Core. REMARQUE : Par défaut, le champ **Adresse de Core** est vide. Le champ **Adresse de Core** n'exige aucune adresse IP car les fichiers d'installation sont installés sur l'appliance.

   d. Cliquez sur **OK**.

3. Cliquez sur l'onglet **Outils**, puis cliquez sur **Déploiement en masse** dans le volet de gauche.

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

   Suite au déploiement de l'agent, une sauvegarde du client démarre automatiquement.

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

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

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

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

1. Dans la boîte de dialogue **Protéger un ordinateur** → **Connecter**, après avoir entré les paramètres de connexion appropriés, cliquez sur **Connecter**.

   La boîte de dialogue **Déployer l'agent** s'affiche.
2. Cliquez sur **Oui** pour déployer à distance le logiciel d'agent sur l'ordinateur.

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

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

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

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

4. Cliquez sur **Déployer**.

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

Installation des agents Microsoft Windows sur le client

Pour installer les agents :

1. Vérifiez que l'infrastructure Microsoft .NET4 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 auprès de **microsoft.com**.
2. Installez l'agent :
   a. Sur l'appliance AppAssure, partagez le répertoire C:\install\AppAssure avec le(s) client(s) que vous comptez sauvegarder.
   b. Sur le système client, adressez un lecteur à C:\install\AppAssure sur l'appliance AppAssure.
   c. Sur le système client, ouvrez le répertoire C:\install\AppAssure et double-cliquez sur l'agent correct du système client pour démarrer l'installation.

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

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

Pour ajouter un agent :

1. Dans l'écran d'**Accueil du portail de licences d'AppAssure** , sélectionnez un groupe, puis cliquez sur **Télécharger un agent**.

   La boîte de dialogue **Télécharger un agent** s'affiche.
2. Cliquez sur **Télécharger**, en regard de la version du programme d'installation à télécharger.

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

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

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

Le fichier **Agent** se télécharge.

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

REMARQUE : Pour en savoir plus sur l'ajout d'agents à l'aide de l'ordinateur Core, voir la section « Déploiement d'un agent (Installation en mode Push) » dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance Dell DL4000) à l'adresse **dell.com/support/home**.

Installation d'agents sur des ordinateurs Linux

Téléchargez le programme d'installation 32 bits ou 64 bits sur chaque serveur Linux que vous souhaitez protéger à l'aide de l'AppAssure Core. Vous pouvez télécharger les programmes d'installation depuis le Portail de licences AppAssure à l'adresse **https://licenseportal.com**. Pour en savoir plus, voir Ajout d'un agent à l'aide du portail de licences.

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

- sudo
- admin
- appassure
- wheel

Pour en savoir plus sur la protection d'un ordinateur, voir la section « Protection d'un ordinateur » dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance DL4000) à l'adresse **dell.com/support/home**.

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

- Installation de l'agent sur Ubuntu
- Installation de l'agent sur Red Hat Enterprise Linux et CentOS
- Installation de l'agent sur SUSE Linux Enterprise Server

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

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

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

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

Emplacement des fichiers de l'agent Linux

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

Composant	Emplacement/Chemin
mono	/opt/appassure/mono
agent	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk et aavdctl	/usr/bin
fichiers de configuration de aavdisk	/etc/appassure/aavdisk.conf
wrappers pour aamount et agent	• /usr/bin/aamount • /usr/bin/aagent
scripts d'exécution automatique pour aavdisk et agent	• /etc/init.d/appassure-agent • /etc/init.d/appassure-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 Ubuntu	Dépendance
L'appassure-vss exige	`dkms, gcc, make, linux-headers-‘uname-r‘`
L'appassure-aavdisk exige	`libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3`
L'appassure-mono exige	`libc6 (>=2.7-18)`

Pour Red Hat Enterprise Linux et CentOS	Dépendance
Le nbd-dkms exige	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
L'appassure-vss exige	`dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘`
L'appassure-aavdisk exige	`nbd-dkms, libblkid, pam, pcre`

Pour Red Hat Enterprise Linux et CentOS	Dépendance
L'appassure-mono exige	`glibc >=2.11`

Pour SUSE Linux Enterprise Server	Dépendance
Le nbd-dkms exige	`dkms, gcc, make, kernel-syms`
L'appassure-vss exige	`dkms, kernel-syms, gcc, make`
L'appassure-aavdisk exige	`libblkid1, pam, pcre`
L'appassure-mono exige	`glibc >=2.11`

Installation de l'agent sur Ubuntu

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

Pour installer l'agent AppAssure sur Ubuntu :

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent AppAssure, saisissez la commande suivante :

   `chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

   Le fichier devient exécutable.

   REMARQUE : Pour les environnements 32 bits, le programme d'installation est nommé **appassureinstaller_ ubuntu_i386_5.x.x.xxxxx.sh**
3. Pour extraire et installer l'agent AppAssure, saisissez la commande suivante :

   `/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` et appuyez sur <Entrée>.

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

   REMARQUE : Pour en savoir plus sur les fichiers requis par l'agent, voir Dépendances de l'agent.

Une fois le programme d'installation terminé, l'agent s'exécute sur votre ordinateur. Pour savoir comment protéger cet ordinateur à l'aide du Core, voir la section Protection des stations de travail et serveurs dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance DL4000) à l'adresse **dell.com/support/home**.

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

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

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

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent AppAssure, 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 AppAssure, 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.

L'agent s'exécute sur votre ordinateur après l'exécution du programme d'installation. Pour savoir comment protéger cet ordinateur à l'aide du Core, voir la section Protection des stations de travail et des serveurs dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance Dell DL4000) à l'adresse **dell.com/support/home**.

Installation de l'agent sur SUSE Linux Enterprise Server

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

Pour installer l'agent sur SLES :

1. Ouvrez une session de terminal avec accès root.
2. Pour rendre exécutable le programme d'installation de l'agent AppAssure, saisissez la commande suivante :

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

   REMARQUE : Pour les environnements 32 bits, le programme d'installation est nommé `appassureinstaller__ sles_i386_5.x.x.xxxxx.sh`

   Le fichier devient exécutable.
3. Pour extraire et installer l'agent AppAssure, saisissez la commande suivante :

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

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

   Pour en savoir plus sur les fichiers requis par l'agent, voir Dépendances de l'agent.

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

Une fois le programme d'installation terminé, l'agent s'exécute sur votre ordinateur. Pour savoir comment protéger cet ordinateur à l'aide du Core, voir la section « Protection des stations de travail et serveurs » dans le *Dell DL4300 Appliance User's Guide* (Guide d'utilisation de l'appliance DL4000) à l'adresse **dell.com/support/home**.

5

Obtention d'aide

Recherche de documentation et de mises à jour logicielles

Dans la console AppAssure Core, il existe des liens directs vers AppAssure, la documentation de l'appliance et les mises à jour logicielles. Pour accéder aux liens, cliquez sur l'onglet **Appliance**, puis cliquez sur **État global**. Les liens vers les mises à jour et la documentation se trouvent dans la section **Documentation**.

Recherche de mises à jour du logiciel

Il existe des liens directs vers les mises à jour du logiciel de l'appliance AppAssure et DL4300 disponible dans la console AppAssure 5 Core. Pour accéder aux liens vers les mises à jour du logiciel, sélectionnez l'onglet **Appliance**, puis cliquez sur **État global**. Les liens vers les mises à jour se trouvent dans la section **Documentation**.

Contacter Dell

REMARQUE : 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.