

Acronis



Acronis Backup Advanced for vCloud

Update 3

GUIDE DE L'ADMINISTRATEUR

Table des matières

1	Guide de l'administrateur.....	4
1.1	À propos de ce document	4
1.2	Présentation d'Acronis Backup Advanced for vCloud.....	4
1.2.1	Nouveautés de la mise à jour Update 3	4
1.2.2	Nouveautés de la mise à jour Update 1	5
1.2.3	Exigences logicielles.....	5
1.2.4	Architecture d'Acronis Backup Advanced for vCloud.....	6
1.2.5	Planification des ressources matérielles.....	8
1.3	Installation d'Acronis Backup Advanced for vCloud	11
1.3.1	Préparation.....	11
1.3.2	Installation et configuration de RabbitMQ Server.....	12
1.3.3	Installation d'Acronis Backup Management Server.....	14
1.3.4	Utilisation de la console d'administration	18
1.3.5	Intégration du serveur de gestion à vCenter Server.....	19
1.3.6	Déploiement de l'agent pour VMware.....	19
1.3.7	Installation de l'agent Acronis Backup pour vCloud	21
1.3.8	Configuration de l'agent pour vCloud d'Acronis Backup	21
1.3.9	Vérification des connexions réseau.....	25
1.3.10	Mise à jour avec une nouvelle version	26
1.3.11	Désinstallation	27
1.4	Connexion au service de sauvegarde.....	28
1.5	Administration d'organisations	28
1.5.1	Surveillance des organisations.....	28
1.5.2	Activation de sauvegarde pour une organisation.....	29
1.5.3	Utilisation dans une organisation.....	32
1.5.4	Autoriser les non-administrateurs à utiliser le service	32
1.5.5	Désactivation de sauvegarde pour une organisation.....	33
1.6	Configuration du service de sauvegarde.....	33
1.6.1	Gestion des plans de sauvegarde système.....	35
1.7	Génération de rapports d'utilisation	37
1.8	Affichage des journaux d'audit	38
1.9	Collecte de journaux	39
1.10	Scénarios avancés.....	39
1.10.1	Reprise d'activité après sinistre de machines physiques vers vCloud	39
1.10.2	Configuration de la déduplication	40
1.10.3	Modification du stockage de sauvegarde.....	40
1.10.4	Intégration avec les systèmes tiers.....	42
1.11	Sécurité et personnalisation	42
1.11.1	Modification du certificat SSL.....	42
1.11.2	Modification du logo et personnalisation de l'interface.....	43
2	Guide de l'utilisateur	45
2.1	À propos du service de sauvegarde	45
2.2	Navigateurs Web pris en charge	45
2.3	Installation de VMware Tools.....	45
2.4	Opérations de base.....	46
2.4.1	Connexion au service.....	46

2.4.2	Sauvegarde des machines virtuelles.....	46
2.4.3	Application d'un plan de sauvegarde	47
2.4.4	Écrasement d'une machine virtuelle avec sa version sauvegardée	49
2.4.5	Restauration d'une machine virtuelle	50
2.4.6	Restauration de fichiers à partir d'une sauvegarde de machine virtuelle.....	52
2.4.7	Surveillance des états de protection	53
2.5	Opérations avec des sauvegardes	54
2.6	Opérations avec les plans de sauvegarde	55
2.6.1	Création d'un plan de sauvegarde.....	55
2.6.2	Suppression d'un plan de sauvegarde.....	60
2.6.3	Modification d'un plan de sauvegarde.....	59
2.6.4	Retrait d'un plan de sauvegarde.....	59
2.7	Génération de rapports d'utilisation	60
2.8	Autoriser les non-administrateurs à utiliser le service	61
2.8.1	Attribution d'un rôle vCloud Director à un utilisateur.....	61
2.9	Affichage des journaux d'audit.....	62
3	Références terminologiques.....	63

1 Guide de l'administrateur

1.1 À propos de ce document

Ce document est destiné aux administrateurs système de VMware vCloud Director souhaitant fournir un service de sauvegarde aux organisations vCloud à l'aide d'Acronis Backup Advanced for vCloud.

Le document vous explique comment :

- Installer Acronis Backup Advanced for vCloud
- Le configurer pour qu'il fonctionne avec vCloud Director
- Activer le service de sauvegarde pour les organisations
- Administrer le service de sauvegarde (surveiller le statut du service, configurer les options de sauvegarde et de récupération, générer des rapports d'utilisation, entre autres)

Pour plus d'informations sur la sauvegarde et la restauration de machines virtuelles et sur l'administration d'une organisation, veuillez vous référer au Guide de l'utilisateur (p. 45) d'Acronis Backup Advanced for vCloud.

Acronis Backup Advanced for vCloud appartient à la suite de produits Acronis Backup Advanced. L'aide sur le Web d'Acronis Backup fournit des informations supplémentaires sur cette famille de produits : http://www.acronis.fr/support/documentation/AcronisBackup_11.5/

1.2 Présentation d'Acronis Backup Advanced for vCloud

Acronis Backup Advanced for vCloud est une solution de sauvegarde et de restauration des machines virtuelles gérées par VMware vCloud Director.

Acronis Backup Advanced for vCloud propose le service de sauvegarde aux niveaux administrateur système et utilisateur de l'organisation. Le service de sauvegarde est disponible par le biais d'une interface Web. Les utilisateurs se connectent au service à l'aide de leurs accréditations vCloud Director. Les informations que les utilisateurs voient et les opérations qu'ils peuvent effectuer dépendent des droits utilisateur dans vCloud Director.

Afin de déployer le service de sauvegarde dans votre infrastructure vCloud Director, vous devez installer les composants d'Acronis Backup Advanced for vCloud et les intégrer aux composants vCloud Director.

Veuillez vous référer aux rubriques de cette section avant de commencer l'installation.

1.2.1 Nouveautés de la mise à jour Update 3

La version mise à jour du produit comprend les nouvelles fonctionnalités suivantes :

- **Sauvegarde pour les utilisateurs non-administrateurs** (p. 32)
Les administrateurs peuvent autoriser les utilisateurs non-administrateurs à employer le service.
- **Journaux d'audit** (p. 38)
Les administrateurs système et de l'organisation peuvent voir le journal dont la portée se trouve dans leur zone de contrôle.
- **Planification de sauvegardes par heure** (p. 55)

Lorsque vous créez un plan de sauvegarde, vous pouvez exécuter des sauvegardes toutes les heures.

- **Quota pour les données sauvegardées** (p. 33)
Les administrateurs système peuvent choisir de définir les quotas pour l'utilisation du stockage ou pour la quantité de données sauvegardées.
- **Nouvelle colonne « Excédent de quota » dans les rapports** (p. 37)
Les administrateurs système et d'organisation peuvent voir de combien une organisation a dépassé son quota.

Pour plus d'informations sur les étapes de mise à jour du produit, veuillez vous référer à « Mise à jour avec une nouvelle version » (p. 26).

1.2.2 Nouveautés de la mise à jour Update 1

Le produit Acronis Backup & Recovery pour vCloud a été renommé **Acronis Backup Advanced for vCloud**. Acronis Backup & Recovery 11.5 a été renommé Acronis Backup.

La version mise à jour du produit comprend les nouvelles fonctionnalités suivantes :

- **Récupération de fichiers.** Vous pouvez autoriser les utilisateurs à restaurer des fichiers et dossiers individuels (p. 52) à partir de sauvegardes de machines virtuelles.
- **Application d'un plan de sauvegarde à une vApp.** Vous pouvez appliquer un plan de sauvegarde (p. 47) à une vApp entière plutôt qu'à des machines virtuelles spécifiques. Le plan de sauvegarde s'applique automatiquement à toutes les machines virtuelles actuellement dans la vApp et à toutes celles qui y apparaîtront ultérieurement.
- **Configuration d'un plan de sauvegarde par défaut pour une organisation.** Lorsque vous activez la sauvegarde pour une organisation (p. 29), vous pouvez sélectionner un plan de sauvegarde système qui s'appliquera à toutes les vApps actuelles et futures au sein de l'organisation.
- **Ajout d'adaptateurs réseau lors de la restauration.** Avant de restaurer une machine virtuelle (p. 50), vous pouvez ajouter ou supprimer des adaptateurs réseau pour la machine et préciser les paramètres de ces adaptateurs.
- **Recréation de la vApp d'origine lors de la restauration.** Lors de la restauration d'une machine virtuelle (p. 50), vous pouvez recréer automatiquement la vApp d'origine de la machine si celle-ci n'est plus présente dans l'organisation.
- **Sécurité améliorée.** L'agent pour vCloud utilise une base de données mieux sécurisée, protégée par un mot de passe, pour stocker les métadonnées relatives aux machines virtuelles sauvegardées. Un mot de passe fort est automatiquement sélectionné lors de la mise à niveau. Vous pouvez également modifier le mot de passe dans les paramètres de l'agent pour vCloud (p. 21). L'ensemble du contenu de l'ancienne base de données est transféré vers la nouvelle.

Pour plus d'informations sur les étapes de mise à jour du produit, consultez la section « Mise à jour avec une nouvelle version » (p. 26).

1.2.3 Exigences logicielles

Versions de VMware vCloud Director prises en charge

- VMware vCloud Director 1.5
- VMware vCloud Director 5.0
- VMware vCloud Director 5.1
- VMware vCloud Director 5.5

Systèmes d'exploitation invités compatibles

Acronis Backup Advanced for vCloud prend en charge un grand nombre de systèmes d'exploitation invités, dont Windows 8, Windows Server 2012 et toutes les distributions Linux courantes.

Navigateurs Web pris en charge

- Google Chrome 12 ou plus récent
- Mozilla Firefox 12 ou plus récent
- Windows Internet Explorer 9 ou plus récent
- Safari 5 ou plus récent s'exécutant sur les systèmes d'exploitation Mac OS X et iOS

Les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) peuvent ne pas afficher correctement l'interface utilisateur ou ne pas proposer l'ensemble des fonctions disponibles.

JavaScript doit être activé dans le navigateur.

Pour afficher l'interface graphique, la résolution de l'écran doit être au minimum de 1 024x768.

1.2.4 Architecture d'Acronis Backup Advanced for vCloud

Acronis Backup Advanced for vCloud est constitué de composants devant être installés sur des machines distinctes.

Composants d'Acronis Backup Advanced for vCloud

Une installation par défaut comprend au moins deux machines virtuelles situées dans le cluster de gestion vCloud ainsi qu'un certain nombre de matériels virtuels s'exécutant dans le groupe de ressources vCloud.

Les composants suivants sont exécutés dans le groupe de ressources vCloud :

- Les **agents pour VMware**, anciens agents pour ESX(i), sont exécutés en tant que matériels virtuels.
L'agent pour VMware effectue la sauvegarde et la restauration de machines virtuelles ESX(i) sans installer d'agents sur les systèmes invités.

Les composants suivants sont exécutés dans le cluster de gestion :

- **Management Server** doit être installé sur une machine virtuelle qui fonctionne sous Windows.
Le serveur de gestion s'intègre à vCenter Server (alloué pour le groupe de ressources), déploie les agents pour VMware et gère les sauvegardes et les restaurations.
Le serveur de gestion stocke sa configuration, ses journaux et ses statistiques dans des bases de données Microsoft SQL. Les bases de données peuvent être attachées à l'instance SQL Server Express qui est installée par défaut avec le serveur de gestion ou être attachées à n'importe quelle instance SQL Server accessible par le serveur de gestion.
- L'**agent pour vCloud** s'exécute sur une machine virtuelle Linux qui joue également le rôle de serveur Web. L'agent est disponible en tant que modèle Open Virtualization Format (OVF).
L'agent pour vCloud offre une interface graphique aux utilisateurs. L'agent interroge vCloud Director pour obtenir la liste des utilisateurs qui peuvent se connecter au service, ainsi que la liste des machines virtuelles. Selon les choix des utilisateurs, l'agent indique au serveur de gestion les conditions et la fréquence d'exécution des sauvegardes des machines virtuelles sélectionnées. L'agent récupère l'état de protection des machines virtuelles directement auprès

de la base de données du serveur de gestion. Il génère également des rapports sur l'utilisation du service de sauvegarde.

Logiciels nécessaires à l'utilisation d'Acronis Backup Advanced for vCloud

Les utilisateurs de vCloud interagissent avec Acronis Backup Advanced for vCloud par le biais d'un **navigateur Web**. Pour se connecter au service de sauvegarde, ils emploient les mêmes accreditations que pour vCloud Director. Le navigateur Web se connecte au serveur Web de l'agent et affiche les informations fournies par l'agent. La quantité d'informations dépend des droits utilisateur dans vCloud Director.

Avec **Acronis Backup Management Console**, vous pouvez vous connecter directement au serveur de gestion. Cette connexion est nécessaire pour intégrer le serveur de gestion à vCenter Server et déployer les agents pour VMware. Une fois ces opérations effectuées, Acronis Backup Advanced for vCloud peut fonctionner sans la console d'administration. Cependant, vous pouvez en avoir besoin pour le déploiement d'agents supplémentaires, le dépannage et d'autres tâches d'administration. La console peut être installée avec le serveur de gestion ou sur toute autre machine disposant d'un accès réseau au serveur de gestion.

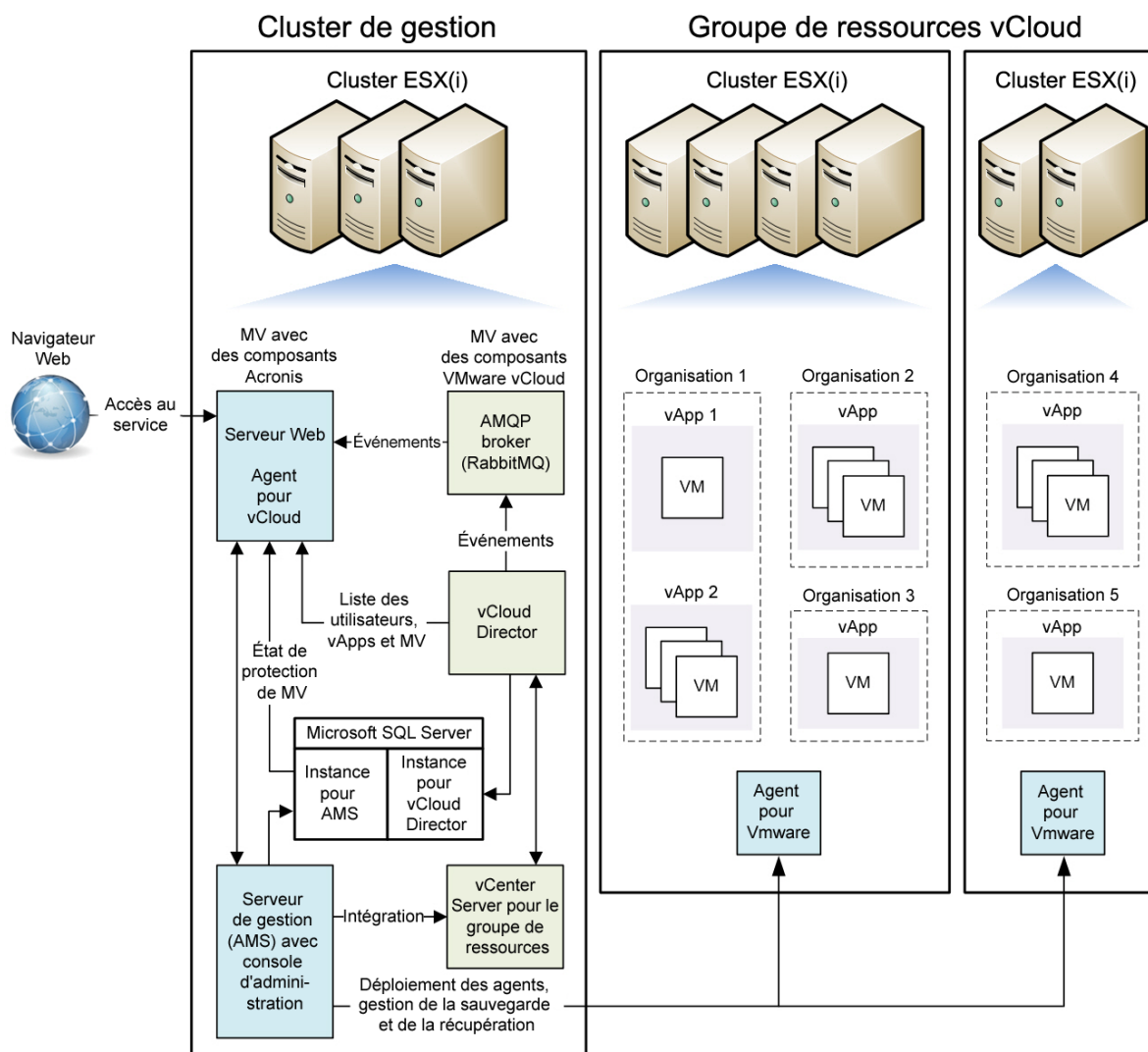
L'agent pour vCloud collecte les événements de vCloud Director via l'AMQP Broker de **RabbitMQ Server**. Si vous ne disposez pas de RabbitMQ Server, ajoutez-le à votre infrastructure vCloud.

Exemple d'installation

Le diagramme suivant illustre les interactions des composants dans le cadre d'une installation par défaut. Dans cet exemple, vCloud Director utilise des bases de données Microsoft SQL. Par conséquent, nous pouvons placer les bases de données du serveur de gestion et les bases de données vCloud Director sur la même machine virtuelle. Cependant, les bases de données du serveur de gestion doivent s'exécuter sur une instance SQL Server distincte.

La console d'administration d'Acronis Backup est installée sur la même machine virtuelle avec le serveur de gestion.

Les machines virtuelles qui exécutent les composants Acronis Backup Advanced for vCloud sont identifiables à leur couleur bleu clair. Les machines virtuelles qui exécutent les composants VMware vCloud figurent en vert clair.



1.2.5 Planification des ressources matérielles

Évaluez la capacité vSphere nécessaire pour exécuter Acronis Backup Advanced for vCloud et déterminez l'emplacement de stockage des sauvegardes.

1.2.5.1 Capacités vSphere exigées

Agent pour VMware (matériel virtuel)

Les agents pour VMware sont exécutés en tant que matériels virtuels dans le groupe de ressources vCloud. Si nécessaire, il est possible de déployer plusieurs agents sur un cluster contenant un grand nombre de machines virtuelles à sauvegarder.

Le tableau suivant contient les capacités vSphere exigées relatives à l'agent pour VMware (matériel virtuel).

Mémoire	Taille du disque dur	Nombre de CPU
1 Go	6 Go (thick provisioning)	2 (paramètre du matériel virtuel par défaut) 4-8 (recommandé en cas de sauvegarde simultanée de cinq à dix machines virtuelles)

Agent pour vCloud

L'agent pour vCloud doit être importé à partir du modèle OVF dans le cluster de gestion.

Le tableau suivant contient les capacités vSphere exigées relatives à l'agent pour vCloud.

Mémoire	Taille du disque dur	Nombre de CPU
2 Go	8 Go (thin provisioning)	1

Serveur de gestion

Acronis Backup Management Server doit être installé dans le cluster de gestion sur une machine virtuelle fonctionnant sous Windows.

Le tableau suivant contient les capacités vSphere exigées et les composants spécifiés pour une machine exécutant Windows Server 2003/2008 R2.

Logiciel installé sur la machine	Mémoire	Taille du disque dur	Nombre de CPU
Management Server + Management Console	2 Go	20 Go minimum (thick provisioning)	1
Management Server + Management Console + Microsoft SQL Server Express (installé par défaut avec le serveur de gestion)	3 Go	30 Go minimum (thick provisioning)	2

1.2.5.2 Planification des stockages de sauvegarde

Acronis Backup Advanced for vCloud stocke les sauvegardes dans des dossiers partagés sur le réseau.

Protocoles réseau pris en charge

Les protocoles réseau suivants sont pris en charge :

- NFS
Pour plus d'informations sur la façon de préparer un stockage NFS, voir « Configuration d'un stockage NFS » (p. 11).
- SMB
- BSP (protocole d'accès à Acronis Backup Storage Node)
Acronis Backup Storage Node prend en charge la déduplication des données sauvegardées. Pour plus d'informations sur la configuration d'un stockage avec déduplication, voir « Configuration de la déduplication » (p. 40).
- FTP
- SFTP

Stockages de sauvegardes

Un stockage de sauvegarde est un dossier affecté au stockage des sauvegardes de l'organisation. Le chemin vers un emplacement de stockage de sauvegarde doit être spécifié selon l'un des formats suivants :

- NFS

nfs://ServeurX/CheminExport:/CheminDossierExport (par exemple :
nfs://Serveur/Sauvegardes/Organisations:/NomOrg)

Remarquez la présence des deux points après le chemin du dossier d'exportation. Pour indiquer le dossier d'exportation sans sous-dossier, utilisez la notation suivante :

nfs://ServeurX/CheminExport:/

- BSP

bsp://ServeurX/NomEmplacement (par exemple : bsp://NoeudStockage/Sauvegardes)

- SMB

smb://ServeurX/.../NomDossier (par exemple,
smb://Serveur/Sauvegardes/Organisations/NomOrg)

\\ServeurX\PartageA\...\NomDossier (par exemple,
\\Serveur\Sauvegardes\Organisations\NomOrg)

- FTP

ftp://ServeurX/.../NomDossier (par exemple,
ftp://Serveur/Sauvegardes/Organisations/NomOrg)

- SFTP

sftp://ServeurX/.../NomDossier (par exemple,
sftp://Serveur/Sauvegardes/Organisations/NomOrg)

Pour tous les types de stockage, à l'exception d'AcronisBackup Storage Node, nous vous recommandons fortement de créer **un dossier individuel** pour chaque organisation. Si vous autorisez plusieurs organisations à partager un stockage de sauvegarde commun, chaque administrateur sera en mesure de voir et de supprimer les sauvegardes des autres organisations, et même de réaliser une restauration à partir de ces sauvegardes.

Sur AcronisBackup Storage Node, créez **un stockage unique** pour toutes les organisations, comme décrit dans « Configuration de la déduplication » (p. 40).

Capacités de stockage exigées

L'espace de stockage requis pour les sauvegardes d'une organisation dépend du volume de données sauvegardées, de la planification des sauvegardes, des règles de rétention et d'autres facteurs. Pour donner une idée, vous pouvez prévoir pour les sauvegardes un espace égal à celui affecté à l'organisation dans vCloud Director.

Organisation d'un stockage de sauvegarde sur un périphérique LUN

Vous avez la possibilité d'utiliser le protocole NFS pour accéder à des périphériques de numéro d'unité logique (LUN) sur Fibre-Channel ou un réseau de zone de stockage iSCSI (SAN).

Pour organiser un dossier NFS sur un périphérique LUN

1. Installez un serveur NFS sur une machine fonctionnant sous Linux.
2. Assignez le périphérique LUN à la machine, afin qu'il apparaisse dans les disques locaux.
3. Dans la configuration du serveur NFS, désignez le périphérique LUN en tant que dossier d'exportation NFS.

Vous pouvez maintenant créer des sous-dossiers et spécifier leur emplacement comme décrit ci-dessus pour le protocole NFS.

Modification d'un stockage de sauvegarde

Le stockage de sauvegarde de l'organisation peut être modifié, si nécessaire, par un administrateur système vCloud. Pour obtenir plus d'informations sur ce processus, veuillez vous référer à « Modification du stockage de sauvegarde » (p. 40).

Configuration d'un stockage NFS

Si vous avez choisi d'utiliser un stockage NFS, configurez-le comme suit.

Sur la machine sur laquelle le serveur de gestion Acronis Backup est installé

Installez Microsoft Windows Services pour NFS. Par exemple, dans Windows 7 ou Windows 8, ouvrez le **Panneau de configuration**, accédez à **Programmes et fonctionnalités**, cliquez sur **Activer ou désactiver des fonctionnalités Windows**, puis activez la case **Services pour NFS** et ses cases imbriquées.

Sur la machine sur laquelle le serveur NFS est installé

Assurez-vous que le dossier d'exportation est configuré correctement :

- a) Le dossier autorise un accès en lecture/écriture.
- b) Vous avez un compte d'utilisateur qui servira de compte anonyme, et vous connaissez l'ID utilisateur et l'ID groupe de ce compte.
Pour trouver l'ID utilisateur et l'ID groupe, exécutez la commande `id <nom d'utilisateur>`.
- c) Tous les comptes d'utilisateur sont mappés au compte anonyme.

Pour configurer le dossier de cette façon, activez-lui l'accès en lecture/écriture en utilisant la commande `chmod`, puis définissez les paramètres dans le fichier de configuration `/etc/exports` pour le dossier, comme suit :

```
/opt/backups *(rw, sync, all_squash, anonuid=65534, anongid=65534)
```

Dans cet exemple, le nom du dossier est `/opt/backups`, et l'ID utilisateur et l'ID groupe du compte anonyme sont 65534 (c'est le compte d'utilisateur `nfsnobody` sur le serveur NFS).

1.3 Installation d'Acronis Backup Advanced for vCloud

1.3.1 Préparation

Avant de lancer l'installation, familiarisez-vous avec l'architecture (p. 6) d'Acronis Backup Advanced for vCloud et assurez-vous que :

- **vCloud Director est installé et configuré.**
- **Les ressources vSphere disponibles sont suffisantes pour déployer Acronis Backup Advanced for vCloud.**

Vous trouverez les valeurs exactes requises dans « Capacités vSphere exigées » (p. 8).

- **Votre stockage prend en charge l'un des protocoles réseau suivants : NFS, SMB, FTP, SFTP ou BSP (protocole d'accès au nœud de stockage Acronis Backup).**

Vous trouverez les exigences exactes dans « Planification des stockages de sauvegarde » (p. 9).

- **Vous détenez un fichier txt contenant vos clés de licence.**

Si vous disposez de plusieurs clés de licence, le format de texte est une clé spécifiée par ligne.

- **Vous possédez le package d'installation d'Acronis Backup Advanced for vCloud.**

Il est constitué :

- Du programme d'installation d'Acronis Backup Advanced.
- Du modèle OVF de l'agent pour vCloud.
- Du script **enable_remote_sql_access.js**.
- **Vous disposez d'une machine virtuelle sur laquelle installer le serveur de gestion,**
 - fonctionnant sous un système d'exploitation Windows (sauf pour les éditions Start, Home et RT).
 - Elle doit posséder un accès réseau à vCenter Server pour le groupe de ressources, ainsi qu'aux clusters ESX(i) du groupe de ressources.
 - Le fuseau horaire Windows sur la machine doit être le même que celui de vCloud Director. (Pour connaître le fuseau horaire de vCloud Director, exécutez la commande **date** sur la machine vCloud Director.)
- **Les noms d'hôte sur votre réseau sont correctement résolus par le DNS en adresses IP.**

Sinon, les hôtes que vous spécifiez pendant l'installation et la configuration doivent utiliser des adresses IP constantes. Selon la condition remplie, vous spécifiez les hôtes par nom d'hôte ou par adresse IP.

1.3.2 Installation et configuration de RabbitMQ Server

L'agent pour vCloud collecte les événements de vCloud Director via l'AMQP Broker de RabbitMQ Server.

Si votre vCloud Director utilise déjà RabbitMQ Server, assurez-vous que le type d'échange est paramétré sur **topic** et suivez les instructions de la section « Installation d'Acronis Backup Management Server » (p. 14).

Si RabbitMQ Server est déjà installé mais **n'est pas** utilisé par vCloud Director, passez à l'étape 5 de la procédure suivante.

Pour installer et configurer RabbitMQ Server

1. Téléchargez RabbitMQ Server sur <http://www.rabbitmq.com/download.html>.
2. Pour installer RabbitMQ Server sur une machine exécutant Windows, téléchargez et exécutez le fichier binaire Windows d'Erlang, disponible à l'adresse <http://www.erlang.org/download.html>.
3. Suivez les instructions d'installation de RabbitMQ pour installer ce produit sur un hôte adéquat. L'hôte doit disposer d'un accès réseau à vCloud Director.
4. Le plug-in de gestion RabbitMQ est indispensable pour la configuration de RabbitMQ Server. Selon le système d'exploitation de l'hôte RabbitMQ Server, effectuez l'une des opérations suivantes :
 - Sous Linux, exécutez les commandes suivantes :

```
rabbitmq-plugins enable rabbitmq_management
service rabbitmq-server stop
service rabbitmq-server start
```
 - Sous Windows :
 - Accédez **Démarrer > Tous les programmes > RabbitMQ Server > RabbitMQ Command Prompt**.
 - Vérifiez que l'invite de commande affiche le dossier contenant les fichiers exécutables RabbitMQ Server, comme C:\Program Files\RabbitMQ Server\rabbitmq_server-3.1.5\sbin. Si nécessaire, modifiez le dossier à l'aide de la commande **cd**.

- Exécutez la commande suivante : **rabbitmq-plugins enable rabbitmq_management**
 - Exécutez **Démarrer > Tous les programmes > RabbitMQ Server > RabbitMQ Service - stop**.
 - Exécutez **Démarrer > Tous les programmes > RabbitMQ Server > RabbitMQ Service - start**.
5. Exécutez les commandes suivantes sur l'hôte RabbitMQ Server pour créer un nouveau compte d'utilisateur :

```
rabbitmqctl add_user <nom d'utilisateur> <mot de passe>
rabbitmqctl set_user_tags <nom d'utilisateur> management
rabbitmqctl set_permissions -p / <nom d'utilisateur> ".*" ".*" ".*"
```

Ici, <nom d'utilisateur> et <mot de passe> sont le nom et le mot de passe du compte d'utilisateur à créer.

Remarque Vous pouvez utiliser un compte d'utilisateur RabbitMQ Server existant avec des autorisations égales ou supérieures à celles indiquées par les commandes ci-dessus.

L'agent pour vCloud d'Acronis Backup Advanced for vCloud utilisera ce compte pour recevoir des notifications d'événements de vCloud Director. Conservez les informations d'identification du compte car vous devrez les indiquer lors de la configuration de l'agent pour vCloud.

6. Dans un navigateur Web, accédez à l'interface utilisateur Internet de RabbitMQ Server, à l'adresse : **http://<nom du serveur>:15672/** Dans le cas présent, <nom du serveur> est l'adresse de l'hôte RabbitMQ Server.
7. Fournissez les informations d'identification de l'utilisateur RabbitMQ Server créé à l'étape 5.
8. Cliquez sur **Exchanges**.
9. Sous **Add a new exchange** :
 - a. Dans **Name**, spécifiez le nom d'un nouvel échange qui sera utilisé par l'agent pour vCloud. Par exemple, spécifiez **vcdExchange**.
 - b. Dans **Type**, sélectionnez **topic**.
 - c. Conservez les valeurs par défaut pour tous les autres paramètres.
 - d. Cliquez sur **Add exchange**.
10. Connectez-vous à vCloud Director en tant qu'administrateur.
11. Cliquez sur **Administration**.
12. Sous **System settings**, cliquez sur **Extensibility**.
13. Sous **Notifications**, cochez la case **Enable notifications**.
14. Sous **AMQP Broker Settings** :
 - a. Dans **AMQP Host**, spécifiez le nom ou l'adresse IP de l'hôte RabbitMQ Server.
 - b. Dans **AMQP Port**, saisissez 5672.
 - c. Dans **Exchange**, spécifiez le nom de l'échange que vous avez créé à l'étape 9.
 - d. Dans **vHost**, saisissez **/**.
 - e. Dans **Prefix**, saisissez **vcd**.
 - f. Dans **User Name** et **Password**, saisissez les informations d'identification du compte d'utilisateur créé à l'étape 5.
15. Cliquez sur **Apply**.

1.3.3 Installation d'Acronis Backup Management Server

Acronis Backup Management Server enregistre sa configuration, ses journaux et ses statistiques dans des bases de données Microsoft SQL, qui peuvent être stockées de deux manières :

- Installez et utilisez SQL Server Express, fourni avec le serveur de gestion. Cette option est disponible lors de l'installation par défaut.
- Utilisez n'importe quelle instance SQL Server existante, accessible par l'intermédiaire du serveur de gestion. Cette option est disponible lors de l'installation personnalisée.

Cette dernière permet notamment de spécifier des paramètres d'installation supplémentaires.

Selon l'emplacement sélectionné pour stocker les bases de données du serveur de gestion, suivez l'une des procédures ci-dessous.

1.3.3.1 Installation type

1. Connectez-vous en tant qu'administrateur sur la machine qui servira de serveur de gestion
2. Lancez le programme d'installation d'Acronis Backup Advanced.
3. Cliquez sur **Installer Acronis Backup**.
4. Acceptez les termes du contrat de licence.
5. Cochez la case **Surveiller et configurer de façon centralisée la sauvegarde des machines physiques et virtuelles**.
6. Fournissez la licence pour Acronis Backup Advanced for vCloud. Entrez toutes vos clés de licence ou importez-les à partir d'un fichier texte.
7. Décidez si la machine participera au programme d'expérience client d'Acronis (CEP).
8. Cliquez sur **Installer** pour procéder à l'installation.
9. Si l'installation est réussie, cliquez sur **Terminer** pour fermer la fenêtre de l'assistant.
10. Copiez le script **enable_remote_sql_access.js** fourni avec le produit sur la machine du serveur de gestion.

Détails. Le script configure l'instance SQL Server pour la rendre accessible à l'agent pour vCloud. Il crée un nouveau compte SQL Server utilisable par l'agent pour vCloud, configure l'instance pour qu'elle écoute un port statique, puis configure le pare-feu Windows pour qu'il autorise les connexions à ce port.

11. Exécutez le script au format suivant :

```
cscript enable_remote_sql_access.js <nouveau-nom-utilisateur>  
<nouveau-motdepasse> [-p <port>]
```

Où :

- <nouveau-nom-utilisateur> et <nouveau-motdepasse> sont le nom d'utilisateur et le mot de passe du nouveau compte.
- **-p** <port> est un paramètre optionnel permettant d'indiquer le port à utiliser.

Par exemple :

```
C:\>cscript enable_remote_sql_access.js User 123 -p 3322
```

Si vous ne spécifiez pas le port, il sera sélectionné automatiquement. Contrôlez le numéro de port sélectionné par le script :

```
Port 1433 is picked
```

Important. Retenez les accréditations et le numéro de port. Vous devrez les indiquer lors de la configuration de l'agent pour vCloud.

1.3.3.2 Installation personnalisée

Préparation de SQL Server

Assurez-vous que l'instance SQL Server qui sera utilisée par le serveur de gestion répond aux exigences suivantes :

- L'instance utilise le mode d'authentification mixte. Ce mode garantit que l'agent pour vCloud peut également accéder à l'instance.
- Le protocole TCP/IP est activé pour l'instance, l'instance utilise un port TCP statique, vous connaissez le numéro de port et votre pare-feu autorise les connexions par le biais de ce port.

Pour changer le mode d'authentification

1. Lancez Microsoft SQL Server Management Studio.
Vous pouvez télécharger Microsoft SQL Server Management Studio à l'adresse <http://www.microsoft.com/fr-fr/download/details.aspx?id=7593>
2. Cliquez avec le bouton droit de la souris sur l'instance et sélectionnez **Propriétés**.
3. Dans **Sécurité**, sous **Authentification serveur**, sélectionnez **Mode d'authentification SQL Server et Windows**.
4. Redémarrez le service de l'instance.

Pour définir les propriétés TCP/IP requises

1. Dans le Gestionnaire de configuration Microsoft SQL Server, développez le noeud **Configuration réseau SQL Server XXXX**. (XXXX correspond à la version de SQL Server, par exemple 2008.)
2. Sélectionnez l'instance.
3. Dans le volet des détails, double-cliquez sur **TCP/IP**.
4. Dans l'onglet **Protocole**, au niveau d'**Activé**, assurez-vous que **Oui** est sélectionné.
5. Dans l'onglet **Adresses IP**, sous **IPAll**, procédez comme suit :
 - Affichez ou modifiez la valeur dans **Port TCP**.

- Assurez-vous que le champ **Ports dynamiques TCP** est vide.

The screenshot shows the 'TCP/IP Properties' dialog box with the 'IP Addresses' tab selected. It contains three IP configuration sections: IP1, IP2, and IPAll. Each section has fields for 'Active', 'Enabled', 'IP Address', 'TCP Dynamic Ports', and 'TCP Port'. In the IPAll section, the 'TCP Port' field is highlighted with a red rectangle and contains the value '1433'. The 'TCP Dynamic Ports' field for IPAll is empty. At the bottom, there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

IP Configuration	Active	Enabled	IP Address	TCP Dynamic Ports	TCP Port
IP1	Yes	No	192.168.1.2	0	
IP2	Yes	No	127.0.0.1	0	
IPAll					1433

- Si vous avez apporté des modifications aux champs lors des étapes précédentes, redémarrez le service de l'instance.

Préparation du compte SQL Server pour le serveur de gestion

Déterminez si le serveur de gestion doit utiliser l'authentification Windows ou l'authentification SQL Server pour se connecter au serveur SQL. Effectuez l'une des opérations suivantes en fonction de votre choix.

Authentification Windows

Si l'authentification Windows est utilisée, créez des comptes d'administrateur local avec le même nom d'utilisateur et le même mot de passe sur la machine qui exécute SQL Server et sur la machine où le serveur de gestion sera installé.

Après l'installation, vous pouvez supprimer le compte du groupe **Administrateurs** sur la machine SQL Server. Sur la machine hébergeant le serveur de gestion, le compte doit rester un administrateur local.

Authentification SQL Server

Si l'authentification SQL Server doit être utilisée, créez un compte de connexion SQL Server qui est membre du rôle serveur **sysadmin**. Lors de la création du compte, désélectionnez les cases

L'utilisateur doit changer de mot de passe à la connexion suivante et **Imposer l'expiration du mot de passe**.

Pendant l'installation, le compte deviendra membre du rôle de base de données **db_owner** pour les bases de données du serveur de gestion (leurs noms commencent par **acronis**). Après l'installation, vous pouvez supprimer le compte du rôle serveur **sysadmin**.

Installation du serveur de gestion

1. Connectez-vous en tant qu'administrateur sur la machine qui servira de serveur de gestion
2. et lancez le programme d'installation d'Acronis Backup Advanced.
3. Cliquez sur **Installer Acronis Backup**.
4. Acceptez les termes du contrat de licence.
5. Dans la page **Comment voulez-vous utiliser cette machine ?** :
 - Cochez la case **Surveiller et configurer de façon centralisée la sauvegarde des machines physiques et virtuelles**.
 - Cochez la case **Je veux sélectionner les composants Acronis manuellement et personnaliser le processus d'installation**.
6. [Facultatif] Dans la page **Sélectionnez les composants que vous voulez installer**, décochez la case **Composants pour l'installation à distance**. Cela vous permettra d'économiser environ 900 Mo d'espace disque.
7. Fournissez la licence pour Acronis Backup Advanced for vCloud. Entrez toutes vos clés de licence ou importez-les à partir d'un fichier texte.
8. Conservez le chemin d'installation par défaut.
9. Acronis Backup Management Server s'exécute en tant que service. Spécifiez le compte utilisateur pour l'exécution du service de l'une des façons suivantes :
 - [Si vous avez opté pour l'authentification Windows] Cliquez sur **Utiliser un compte existant**, cliquez sur **Sélectionner**, puis spécifiez le compte d'un administrateur Windows local que vous avez créé à l'étape « Préparation des comptes d'utilisateur » (p. 16). Si vous y êtes invité, confirmez l'ajout des droits utilisateur supplémentaires au compte.
 - [Si vous avez opté pour l'authentification SQL Server] Conservez le paramètre par défaut afin de créer un compte d'utilisateur dédié à l'exécution du service.
10. Spécifiez l'instance Microsoft SQL Server pour **Serveur SQL opérationnel** et **Serveur SQL de rapports**.

Pour chaque serveur :

 - a. Cliquez sur **Modifier > Utiliser le serveur SQL existant**. Spécifiez l'instance SQL Server au format <Nom d'hôte>\<Nom d'instance> ou <Nom d'hôte>,<Port d'instance>. Par exemple : **dbserver\MyDatabases** ou **dbserver,1433**
 - b. Choisissez la façon dont le serveur de gestion se connectera au serveur SQL :
 - [Si vous avez opté pour l'authentification Windows] Choisissez l'option **Service de serveur de gestion d'Acronis**. Le serveur de gestion se connectera à l'aide du compte du service de serveur de gestion.
 - [Si vous avez opté pour l'authentification SQL Server] Choisissez l'option **Authentification SQL Server**. Spécifiez le nom et le mot de passe de connexion du compte de connexion SQL Server que vous avez choisi à l'étape « Préparation des comptes d'utilisateur » (p. 16).
11. N'activez pas la **page Web du serveur de gestion**.
12. Décidez si la machine participera au programme d'expérience client d'Acronis (CEP).
13. Cliquez sur **Installer** pour procéder à l'installation.
14. Si l'installation est réussie, cliquez sur **Terminer** pour fermer la fenêtre de l'assistant.

Préparation d'un compte SQL Server pour l'agent pour vCloud

L'agent pour vCloud peut se connecter à l'instance SQL Server en utilisant une authentification Windows ou une authentification SQL Server. Afin de préparer un compte pour l'agent pour vCloud, suivez les instructions suivantes :

- Si vous avez choisi **Authentification SQL Server** lors de l'installation du serveur de gestion, utilisez le compte de connexion SQL Server que vous avez spécifié pour celui-ci (voir étape 10b dans « Installation du serveur de gestion » (p. 17)).
- Si vous avez choisi **Authentification Windows** pour le serveur de gestion, utilisez le compte d'utilisateur que vous avez spécifié pour le service du serveur de gestion (voir étape 9 dans « Installation du serveur de gestion » (p. 17)).

Sinon, vous pouvez créer un compte SQL Server dédié comportant un minimum de droits et un mot de passe sans date d'expiration.

Pour créer un compte dédié pour l'agent pour vCloud

1. Exécutez Microsoft SQL Server Management Studio.
2. Développez l'instance, développez **Sécurité**, cliquez avec le bouton droit de la souris sur **Connexions**, puis cliquez sur **Nouvelle connexion**.
3. Dans **Nom connexion**, entrez le nom du compte. Par exemple : **vCloudBackupUser**
4. Sélectionnez **Authentification SQL Server**, puis entrez et confirmez le mot de passe du compte.
5. Décochez la case **L'utilisateur doit changer de mot de passe à la prochaine connexion**. Nous vous conseillons de décocher également la case **Imposer l'expiration du mot de passe**. Si vous ne le faites pas, vous devrez modifier la configuration de l'agent pour vCloud à chaque expiration du mot de passe.
6. Sur la page **Mappage des utilisateurs**, cochez les cases correspondant à toutes les bases de données dont le nom commence par **acronis** (par exemple **acronis_cms**). Pour chacune de ces bases de données, sous **Appartenance au rôle de base de données...**, cochez les cases **db_datareader** et **public**.

1.3.4 Utilisation de la console d'administration

Avec Acronis Backup Management Console, vous pouvez vous connecter directement au serveur de gestion. La console peut être installée avec le serveur de gestion (par défaut) ou sur n'importe quelle autre machine ayant un accès réseau au serveur de gestion.

Pour pouvoir connecter la console au serveur de gestion, l'utilisateur doit être membre du groupe **Centralized Admins Acronis** sur la machine du serveur de gestion.

Si la console est installée sur une machine différente, l'utilisateur doit également être membre du groupe **Remote Users Acronis** sur la machine du serveur de gestion.

Ces deux groupes sont créés automatiquement lors de l'installation du serveur de gestion. Les membres du groupe **Administrateurs** font partie des deux groupes.

Pour démarrer la console d'administration

Double-cliquez sur l'icône **Acronis Backup** du bureau ou effectuez une sélection dans le menu **Démarrer : Acronis > Console d'administration Acronis Backup > Acronis Backup**.

Pour connecter la console au serveur de gestion :

1. Cliquez sur **Se connecter au serveur de gestion**.

2. Spécifiez le nom d'hôte ou l'adresse IP de la machine du serveur de gestion, ainsi que les accréditations d'un compte utilisateur possédant les droits décrits précédemment.

1.3.5 Intégration du serveur de gestion à vCenter Server

Acronis Backup Management Server doit être intégré à vCenter Server pour le groupe de ressources.

Pour cela, utilisez Acronis Backup Management Console. La console est installée automatiquement avec le serveur de gestion.

Pour intégrer le serveur de gestion à vCenter Server

1. Connectez la console au serveur de gestion comme décrit dans « Utilisation de la console d'administration » (p. 18).
2. Dans l'**arborescence de navigation**, cliquez sur **Machines virtuelles**, puis sur **Configurer l'intégration à VMware vCenter**.
3. Cochez la case **Permettre l'intégration avec le serveur vCenter Server suivant**.
4. Indiquez l'adresse IP ou le nom du vCenter Server pour le groupe de ressources. Entrez les accréditations pour accéder au serveur.

Détails. Ce compte sera utilisé pour le déploiement des agents depuis le serveur de gestion. Il doit donc disposer de droits permettant de créer des machines virtuelles sur vCenter Server. Nous recommandons également qu'il possède les droits nécessaires pour la sauvegarde et la restauration, car les agents l'utiliseront pour se connecter au vCenter Server par défaut. Pour consulter la liste complète des droits nécessaires, veuillez vous référer à la section « Droits pour la sauvegarde et la restauration de MV » de l'aide intégrée Acronis Backup.

5. Si un serveur DHCP est présent sur le réseau, vous pouvez, si vous le souhaitez, laisser la case **Déployer automatiquement l'agent pour VMware (matériel virtuel)** activée. Lorsqu'une sauvegarde est sur le point de démarrer, le serveur de gestion déploie automatiquement l'agent pour VMware sur chaque cluster possédant des machines virtuelles à sauvegarder mais sur lesquelles l'agent n'est pas encore installé.

Si le réseau emploie un système d'adresses IP statiques, si vous préférez déployer les agents manuellement ou si le déploiement automatique échoue, désactivez la case **Déployer automatiquement....** Vous devrez alors suivre quelques étapes supplémentaires, décrites dans « Déploiement de l'agent pour VMware » (p. 19).

6. Cliquez sur **OK** pour confirmer les modifications.

Les machines virtuelles gérées par vCenter Server s'affichent dans la section **Machines virtuelles de l'arborescence de navigation**. Elles apparaissent en grisé car l'agent pour VMware n'a pas encore été déployé.

1.3.6 Déploiement de l'agent pour VMware

L'agent pour VMware (matériel virtuel) sera déployé automatiquement le cas échéant si l'option a été activée lors de l'intégration du serveur de gestion à vCenter Server (p. 19).

Si vous avez désactivé le déploiement automatique, déployez l'agent sur chaque cluster ESX(i) dont les machines virtuelles seront sauvegardées.

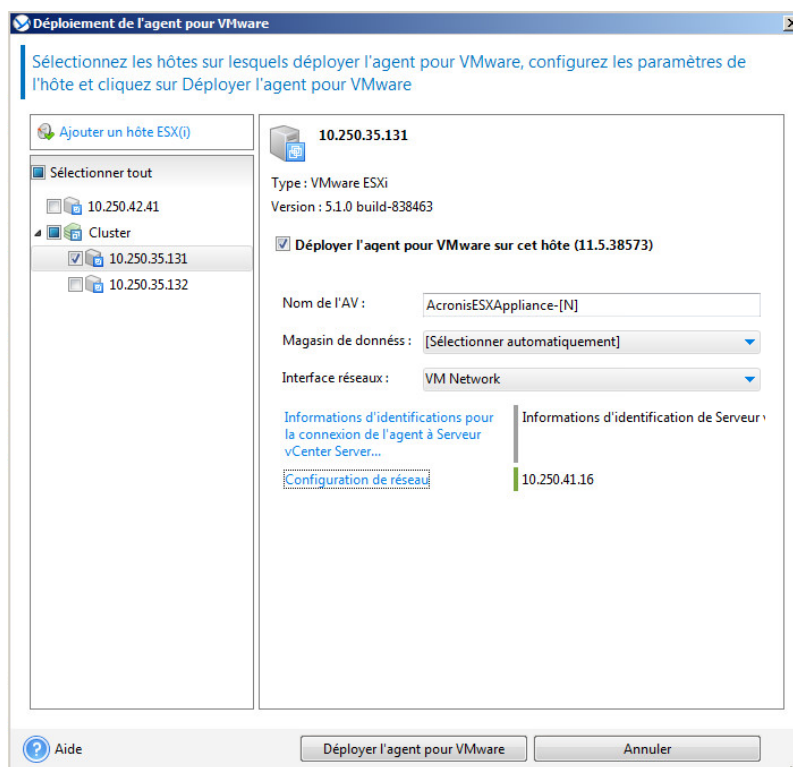
Si un groupe contient un grand nombre de machines virtuelles, vous pouvez déployer des agents supplémentaires dans ce cluster, indépendamment du réglage de déploiement automatique.

Pour déployer l'agent pour VMware

1. Connectez la console au serveur de gestion comme décrit dans « Utilisation de la console d'administration » (p. 18).
2. Dans l'arborescence **Navigation**, développez **Machines virtuelles**, puis cliquez avec le bouton droit de la souris sur l'adresse IP ou le nom du serveur vCenter Server pour le groupe de ressources.
3. Cliquez sur **Déployer l'agent pour VMware**.
4. Pour chaque cluster dont la machine virtuelle sera sauvegardée, procédez comme suit :
 - a. Sélectionnez un hôte vers lequel déployer l'agent.
 - b. Dans **Interface réseau**, sélectionnez l'interface réseau qui fournit un accès au serveur de gestion, au serveur vCenter Server pour le groupe de ressources, aux machines virtuelles du cluster et au stockage de sauvegarde.
 - c. Le lien **Configuration réseau** vous permet d'indiquer si l'agent utilisera une adresse IP dynamique (fournie par un serveur DHCP) ou une adresse IP statique. Vous pouvez ignorer cette étape si vous souhaitez utiliser par défaut une adresse dynamique.

Si vous souhaitez que l'agent utilise une adresse IP statique :

- Cliquez sur **Configuration réseau**.
- Sélectionnez **Utiliser les paramètres réseau suivants**.
- Spécifiez les paramètres réseau appropriés pour l'agent, puis cliquez sur **OK**.



Conseil : vous pourrez modifier les paramètres réseau après le déploiement de l'agent. Pour ce faire, sélectionnez le matériel virtuel dans l'inventaire VMware vSphere et accédez à la console du matériel virtuel. Sous **Options de l'agent**, cliquez sur le lien **Modifier** en regard du nom de l'interface réseau (par exemple, eth0).

5. Cliquez sur **Déployer l'agent pour VMware**.

Le serveur de gestion commence le déploiement de l'agent pour VMware. La progression s'affiche dans la partie inférieure de la fenêtre.

Une fois que l'agent est déployé, la machine de l'agent apparaît dans l'affichage **Machines avec des agents** du serveur de gestion.

1.3.7 Installation de l'agent Acronis Backup pour vCloud

L'agent pour vCloud est fourni sous forme de modèle OVF.

Pour l'installer, déployez le modèle OVF sur votre cluster de gestion. Mappez le réseau du modèle OVF à un réseau autorisant l'accès aux machines virtuelles du cluster de gestion, à l'hôte RabbitMQ Server et à l'instance SQL Server contenant les bases de données du serveur de gestion.

Pour obtenir des informations générales sur le déploiement d'un modèle OVF, veuillez consulter l'article suivant de la base de connaissances VMware :

http://pubs.vmware.com/vsphere-50/topic/com.vmware.vsphere.vm_admin.doc_50/GUID-6C847F77-78CB2-4187-BD7F-E7D3D5BD897B.html.

1.3.8 Configuration de l'agent pour vCloud d'Acronis Backup

Avant de configurer l'agent pour vCloud d'Acronis Backup, assurez-vous que Acronis Backup Management Server est installé (p. 14) et configuré (p. 19).

Connexion

Connectez-vous en tant qu'utilisateur root à la machine avec l'agent pour vCloud. Les accreditations par défaut sont :

- Nom d'utilisateur : **root**
- Mot de passe : **Default0** (sensible à la casse)

Configuration du fuseau horaire

Réglez le fuseau horaire sur celui de la machine vCloud Director. Cela permettra à l'agent pour vCloud de convertir l'heure entre le fuseau horaire de l'utilisateur et le fuseau horaire de vCloud Director.

1. Déterminez le fuseau horaire de la machine vCloud Director. En cas de doute, connectez-vous à la machine et exécutez la commande **date**. La sortie contient l'abréviation du fuseau horaire. Par exemple :

```
Mon Aug 26 23:00:00 EST 2013
```

EST est l'abréviation d'Eastern Standard Time (heure de l'Est des États-Unis). Ce fuseau horaire comprend des zones géographiques des États-Unis et du Canada, ainsi que certains pays d'Amérique du Sud. Pour connaître d'autres abréviations, rendez-vous à l'adresse <http://www.timeanddate.com/library/abbreviations/timezones/>.

2. Dans le répertoire **/usr/share/zoneinfo** de la machine hébergeant l'agent pour vCloud, recherchez le fichier correspondant à votre région et à votre fuseau horaire.
Par exemple, pour le fuseau de l'heure de l'Est des États-Unis, le fichier du fuseau horaire est le suivant : **/usr/share/zoneinfo/US/Eastern**

3. Supprimez les anciens paramètres de fuseau horaire :

```
rm -f /etc/localtime
```

4. Spécifiez les nouveaux paramètres de fuseau horaire :

```
ln -s <fichier_fuseau_horaire> /etc/localtime
```

Par exemple :

```
ln -s /usr/share/zoneinfo/US/Eastern /etc/localtime
```

Configuration des paramètres de connexion

1. Accédez au dossier **/opt/acronis/vcd-agent/bin** et exécutez la commande **configure.sh**.
Tous les scénarios de configuration disponibles sont affichés.

```
Acronis Agent for vCloud configuration:
'1' Initial agent configuration
'2' Show agent configuration
'3' Change agent configuration
'4' Show network settings
'5' Change network settings
'0' Exit
Action [2]:
```

2. Choisissez le scénario **Configuration initiale** de l'agent.
3. Fournissez les paramètres de connexion de vCloud Director :
 - Nom d'hôte ou adresse IP de vCloud Director
 - Accréditations de l'administrateur système vCloud Director
4. Fournissez les informations d'identification de l'utilisateur RabbitMQ Server que vous avez créé lors de la configuration de RabbitMQ Server.
5. Fournissez les paramètres de connexion de Acronis Backup Management Server :
 - Nom d'hôte ou adresse IP de la machine hébergeant le serveur de gestion
 - Nom d'utilisateur et mot de passe d'un utilisateur qui est membre du groupe **Acronis Centralized Admins** et du groupe **Acronis Remote Users** sur la machine hébergeant le serveur de gestion
6. Fournissez les paramètres de connexion pour l'instance SQL Server qui stocke les bases de données du serveur de gestion.

	SQL Server Express installé par défaut	Autre instance SQL Server
Nom d'hôte/Adresse IP :	Nom d'hôte ou adresse IP du serveur de gestion.	Nom d'hôte ou adresse IP de la machine avec l'instance SQL Server utilisée par le serveur de gestion.
Port [1433] :	Port qui a été défini lors de l'exécution du script de configuration (p. 14) sur le serveur de gestion. Si vous avez oublié le numéro de port, ouvrez le Gestionnaire de configuration SQL Server sur le serveur de gestion, sélectionnez Configuration réseau SQL Server XXXX > Protocoles pour ACRONIS , double-cliquez sur TCP/IP , puis examinez le champ Port TCP .	Port qui est utilisé par l'instance SQL Server (p. 15).

Nom d'utilisateur :	Accréditations que vous avez saisies lors de l'exécution du script de configuration (p. 14) sur le serveur de gestion.	Accréditations du compte de connexion SQL Server que vous avez préparé pour l'agent pour vCloud (p. 18).
Mot de passe :		Pour utiliser l'authentification Windows pour l'agent, indiquez le compte d'utilisateur au format <nom d'hôte>\\<nom d'utilisateur> (remarquez l'utilisation des barres obliques inverses <i>doubles</i>). Par exemple : dbserver\\administrator

7. Si vous souhaitez autoriser les utilisateurs à restaurer des fichiers à partir de sauvegardes de machines virtuelles (p. 52), procédez comme suit :

- À l'invite **Voulez-vous autoriser les utilisateurs à restaurer des fichiers individuels...**, appuyez sur **y**.
- Spécifiez le chemin d'accès à un dossier réseau qui sera utilisé comme emplacement de stockage temporaire pour les fichiers restaurés. Les protocoles SMB et NFS sont pris en charge.

Il est judicieux d'utiliser un dossier partagé sur la machine du serveur de gestion. Réservez au moins 20 Go d'espace pour les fichiers temporaires. Si nécessaire, ajoutez un disque individuel à la machine et créez le dossier sur ce disque.

Lorsque vous utilisez le protocole SMB, spécifiez le dossier au format **//Serveur/Partage réseau/Dossier** (remarquez l'utilisation des barres *obliques*). Indiquez le nom d'utilisateur et le mot de passe pour accéder au dossier. Si le stockage se situe sur une machine qui est membre d'un domaine Active Directory, spécifiez le nom d'utilisateur au format <nom de domaine>\\<nom d'utilisateur> (remarquez l'utilisation des barres obliques inverses doubles) ou au format <nom d'utilisateur>@<nom de domaine>.

Lorsque vous utilisez le protocole NFS, spécifiez le dossier au format **nfs://Serveur/CheminExport:/CheminDossierExport** (remarquez la présence des deux points avant la barre finale). Si nécessaire, fournissez les informations d'identification correspondant au dossier. Assurez-vous que le dossier d'exportation est correctement configuré. Pour plus de détails, voir « Configuration d'un stockage NFS » (p. 11).

Configuration des paramètres réseau

La machine dotée de l'agent pour vCloud possède deux adaptateurs réseau : **eth0** pour le réseau interne et **eth1** pour le réseau externe.

eth0 se connecte au réseau interne sur lequel les composants Acronis Backup Advanced for vCloud communiquent avec les composants VMware vCloud. Elle accepte également les connexions entrantes des clients SSH et les navigateurs Web sur le réseau interne.

eth1 accepte les connexions entrantes des navigateurs Web du réseau externe. Assurez-vous que votre pare-feu, votre routeur NAT et les autres composantes du système de sécurité du réseau permettent la connexion externe à cet adaptateur sur les ports 80 et 443.

Par défaut, les adaptateurs récupèrent les paramètres réseau auprès d'un serveur DHCP. Vous pouvez assigner une adresse IP statique à un adaptateur. Par exemple, pour faciliter le réacheminement de port, vous pouvez assigner une adresse IP statique à l'adaptateur externe.

Pour modifier les paramètres réseau de l'agent pour vCloud

1. Exécutez la commande **configure.sh**, puis choisissez le scénario **Modifier les paramètres réseau**.

2. Spécifiez les paramètres réseau de l'adaptateur **eth0**.
 - Pour récupérer les paramètres réseau auprès d'un serveur DHCP, appuyez sur **o**.
 - Pour spécifier les paramètres réseau avec une adresse IP statique, appuyez sur **n**, puis :
 - a. Spécifiez l'adresse IP statique de l'adaptateur. Par exemple : **192.168.0.10**
 - b. Spécifiez le masque de sous-réseau de l'adaptateur. Par exemple : **255.255.0.0**
 - c. Spécifiez l'adresse IP de la passerelle par défaut de l'adaptateur. Par exemple : **192.168.0.1**
3. Spécifiez les paramètres réseau de l'adaptateur **eth1**.
 - Pour récupérer les paramètres réseau auprès d'un serveur DHCP, appuyez sur **o**.
 - Pour spécifier les paramètres réseau avec une adresse IP statique, appuyez sur **n**, puis :
 - a. Spécifiez l'adresse IP statique de l'adaptateur. Par exemple : **10.0.0.10**.
 - b. Spécifiez le masque de sous-réseau de l'adaptateur. Par exemple : **255.0.0.0**

La commande ne demande pas la passerelle par défaut, parce que l'adaptateur est utilisé seulement pour les connexions entrantes.
4. Si vous avez configuré les deux adaptateurs de sorte qu'ils utilisent des adresses IP statiques, spécifiez ce qui suit :
 - a. Dans **Serveur DNS 1**, spécifiez l'adresse IP du serveur DNS.
 - b. [Facultatif] Dans **Serveur DNS 2**, spécifiez l'adresse IP du serveur DNS secondaire.

Les paramètres de serveur DNS s'appliquent aux deux adaptateurs.

Si l'un des adaptateurs utilise un serveur DHCP, les paramètres du serveur DNS pour les deux adaptateurs sont récupérés auprès de ce serveur DHCP.

Si les deux adaptateurs utilisent des serveurs DHCP, leurs paramètres sont récupérés auprès du serveur DHCP pour **eth1** (à condition que la liste de serveurs DNS ne soit pas vide).

Autres opérations

Pour afficher les paramètres réseau

- Exécutez la commande **configure.sh**, puis choisissez le scénario **Afficher les paramètres réseau**.

Pour afficher les paramètres de connexion

- Exécutez la commande **configure.sh**, puis choisissez le scénario **Afficher la configuration de l'agent**.

Pour modifier les paramètres de connexion

- Exécutez la commande **configure.sh**, choisissez le scénario **Modifier la configuration de l'agent**, puis sélectionnez la connexion dont vous souhaitez changer la configuration.

```
'1' Configure connection to vCloud Director
'2' Configure connection to AMQP broker
'3' Configure connection to Acronis Backup Management Server
'4' Configure connection to Acronis Backup Management Server database
'5' Configure access to local agent database
'6' Configure recovery of individual files from backups of VMs
'0' Go to main menu
Action [0]:
```

Pour activer ou désactiver la restauration de fichiers à partir de sauvegardes de machines virtuelles.

1. Exécutez la commande **configure.sh**, puis choisissez le scénario **Modifier la configuration de l'agent**.
2. Choisissez **Configurer la restauration de fichiers individuels à partir de sauvegardes de MV**.

3. Effectuez l'une des actions suivantes :

- Pour activer le paramètre, appuyez sur **y** et spécifiez l'emplacement de stockage temporaire des fichiers restaurés, comme décrit dans l'étape 7 de « Configuration des paramètres de connexion » (voir plus haut dans cette section).
- Pour désactiver ce paramètre, appuyez sur **n**. Les fichiers restaurés se trouvant dans l'emplacement de stockage temporaire ne seront plus à la disposition des utilisateurs.

Mot de passe d'accès à la base de données de l'agent pour vCloud

L'agent pour vCloud fonctionne avec sa base de données à l'aide d'un compte d'utilisateur de base de données avec mot de passe sécurisé. Le nom du compte est **vcda_db_user**. Le mot de passe est généré automatiquement.

Il est généralement inutile de changer le mot de passe. Vous pouvez être amené à changer le mot de passe si votre politique de sécurité prescrit des changements de mot de passe réguliers.

Pour modifier le mot de passe

1. Sur la machine dotée de l'agent pour vCloud, exécutez les commandes suivantes :

```
su postgres
psql
ALTER USER vcda_db_user WITH PASSWORD '<nouveau mot de passe>';
\q
exit
```

2. Exécutez la commande **configure.sh**, puis choisissez le scénario **Modifier la configuration de l'agent**.
3. Choisissez **Configurer l'accès à la base de données agent locale**.
4. Spécifiez le nouveau mot de passe.

1.3.9 Vérification des connexions réseau

Les composants Acronis Backup Advanced for vCloud utilisent les ports TCP pour communiquer les uns avec les autres et avec les composants VMWare vCloud. Assurez-vous que votre pare-feu et les autres composants de votre système de sécurité du réseau autorisent les connexions sur ces ports.

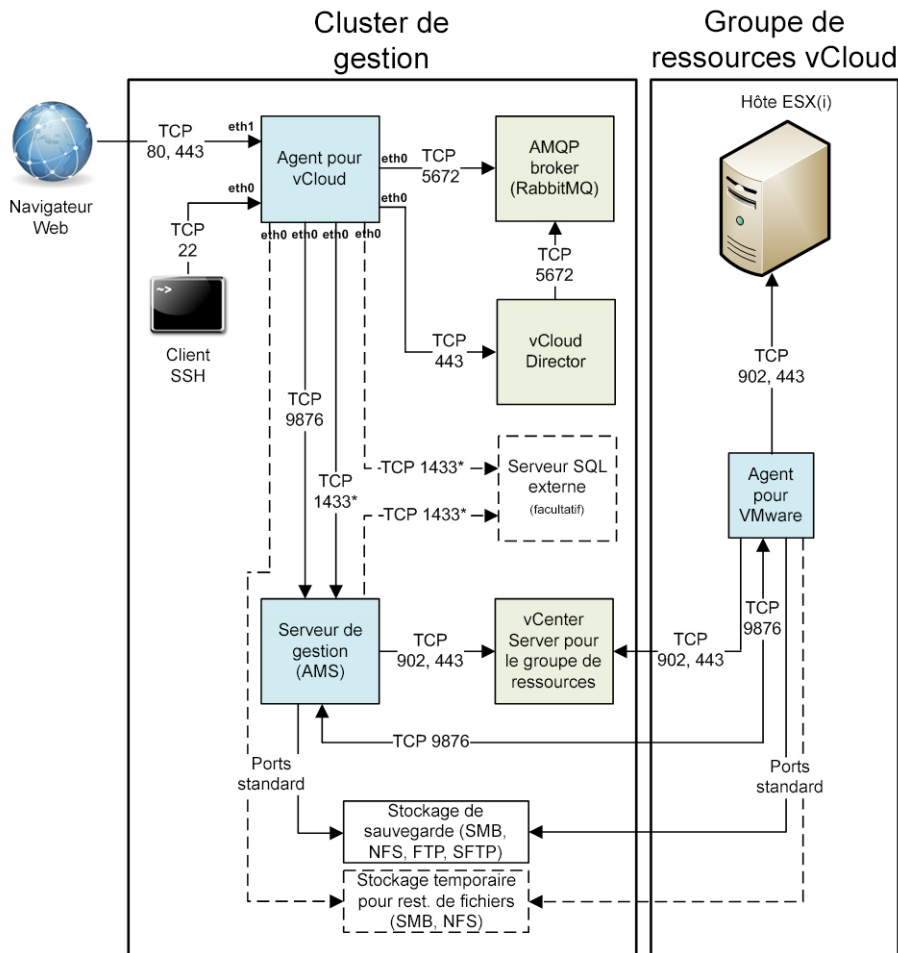
Le schéma ci-dessous illustre les connexions réseau qui sont nécessaires au fonctionnement du service de sauvegarde.

La direction de la flèche indique le composant qui établit une connexion. Le texte indique le port de destination. Le port source est extrait d'une plage standard selon le système d'exploitation :

- L'**agent pour vCloud** et l'**agent pour VMware** utilisent la plage comprise entre 32768 et 61000.
- Le **serveur de gestion** et le **serveur SQL externe** utilisent la plage comprise entre 1025 et 5000 (en cas d'installation sur un système Windows antérieur à Windows Vista) ou entre 49152 et 65535 (en cas d'installation sous Windows Vista ou version ultérieure).

Normalement, les plages standard sont déjà ouvertes.

Pour la machine hébergeant l'agent pour vCloud, **eth0** et **eth1** indiquent la carte réseau grâce à laquelle la connexion est établie.



* Le port est configurable. Le diagramme indique la valeur par défaut.

1.3.10 Mise à jour avec une nouvelle version

La mise à jour d'Acronis Backup Advanced for vCloud (anciennement connu sous le nom Acronis Backup & Recovery pour vCloud) vers une nouvelle version implique la mise à jour du serveur de gestion, des agents pour VMware (anciens agents pour ESX (i)) et de l'agent pour vCloud.

La mise à jour conserve tous les paramètres, y compris les plans de sauvegarde. Les plans de sauvegarde restent appliqués aux machines virtuelles correspondantes.

La mise à jour n'exige aucune licence supplémentaire.

Pré-requis

Avant de commencer la mise à jour, assurez-vous que :

- Vous disposez du programme d'installation de la nouvelle version d'Acronis Backup Advanced.
- Vous disposez du script de mise à jour de l'agent pour vCloud. Le nom du fichier de script est **updateX.sh**, où X est le numéro de version du produit.
- La machine avec l'agent pour vCloud est connectée à Internet. Le script de mise à jour exige une connexion Internet pour télécharger d'autres packages depuis un référentiel Linux.

- Aucune sauvegarde ne sera exécutée pendant la mise à jour. Pour vous en assurer, vous pouvez désactiver la sauvegarde (p. 33) pour toutes les organisations au moment de la mise à jour.

Étape 1 : Mise à jour du serveur de gestion

1. Sur la machine sur laquelle le serveur de gestion est installé, connectez-vous en tant qu'administrateur.
2. Lancez le programme d'installation de la nouvelle version d'Acronis Backup Advanced.
3. Cliquez sur **Installer Acronis Backup**.
4. Acceptez les termes du contrat de licence.
5. Cliquez sur **Mettre à jour**.
6. Poursuivez la mise à jour d'Acronis Backup.

Étape 2 : Mise à jour des agents pour VMware

1. Connectez la console au serveur de gestion comme décrit dans « Utilisation de la console d'administration » (p. 18).
2. Dans l'**arborescence Navigation**, développez **Machines virtuelles**, puis cliquez avec le bouton droit de la souris sur l'adresse IP ou le nom du serveur vCenter Server du groupe de ressources.
3. Cliquez sur **Mettre à jour l'agent pour VMware**.
4. Sélectionnez tous les agents pour VMware de la liste, puis cliquez sur **Mettre à jour l'agent pour VMware**.

Étape 3 : Mise à jour de l'agent pour vCloud

1. Connectez-vous à la machine avec l'agent pour vCloud.
2. Copiez le script de mise à jour vers la machine. Veillez à ne pas placer le fichier de script dans le dossier /opt/acronis. Placez-le par exemple dans le dossier **/root**.
3. Pour que le fichier de script soit exécutable, appliquez la commande suivante :

```
chmod 755 updateX.sh
```
4. Exécutez le script de mise à jour.

Actions à effectuer après la mise à jour

Si vous avez désactivé la sauvegarde au moment de la mise à jour, connectez-vous au service et réactivez la sauvegarde (p. 29).

1.3.11 Désinstallation

Pour désinstaller Acronis Backup Advanced for vCloud :

1. Connectez-vous au service (p. 28).
2. Désactivez la sauvegarde (p. 33) pour chaque organisation.
3. Supprimez tous les agents pour VMware.
 - a. Exécutez Acronis Backup Management Console, puis cliquez sur **Se connecter à un serveur de gestion**.
 - b. Spécifiez le nom d'hôte ou l'adresse IP de la machine actuelle, ainsi que les accréditations d'un compte utilisateur membre du groupe **Centralized Admins Acronis** sur la machine.
 - c. Dans l'**arborescence de navigation**, cliquez sur **Machines virtuelles**.
 - d. Dans la barre d'outils, cliquez sur **Supprimer l'agent pour VMware**.
 - e. Sélectionnez tous les agents.
 - f. Cliquez sur **Supprimer l'agent pour VMware**.

Le serveur de gestion supprime les agents pour VMware. La progression s'affiche dans la partie inférieure de la fenêtre.

- g. Attendez que tous les agents aient été supprimés.
4. Démarrez vSphere Client et connectez-vous au vCenter Server pour le cluster de gestion.
5. Supprimez la machine virtuelle de l'agent pour vCloud.
6. Supprimez la machine virtuelle d'Acronis Backup Management Server ou désinstallez le serveur de gestion comme suit :
 - a. Connectez-vous en tant qu'administrateur sur la machine.
 - b. Cliquez sur **Démarrer -> Tous les programmes -> Acronis -> Désinstaller Acronis Backup**.
 - c. [Option] Pour supprimer les bases de données du serveur de gestion, activez la case **Supprimer le journal, les tâches, les emplacements de stockage et les paramètres de configuration du produit**.
 - d. Cliquez sur **Supprimer**.
7. [Option] Supprimez toutes les sauvegardes des stockages de sauvegarde.

1.4 Connexion au service de sauvegarde

Vous pouvez vous connecter en tant qu'administrateur au service de sauvegarde si les conditions suivantes sont réunies :

- Acronis Backup Advanced for vCloud est installé et configuré.
- Vous possédez un compte d'administrateur système vCloud Director.

Pour vous connecter au service de sauvegarde

1. Accédez à la page de connexion du service de sauvegarde. L'adresse est la suivante : **https://<AdresseServiceSauvegarde>/**.
 - En cas de connexion depuis un réseau interne : <AdresseServiceSauvegarde> est le nom de domaine complet ou l'adresse IP de l'hôte de l'agent pour vCloud sur ce réseau.
Par exemple, **https://vcloudagent.vcloud.example.com/** ou **https://10.200.200.10/**
 - En cas de connexion depuis un réseau externe : <AdresseServiceSauvegarde> est l'URL du service de sauvegarde telle qu'elle s'affiche du côté public d'un pare-feu, d'un équilibreur de charge, d'un proxy NAT/inverse et d'autres composants réseau qui pourraient se trouver avant votre infrastructure.
Par exemple : **https://backup.example.com/**
2. Saisissez le nom d'utilisateur et le mot de passe de votre compte d'administrateur système vCloud Director.
3. Cliquez sur **Connex..**

1.5 Administration d'organisations

1.5.1 Surveillance des organisations

Pour accéder aux informations suivantes sur les organisations, cliquez sur l'onglet **Organisations**.

- **Sauv. activée**
Oui/Non
- **État de protection**

- **Non protégé**

Aucune machine virtuelle de l'organisation n'est protégée. Une machine virtuelle est considérée comme protégée si un plan de sauvegarde (p. 35) lui est appliqué.

- **Jamais sauvegardé**

L'organisation compte des machines protégées mais aucune d'elles n'a exécuté de sauvegarde.

- **OK**

La dernière sauvegarde a réussi sur toutes les machines protégées.

- **Erreur**

La dernière sauvegarde a échoué sur au moins une machine protégée de l'organisation.

Pour afficher l'état d'une machine spécifique, accédez à la vue Administrateur de l'organisation (p. 32). Les états d'une machine virtuelle sont détaillés dans « Surveillance des états de protection » (p. 53).

- **Stockage de sauvegarde**

Stockage de sauvegarde affecté à l'organisation.

- **Quota**

Quota de stockage pour l'organisation.

Si le quota est dépassé, les administrateurs système et les utilisateurs de l'organisation peuvent voir les alertes dans l'interface du service de sauvegarde. À moins d'être appliquées manuellement par un administrateur système, les restrictions d'utilisation du service de sauvegarde ne s'appliquent pas.

Pour consulter les informations suivantes concernant une organisation, sélectionnez l'organisation dans la liste :

- **Nombre de vApps et Nombre de MV**

Les informations suivantes s'affichent pour les organisations ayant le service de sauvegarde activé :

- **Page de connexion**

Adresse employée par les utilisateurs de l'organisation pour se connecter au service.

- **Stockage de sauvegarde**

Chemin du stockage de sauvegarde, quota de stockage de l'organisation et espace occupé par les sauvegardes de l'organisation.

- **Plans de sauvegarde système**

Plans de sauvegarde système (p. 35) disponibles dans l'organisation.

- **Priv. pour les util. de l'org.**

Actions que les utilisateurs de l'organisation sont autorisés à réaliser.

1.5.2 Activation de sauvegarde pour une organisation

Pré-requis

Assurez-vous que l'URL publique est indiquée pour le service de sauvegarde, comme décrit dans la section « URL publique » du chapitre « Configuration du service de sauvegarde » (p. 33).

Si l'URL publique n'est pas indiquée, les utilisateurs ne pourront pas se connecter au service de sauvegarde à l'aide de l'adresse de la page de connexion que vous fournissez.

Pour activer une sauvegarde pour une organisation

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Organisations**.
Une liste des organisations enregistrées dans vCloud Director apparaît.
3. Sélectionnez l'organisation pour laquelle vous souhaitez activer la sauvegarde.
4. Cliquez sur **Configurer**.

The screenshot shows a dialog box titled "Configurer la sau. pour l'org." with a close button (X) in the top right corner. The organization name "Orga2_Cluster02" is displayed in blue text. Below the title, there is a checkbox labeled "Activer la sau. pour l'org." which is checked. Underneath, there are three tabs: "Stock. de sau.", "Plans de sau. système", and "Priv. d'util.", with "Stock. de sau." being the active tab. A text field for "Stock. de sau.:" contains the path "\\10.20.1.30\\phases3\\Acronis\\AVMP9\\Backup\\Acronis". Below this field, there are examples of valid paths: "nfs://server/opt/export/backups/org,", "\\server\\backups\\org,", and "ftp://server/backups/org". There are also input fields for "Nom util.:" (containing "admin") and "Mot de p.:" (masked with dots). At the bottom, there is a "Quota" section with a checked checkbox, a dropdown menu set to "1", and a "Go" button. A small note at the bottom states: "C'est un quota souple. Son dépassement n'empêchera pas la création de sauvegardes. Vous et tous les utilisateurs de l'org. verrez simplement une alerte apparaître." At the bottom right of the dialog are two buttons: "OK" and "Annuler".

5. Dans l'onglet **Stock. de sau.**, procédez comme suit :

- Dans **Stock. de sau.**, indiquez le chemin d'accès au dossier partagé alloué pour le stockage des sauvegardes de l'organisation. Si l'authentification est requise pour accéder au dossier, indiquez les accréditations d'un compte d'utilisateur possédant des autorisations de lecture/écriture pour ce dossier.

Nous recommandons vivement que chaque organisation possède un stockage de sauvegarde distinct. Vous pouvez autoriser plusieurs organisations à partager un stockage de sauvegarde commun, mais, dans ce cas, chaque administrateur de chaque organisation pourra afficher, consulter, supprimer, voire effectuer une restauration à partir des sauvegardes des autres organisations.

Pour plus d'informations sur les types de stockages de sauvegarde pris en charge, reportez-vous à « Planification des stockages de sauvegarde » (p. 9).

- [Facultatif] Indiquez le quota pour l'organisation.

Si le quota est dépassé, les administrateurs système et les utilisateurs de l'organisation peuvent voir les alertes dans l'interface du service de sauvegarde. À moins d'être appliquées manuellement par un administrateur système, les restrictions d'utilisation du service de sauvegarde ne s'appliquent pas.

6. [Facultatif] Dans l'onglet **Plans de sauv. système**, indiquez les plans de sauvegarde système (p. 35) disponibles dans l'organisation. Par défaut, tous les plans de sauvegarde système seront disponibles.

Vous pouvez faire de l'un de ces plans le *plan de sauvegarde par défaut*. Pour ce faire, spécifiez le plan de sauvegarde dans **Plan de sauvegarde par défaut**. Celui-ci s'appliquera automatiquement à toutes les machines virtuelles futures de l'organisation. Pour appliquer aussi ce plan de sauvegarde à toutes les machines virtuelles actuelles, cochez la case **Appliquer à tous les vApps et machines virtuelles de l'organisation**.

Les utilisateurs pourront changer le plan de sauvegarde par défaut sur leur machine, à condition qu'ils soient autorisés à appliquer des plans de sauvegarde (voir étape 7).

7. [Facultatif] Dans l'onglet **Priv. d'util.**, indiquez les actions que les utilisateurs de l'organisation seront autorisés à effectuer. Par défaut, les actions suivantes sont disponibles pour les utilisateurs :

- Appliquer et retirer des plans de sauvegarde
- Créer, modifier et supprimer des plans de sauvegarde
- Effectuer une sauvegarde par heure
- Effectuer une sauvegarde à la demande (« Sauv. maint. »)
- Restaurer des machines virtuelles
- Restaurer des fichiers à partir de sauvegardes de machines virtuelles

Quel que soit votre choix, les administrateurs système sont autorisés à effectuer toutes ces actions au sein de l'organisation.

Si vous décochez la case **Connex. au service de sauv.**, seuls les administrateurs système pourront utiliser le service de sauvegarde pour cette organisation. Pour plus d'informations sur la procédure, veuillez vous référer à « Exploitation dans une organisation » (p. 32).

Configurer la sauv. pour l'org.



MyOrganization

☒ Activer la sauv. pour l'org.

Stock. de sauv.

Plans de sauv. système

Priv. d'util.

Spécifiez les priv. pour les util. de l'organisation.

☒ Connex. au service de sauv.

☒ Appli. et retirer plans de sauv.

☒ Créer, modif. et suppr. des plans de sauv.

☒ Fréquence sauv. par heure

Examiner l'impact sur votre infrastructure

☒ Effec. sauv. à la demande (« Sauv. maint. »)

☒ Restaurer les MV

☒ Restaurer fichiers des MV

OK

Annuler

8. Confirmez les modifications.

9. S'il s'agit de la première activation d'une sauvegarde pour cette organisation, effectuez une sauvegarde de test afin de vérifier que l'agent pour VMware est correctement déployé sur le cluster de l'organisation.
 - a. Saisie de l'organisation (p. 32).
 - b. Sauvegarde d'une machine virtuelle (p. 46).

Selon la décision que vous avez prise à l'étape 7, le service de sauvegarde devient disponible soit pour les administrateurs uniquement, soit pour les administrateurs système et les utilisateurs de l'organisation.

Si le service de sauvegarde est disponible pour les utilisateurs de l'organisation :

1. Indiquez aux administrateurs de l'organisation l'adresse de la page de connexion attribuée à l'organisation. Cette adresse figure sous **Page de connexion** dans la zone de détails de l'organisation.
2. Rappelez aux utilisateurs de l'organisation qu'il peuvent avoir recours au lien **Aide** et au Guide de l'utilisateur.

1.5.3 Utilisation dans une organisation

Les administrateurs système vCloud peuvent effectuer n'importe quelle opération réalisable par les administrateurs de l'organisation.

Pour administrer une organisation

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Organisations**.
Une liste des organisations enregistrées dans vCloud Director apparaît.
3. Sélectionnez l'organisation à administrer. Le service de sauvegarde doit déjà avoir été activé pour l'organisation (p. 29).
4. Cliquez sur **Ouvrir**.
L'interface de l'administrateur d'organisation s'affiche alors.
5. Veuillez vous référer à la section du guide de l'utilisateur (p. 45) Acronis Backup Advanced for vCloud correspondant à l'opération que vous souhaitez exécuter.

1.5.4 Autoriser les non-administrateurs à utiliser le service

Les administrateurs système et les administrateurs de l'organisation peuvent autoriser les membres de tout rôle vCloud Director à utiliser le service de sauvegarde.

Vous pouvez soit utiliser un rôle existant, soit créer un rôle dédié pour l'accès aux services de sauvegarde. Si vous voulez utiliser un rôle existant, ignorez la première procédure.

Pour créer un rôle dans vCloud Director

1. Connectez-vous à vCloud Director en tant qu'administrateur.
2. Cliquez sur **Administration > Rôles**.
3. Créez un compte.
Le moyen le plus simple d'y parvenir est de sélectionner le rôle **Utilisateur vApp** et d'utiliser l'action **Copier vers...** dans le menu contextuel. Vous pouvez attribuer le nom de votre choix au nouveau rôle, par exemple : **Administrateur de sauvegarde**.
4. Signalez l'existence du nouveau rôle aux administrateurs d'organisation.

Pour autoriser les membres d'un rôle vCloud Director à utiliser le service de sauvegarde

1. Saisissez l'organisation, comme décrit dans « Utilisation dans une organisation » (p. 32).
2. Pour les étapes suivantes, reportez-vous à la section « Autoriser les non-administrateurs à utiliser le service » (p. 61) du Guide de l'utilisateur Acronis Backup Advanced for vCloud.

1.5.5 Désactivation de sauvegarde pour une organisation

Pour désactiver la sauvegarde pour une organisation

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Organisations**.
3. Sélectionnez l'organisation pour laquelle vous souhaitez désactiver la sauvegarde.
4. Cliquez sur **Configurer**.
5. Décochez la case **Activer la sauv. pour l'org.**
6. Confirmez les modifications.

En conséquence :

- Les utilisateurs de l'organisation ne pourront plus faire usage du service de sauvegarde.
- Les plans de sauvegarde de l'organisation seront retirés des machines virtuelles mais préservés par l'agent pour vCloud. Si vous réactivez la sauvegarde, il suffira de réappliquer les plans de sauvegarde aux machines de sorte que celles-ci soient de nouveau protégées.
- Les sauvegardes existantes seront conservées. Si les sauvegardes sont devenues inutiles, vous pouvez les supprimer manuellement des stockages de sauvegarde.

1.6 Configuration du service de sauvegarde

Pour accéder à ces paramètres, cliquez sur l'onglet **Paramètres**.

Plans de sauvegarde système

Ce paramètre est utilisé pour la gestion des plans de sauvegarde système (p. 35).

Paramètres de serveur de messagerie

Ces paramètres sont nécessaires pour envoyer des notifications par messagerie électronique aux utilisateurs de l'organisation. Aucune notification n'est envoyée tant que les paramètres du serveur de messagerie ne sont pas saisis.

L'objet peut inclure du texte ordinaire et des variables. Dans les messages électroniques reçus, chaque variable est remplacée par sa valeur au moment de l'exécution du plan de sauvegarde.

L'objet par défaut de la notification est le suivant :

[Service de sauv.]: %Organization name% - %Backup plan name%

Où :

- **%Organization name%** est le nom de l'organisation.
- **%Backup plan name%** est le nom du plan de sauvegarde.

Les autres variables ne sont pas prises en charge.

Conseil Les notifications par messagerie électronique adressées à un administrateur système sont configurées sur le serveur de gestion. Sélectionnez **Options > Options du serveur de gestion**, puis spécifiez les paramètres du serveur de messagerie dans **Paramètres de courrier électronique**. Dans **Notifications d'alerte**, vous pouvez sélectionner les alertes spécifiques associées à l'envoi de notifications.

Options de sauvegarde et de récupération

■ Sauvegarde simultanée

Spécifiez le nombre de machines virtuelles que l'agent pour VMware peut sauvegarder simultanément. La valeur par défaut est 5. La valeur maximale est 10.

La valeur que vous spécifiez s'applique à un plan de sauvegarde. Si un agent exécute plusieurs plans de sauvegarde en même temps, le nombre de machines en cours de sauvegarde peut dépasser la valeur du paramètre, mais ne peut malgré tout excéder 10. Un plan de sauvegarde nécessitant la sauvegarde de la 11e machine ne démarre pas tant que l'une des opérations de sauvegarde n'est pas terminée.

Conseil. La sauvegarde simultanée de plusieurs machines virtuelles augmente la quantité de ressources de CPU utilisée par les agents pour VMware. Par défaut, l'agent pour VMware utilise deux processeurs virtuels. Si vous observez que l'utilisation de CPU lors de la sauvegarde approche les 100 %, augmentez le nombre de processeurs virtuels dans le matériel virtuel. Cela peut accroître les performances de sauvegarde simultanée de façon significative.

■ Vitesse de connexion au réseau

Définissez la quantité de bande passante de connexion réseau allouée pour transférer les données de sauvegarde.

Par défaut, la vitesse est définie sur le maximum, de sorte que le logiciel utilise toute la bande passante réseau disponible lors du transfert des données de sauvegarde. Utilisez cette option pour réserver une partie de la bande passante réseau pour d'autres activités réseau.

■ Traitement des erreurs

Spécifiez la façon dont les erreurs éventuelles sont gérées durant la sauvegarde ou la restauration.

Lorsqu'une erreur récupérable se produit, le programme tente à nouveau d'effectuer l'opération qui a échoué. Vous pouvez définir l'intervalle de temps, ainsi que le nombre de tentatives. Les tentatives s'arrêteront dès que l'opération réussira OU que le nombre de tentatives sera atteint, suivant lequel de ces deux cas de figure se produit en premier.

Par exemple, si **Nombre de tentatives** est réglé sur 30, si **Intervalle entre tentatives** est réglé sur 30 secondes et si la destination de sauvegarde sur le réseau devient inaccessible ou inatteignable, le programme essaiera d'atteindre la destination toutes les 30 secondes, mais pas plus de 30 fois.

Rapport d'utilisation pour Acronis

Ces paramètres sont utilisés lorsque vous envoyez des rapports sur l'utilisation du service de sauvegarde à Acronis.

■ Nom société

Spécifiez le nom de votre société. Acronis l'utilisera pour vos rapports d'utilisation.

■ Adresse électronique de contact

Spécifiez votre adresse électronique. Acronis utilisera cette adresse pour vous contacter, si nécessaire.

Si vous souhaitez automatiser l'envoi des rapports, cochez la case **Envoyer automatiquement des rapports d'util. à Acronis le 1er jour de chaque mois**.

Pour plus d'informations sur les rapports d'utilisation, veuillez vous référer à « Génération de rapports d'utilisation » (p. 37).

Quota

Ce paramètre spécifie quel paramètre sera utilisé pour déterminer le quota de stockage d'une organisation. Choisissez l'une des options suivantes :

- **Utilis. stock.** (par défaut)
Le quota sera déterminé en fonction de la taille totale de toutes les sauvegardes dans le stockage de sauvegarde.
- **Total des données sauvegardées**
Le quota sera déterminé en fonction de la quantité totale de données sauvegardées. Ce paramètre est utile si les sauvegardes sont dédoublées.

URL publique

Ce paramètre permet d'afficher une adresse de service de sauvegarde lisible que vous pouvez fournir aux utilisateurs de l'organisation. L'adresse figure dans les détails de l'organisation, sous **Page de connexion**.

Par défaut, l'agent pour vCloud utilise son adresse IP pour élaborer les adresses de page de connexion. Par exemple, si l'adresse IP est **10.200.200.10**, après que la sauvegarde est activée pour une organisation nommée **MyOrganization**, l'adresse sous **Page de connexion** dans les détails de l'organisation s'affichera comme suit : **https://10.200.200.10/org/MyOrganization**

Dans **URL publique**, spécifiez la façon dont l'URL du service de sauvegarde s'affiche du côté public d'un pare-feu, d'un équilibreur de charge, d'un proxy NAT/inverse et d'autres composants réseau pouvant se situer à l'avant de votre infrastructure. L'URL doit comporter une adresse IP externe ou un nom DNS valide pouvant être résolu par les serveurs DNS des utilisateurs.

Par exemple : **https://www.backup.example.com/**

Une fois l'URL publique spécifiée, l'adresse du service de sauvegarde de **MyOrganization** se présente comme suit : **https://www.backup.example.com/org/MyOrganization**

1.6.1 Gestion des plans de sauvegarde système

Qu'est-ce qu'un plan de sauvegarde ?

Il s'agit d'un ensemble de règles établissant la manière dont vos machines virtuelles sont protégées. Il inclut la planification de sauvegarde, les règles de rétention et les options de sauvegarde telles que la protection par mot de passe.

Les utilisateurs du service de sauvegarde créent des plans, puis les appliquent à leurs machines virtuelles.

Qu'est-ce qu'un plan de sauvegarde système ?

Pour simplifier la tâche des utilisateurs du service de sauvegarde, l'administrateur système a la possibilité de créer des plans de sauvegarde prêts à l'emploi, appelés « plans de sauvegarde système ».

Lorsqu'il active la sauvegarde pour une organisation, l'administrateur système indique les plans de sauvegarde système qui seront mis à la disposition des utilisateurs. Les utilisateurs peuvent appliquer

ces plans de sauvegarde à leurs machines virtuelles mais ne peuvent ni les supprimer ni en changer les règles de planification et de rétention.

Le tableau ci-dessous détaille les plans de sauvegarde système fournis avec le logiciel.

Nom	Planification	Période de rétention
Quotidiennement	Tous les jours à 22:00	Une semaine
Hebdomadaire	Tous les vendredis à 22:00	4 semaines
Mensuelle	Un vendredi toutes les quatre semaines, à 22:00	48 semaines

Ces plans de sauvegarde démarrent à 22:00, heure réglée pour l'agent pour VMware. Les dates et heures indiquées à l'utilisateur sont ajustées en fonction du fuseau horaire de sa machine. Ainsi, deux utilisateurs employant la même planification mais situés dans deux fuseaux horaires séparés peuvent voir des horaires différents.

Actions disponibles sur les plans de sauvegarde système

L'administrateur système peut éditer, créer ou supprimer des plans de sauvegarde système.

Pour créer ou éditer un plan de sauvegarde système

Important : éditer un plan de sauvegarde système impactera l'ensemble des organisations à la disposition desquelles vous l'avez mis.

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Paramètres**.
3. Cliquez sur **Plans de sauvegarde système**.
4. Selon votre intention, cliquez sur **Créer** ou sélectionnez le plan à éditer, puis cliquez sur **Éditer**.
5. Dans **Nom**, saisissez le nom du plan de sauvegarde. Il ne doit pas être identique au nom de l'un des autres plans de la liste.
6. Indiquez les règles de planification et de rétention (p. 55) de votre plan de sauvegarde.
Détails. Un plan de sauvegarde système pouvant être distribué sur plusieurs organisations, il n'est pas possible d'activer les options de sauvegarde telles que le chiffrement ou les notifications lors de la création ou de la modification du plan. Vous pouvez à la place activer différentes options de sauvegarde dans chaque organisation où le plan est disponible. Pour activer des options de sauvegarde, passez à une organisation spécifique (p. 32), sélectionnez le plan dans la liste, puis cliquez sur **Définir des options**. Les utilisateurs des organisations peuvent aussi activer ou changer ces options.
7. Cliquez sur **OK**.

Pour mettre un nouveau plan de sauvegarde système à la disposition d'une organisation

1. Dans l'onglet **Organisations**, sélectionnez l'organisation, puis cliquez sur **Configurer**.
2. Cliquez sur **Plans de sauvegarde système**.
3. Cochez la case correspondant au plan.
4. Cliquez sur **OK**.

Le fait de désélectionner la case correspondant à un plan de sauvegarde système a le même effet que la suppression de ce dernier, mais uniquement au sein de l'organisation.

Pour supprimer un plan de sauvegarde système

Attention : la suppression d'un plan de sauvegarde désactivera les sauvegardes des machines auxquelles il était appliqué, jusqu'à ce que les utilisateurs activent de nouveaux plans.

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Paramètres**.
3. Cliquez sur **Plans de sauvegarde système**.
4. Sélectionnez le plan de sauvegarde à supprimer.
5. Cliquez sur **Supprimer**.
6. Confirmez votre choix.

1.7 Génération de rapports d'utilisation

Les rapports d'utilisation fournissent des données d'historique sur l'utilisation du service de sauvegarde. Les rapports suivants sont disponibles :

- **Organisation sélectionnée**
Ce rapport contient les statistiques d'une organisation donnée. Il permet de facturer l'utilisation du service de sauvegarde aux organisations.
- **Toutes les org.**
Ce rapport contient les statistiques pour toutes les organisations qui ont utilisé le service de sauvegarde durant la période de référence (y compris les organisations pour lesquelles le service de sauvegarde est désactivé).
- **Rapport pour Acronis**
Outre les mêmes informations que le rapport de toutes les organisations, ce rapport comporte également le nom de votre société et l'adresse électronique de contact.

Paramètres de rapport

Les valeurs de tous les paramètres sont contrôlées tous les jours à 23 h 55, conformément aux réglages horaires de vCloud Director. Le rapport utilise les valeurs existant à ce moment-là.

Le rapport comprend les paramètres suivants pour l'organisation :

- **Nombre de MV protégées** : Nombre total de machines protégées (c'est-à-dire les machines auxquelles des plans de sauvegarde sont appliqués), que des sauvegardes de ces machines existent ou non.
- **Utilis. stock.** : Taille totale de toutes les sauvegardes dans le stockage de sauvegarde (exprimée en giga-octets). Ce paramètre peut être exclu du rapport, en fonction des paramètres du service de sauvegarde.
- **Total des données sauvegardées** : Quantité totale des données sauvegardées. Cette quantité comprend le contenu initial des disques de la machine virtuelle et les modifications incrémentielles ultérieures apportées à ce contenu.
- **Excédent de quota** : Quantité de données qui dépasse le quota défini pour l'organisation (exprimée en giga-octets).
- **Taille disque MV protégées** : Taille totale des disques durs des machines protégées (exprimée en giga-octets), indépendamment de l'espace occupé sur ces disques.
- **Taille mém. RAM MV protégées** : Taille totale de la mémoire des machines protégées (exprimée en giga-octets).
- **Nombre de CPU des MV protégées** : Nombre total de CPU des machines protégées.

Pour générer un rapport d'utilisation

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Organisations**.

3. Si vous souhaitez générer un rapport pour une organisation, sélectionnez celle-ci. Sinon, ignorez cette étape.
4. Cliquez sur **Générer rapport**, puis cliquez sur **Organisation sélectionnée, Toutes les org.** ou **Rapport pour Acronis**.
5. Dans **Période**, sélectionnez la période couverte par le rapport :
 - **Mois en cours** : le rapport comprendra des données entre le premier jour du mois en cours et le jour actuel (si vous générez le rapport après 23 h 55) ou jusqu'au jour précédent (si vous générez le rapport avant 23 h 55).
 - **Mois précédent** : le rapport comprendra des données pour le mois précédent. Par exemple, en avril, vous obtiendrez un rapport pour la période comprise entre le 1er mars et le 31 mars.
 - **Période personnalisée** : le rapport comprendra des données de l'intervalle que vous spécifiez.
6. Si vous générez un rapport pour Acronis, ignorez cette étape. Le type de rapport sera réglé sur **Statistiques journ..**
 Autrement, dans **Type**, sélectionnez le type de rapport :
 - **Statistiques journ.** : le rapport comprendra les valeurs des paramètres de rapport pour chaque jour de la période visée. Le rapport comprend également le *résumé* : les valeurs minimale, maximale et moyenne de chaque paramètre de rapport pour la période visée.
 - **Rapport synthèse** : le rapport **Organisation sélectionnée** comprendra uniquement le résumé (voir option précédente). Le rapport **Toutes les org.** comprendra des valeurs moyennes tout au long de la période du rapport pour chaque organisation.
7. Cliquez sur **OK**. Le rapport s'affichera dans une fenêtre ou un onglet de navigateur distinct.
8. [Facultatif] Pour imprimer le rapport, cliquez sur **Imprimer**. Pour enregistrer le rapport en tant que fichier .csv (valeurs séparées par des virgules), cliquez sur **Enreg. au form. .csv**.
9. Si vous souhaitez envoyer un rapport que vous avez généré pour Acronis :
 - a. Cliquez sur **Envoyer à Acronis**.
 - b. Si vous y êtes invité, fournissez le nom de votre société et l'adresse électronique de contact.
Conseil. Le logiciel peut mémoriser ces paramètres pour vous éviter d'avoir à les saisir à chaque fois. Veuillez vous référer à « Rapport d'utilisation pour Acronis » dans « Configuration du service de sauvegarde » (p. 33).
 - c. [Facultatif] Si vous souhaitez automatiser l'envoi des rapports, cochez la case **Envoyer automatiquement des rapports d'util. à Acronis le 1er jour de chaque mois**.

1.8 Affichage des journaux d'audit

Le service de sauvegarde comprend un journal d'audit qui enregistre les opérations effectuées par les utilisateurs.

Les administrateurs système et de l'organisation peuvent voir le journal dont la portée se trouve dans leur zone de contrôle.

Pour afficher le journal d'audit

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Paramètres**.

Un administrateur système peut utiliser le journal d'audit pour effectuer des opérations de dépannage. Il peut également afficher les détails d'une tâche qui a échoué ou collecter les journaux

(p. 39), ainsi que d'autres informations de l'agent pour vCloud, et les envoyer pour analyse au support technique Acronis.

1.9 Collecte de journaux

L'outil de collecte de journaux enregistre les fichiers journaux de l'agent pour vCloud dans un fichier **sysinfo.zip**. Ce fichier est nécessaire lorsque vous contactez le support technique d'Acronis.

Pour collecter des journaux à l'aide de l'interface Web

1. Connectez-vous au service.
2. Cliquez sur **Aide -> Collection de Journal**.
3. Si votre navigateur Web vous y invite, indiquez où enregistrer le fichier.

Si vous ne pouvez pas vous connecter au service en raison d'un problème du serveur Web, vous pouvez collecter des journaux à l'aide d'un script.

Pour collecter des journaux à l'aide d'un script

1. Connectez-vous en tant qu'utilisateur root à la machine avec l'agent pour vCloud. Les accréditations par défaut sont :
 - Nom d'utilisateur : **root**
 - Mot de passe : **Default0** (sensible à la casse)
2. Exécutez la commande suivante pour démarrer l'outil de collecte de journaux :

```
/opt/acronis/vcd-agent/bin/sysinfo.sh
```
3. Spécifiez le nom d'utilisateur et le mot de passe d'un administrateur système vCloud Director.
4. Indiquez où enregistrer le fichier.
5. Une fois le fichier enregistré, copiez-le de la machine de l'agent vers un emplacement approprié à l'aide, par exemple, de l'outil **sftp**.

1.10 Scénarios avancés

Cette section décrit la façon d'utiliser Acronis Backup Advanced for vCloud dans des situations plus complexes.

1.10.1 Reprise d'activité après sinistre de machines physiques vers vCloud

Si une organisation sauvegarde ses machines physiques à l'aide d'Acronis Backup, vous pouvez l'autoriser à stocker les sauvegardes obtenues dans son stockage de sauvegarde Acronis Backup Advanced for vCloud.

Pour ce faire, configurez le stockage de sauvegarde comme un partage réseau et autorisez l'administrateur de l'organisation à effectuer l'une des opérations suivantes :

1. Sauvegarder les machines physiques directement sur le stockage de sauvegarde.
2. Dupliquer ou déplacer les sauvegardes de machines physiques vers le stockage de sauvegarde, dans le cadre de plans de sauvegarde Acronis Backup.
3. Exporter les sauvegardes de leur emplacement d'origine vers le stockage de sauvegarde.

En conséquence, l'administrateur de l'organisation verra les sauvegardes des machines physiques dans l'interface Acronis Backup Advanced for vCloud. En cas de sinistre, l'administrateur de

l'organisation pourra recréer un serveur physique en tant que machine virtuelle de son organisation vCloud.

1.10.2 Configuration de la déduplication

Cette section décrit comment configurer un stockage dans lequel les données seront dédupliquées dans toutes les organisations, mais où les utilisateurs ne verront que des sauvegardes de leur organisation.

Important Consultez la section « Meilleures pratiques de déduplication » dans l'aide du produit Acronis Backup avant de configurer la déduplication.

La déduplication est prise en charge par le nœud de stockage Acronis Backup. Le nœud de stockage requiert une machine avec la configuration suivante :

- Processeur multi-noyau avec une vitesse d'horloge d'au moins 2,5 GHz
- Au moins 32 Go de RAM
- Un système d'exploitation Windows 64 bits

Lors de l'utilisation de la déduplication, pensez à modifier le paramètre de quota (p. 33) pour le faire passer de **Utilis. stock.** à **Total des données sauvegardées**, car les statistiques d'utilisation du stockage d'une seule organisation ne peuvent pas être séparées dans ce cas.

Pour configurer la déduplication

1. Sur la machine qui va agir comme nœud de stockage, exécutez le programme d'installation d'AcronisBackup Advanced.
2. Installez le nœud de stockage tel que décrit dans la section « Prise en main avec un nœud de stockage » de l'Aide d'AcronisBackup.
3. Créez des comptes d'utilisateur sur le nœud de stockage (un par organisation). Assurez-vous que ces comptes ne **sont pas** membres du groupe Administrateurs.
4. Créez **un seul emplacement de stockage** avec déduplication, comme décrit dans la section « Création d'un emplacement de stockage géré centralisé » dans l'Aide d'Acronis Backup.

Pour spécifier l'emplacement de stockage de sauvegarde

Lors de l'activation de la sauvegarde pour une organisation (p. 29) :

1. Spécifiez l'emplacement de stockage au format **bsp://ServerX/VaultName** (par exemple, bsp://StorageNode/Backups).
2. Spécifiez le compte d'utilisateur pour cette organisation.

1.10.3 Modification du stockage de sauvegarde

Les administrateurs système vCloud peuvent changer le stockage de sauvegarde attribué à une organisation.

Si le périphérique de stockage manque d'espace et ne peut pas être mis à niveau, vous pouvez faire migrer une partie ou l'ensemble des stockages de sauvegarde vers un nouveau périphérique. Outre le fait de modifier les chemins de stockage, vous avez besoin de déplacer vers le nouvel emplacement les sauvegardes créées précédemment. Sinon, ces sauvegardes ne seront pas disponibles pour les utilisateurs de l'organisation. Durant le déplacement des sauvegardes, toutes les opérations qui nécessitent un accès au stockage de sauvegarde doivent être désactivées. Cela risque de ralentir l'accès à d'autres périphériques de stockage situés sur le même périphérique. Pour ces raisons, il est recommandé d'informer les utilisateurs de l'organisation de la maintenance à venir.

Les étapes suivantes sont requises pour la migration des stockages de sauvegarde vers un nouvel emplacement. Pour faciliter l'accès à la fois au serveur de gestion et à l'interface du service de sauvegarde, nous vous recommandons d'effectuer ces étapes sur le serveur de gestion.

Désactivation de l'accès utilisateur au service

1. Connectez-vous au service et cliquez sur l'onglet **Organisations**.
2. Sélectionnez l'organisation pour laquelle vous souhaitez changer de stockage de sauvegarde, puis cliquez sur **Configurer**.
3. Dans l'onglet **Priv. d'util.**, décochez la case **Connex. au service de sauv..** Cliquez sur **OK** pour confirmer les modifications.

Cela empêchera les utilisateurs de l'organisation d'employer le service de sauvegarde lorsque vous changerez de stockage de sauvegarde. (Les utilisateurs actuellement connectés le resteront jusqu'à ce qu'ils se déconnectent ou que leur session vCloud expire.)

4. Répétez les étapes 2 et 3 pour chaque organisation dont vous voulez changer le stockage de sauvegarde.

Désactivation des plans de sauvegarde

1. Connectez la console au serveur de gestion (p. 18).
2. Cliquez sur **Plans et tâches de sauvegarde**.
3. Désactivez tous les plans de sauvegarde qui sont appliqués aux machines virtuelles de l'organisation en sélectionnant chaque plan de sauvegarde, puis en cliquant sur **Désactiver**.

Conseil. Le nom d'un plan de sauvegarde commence par le nom de l'organisation. Vous pouvez filtrer les plans de sauvegarde en saisissant leurs noms dans le champ sous l'en-tête de la colonne **Nom**.

Le serveur de gestion nomme les plans de sauvegarde en utilisant le modèle suivant :

*%OrgName%_%BackupPlanOwner%_%BackupPlanName%, dans lequel %OrgName% est le nom de l'organisation, %BackupPlanOwner% est le nom du propriétaire du plan de sauvegarde tel qu'il figure dans l'interface Acronis Backup Advanced for vCloud, et %BackupPlanName% est le nom du plan de sauvegarde tel qu'il figure dans l'interface Acronis Backup Advanced for vCloud. Par exemple, **MonOrg_UtilOrg_Journ.***

4. Répétez les étapes 2 et 3 pour chaque organisation dont vous voulez changer le stockage de sauvegarde.
5. Si des plans de sauvegarde désactivés sont en cours d'exécution, attendez qu'ils s'arrêtent tous.
Conseil. Vous pouvez inspecter l'**état d'exécution** du plan de sauvegarde pour vérifier si celui-ci est actuellement en cours d'exécution.

Déplacement des sauvegardes

1. Déplacez le stockage de sauvegarde d'une organisation vers le nouveau périphérique de stockage.
Important. Tous les dossiers et les fichiers du stockage de sauvegarde doivent être déplacés. Cette opération peut durer un certain temps.
2. Répétez l'étape 1 pour chaque organisation dont vous souhaitez changer le stockage de sauvegarde.

Modification du stockage de sauvegarde

1. Connectez-vous au service (si vous êtes déconnecté) et cliquez sur l'onglet **Organisations**.
2. Sélectionnez l'organisation pour laquelle vous souhaitez changer de stockage de sauvegarde, puis cliquez sur **Configurer**.

3. Dans **Stock. de sauv.**, spécifiez le chemin d'accès du nouveau stockage de sauvegarde. Si l'authentification est requise pour accéder au dossier, indiquez les accréditations d'un compte d'utilisateur possédant des autorisations de lecture/écriture pour ce dossier.
4. Répétez les étapes 2 et 3 pour chaque organisation dont vous voulez changer le stockage de sauvegarde.

Activation des plans de sauvegarde

1. Connectez la console au serveur de gestion (p. 18) (si elle n'est pas connectée).
2. Cliquez sur **Plans et tâches de sauvegarde**.
3. Activez les plans de sauvegarde précédemment désactivés en sélectionnant chaque plan de sauvegarde puis en cliquant sur **Désactiver**.

Activation de l'accès utilisateur au service

1. Connectez-vous au service (si vous êtes déconnecté) et cliquez sur l'onglet **Organisations**.
2. Sélectionnez l'organisation pour laquelle le stockage de sauvegarde a été changé, puis cliquez sur **Configurer**.
3. Dans l'onglet **Priv. d'util.**, cochez la case **Connex. au service de sauv.**. Cliquez sur **OK** pour confirmer les modifications.
4. Répétez les étapes 2 et 3 pour chaque organisation dont le stockage de sauvegarde a été changé.

1.10.4 Intégration avec les systèmes tiers

Le service de sauvegarde peut être intégré avec des systèmes tiers, tels que les outils d'automatisation ou les portails de gestion à l'aide de Acronis Backup l'API Agent pour vCloud. Le guide de référence des API est disponible sur demande.

1.11 Sécurité et personnalisation

Cette section explique comment modifier les certificats de sécurité utilisés par le service et comment personnaliser l'interface utilisateur.

1.11.1 Modification du certificat SSL

L'agent pour vCloud utilise un certificat SSL (Secure Socket Layer) pour assurer le chiffrement pour l'interface Web. Par défaut, l'agent utilise un certificat auto-signé identique à l'échelle du globe pour toutes les copies d'Acronis Backup Advanced for vCloud.

Avec ce certificat par défaut, les utilisateurs qui se connectent au service verront une alerte de sécurité qui ressemblera à ce qui suit :



Nous vous conseillons de remplacer le certificat par défaut par votre propre certificat avant d'utiliser pleinement le service.

Pour modifier le certificat SSL

1. Vérifiez que votre certificat est associé à un fichier .pem. Vous pouvez acheter un certificat auprès d'une autorité de certification (CA) ou en créer un en utilisant un outil tel que **openssl**.
2. Copiez le fichier .pem vers la machine sur laquelle est installé l'agent pour vCloud. Vous pouvez placer le fichier dans le dossier **/opt/keystore**.
3. Sur la machine sur laquelle est installé l'agent pour vCloud, modifiez le fichier de configuration **/etc/lighttpd/conf.d/vcda_https.conf** et indiquez le nom de fichier de votre certificat. Le fichier de configuration peut par exemple se présenter comme suit :

```
$SERVER["socket"] == ":443" {  
    ssl.pemfile = "/opt/keystore/my_certificate.pem"  
    ssl.engine = "enable"  
}
```

Selon votre type de certificat, vous devrez peut-être indiquer d'autres paramètres dans le fichier de configuration. Pour plus de détails sur la spécification des certificats SSL, consultez l'article Lighttpd Wiki suivant : http://redmine.lighttpd.net/projects/1/wiki/Docs_SSL.

4. Redémarrez le serveur Web en exécutant la commande suivante :

```
service lighttpd restart
```

1.11.2 Modification du logo et personnalisation de l'interface

L'apparence d'une interface Web repose sur les fichiers .ccs (Cascading Style Sheets). Vous pouvez personnaliser l'interface en modifiant le fichier **custom.css**. Par exemple, vous pouvez modifier le logo ou les couleurs de l'arrière-plan, du texte et des boutons.

Cette section décrit la méthode permettant de remplacer le logo Acronis par celui de votre société.

Exigences relatives aux fichiers de logo

Emplacement	Format	Taille recommandée
Page de connexion	PNG, JPG ou GIF	160 px x 72 px
Interface principale	PNG, JPG ou GIF	160 px x 72 px
Onglet de navigateur (icône favorite)	ICO	16 px x 16 px

Pour modifier le logo

1. Préparez les fichiers de logo en fonction des exigences indiquées ci-dessus.
2. Copiez le(s) fichier(s) de logo vers la machine possédant l'agent pour vCloud.
3. Sur la machine sur laquelle est installé l'agent pour vCloud, modifiez le fichier **/opt/acronis/vcd-agent/client/custom/custom.css** comme suit :

- a. Les sélecteurs de classe **.login-header-logo** et **.header-logo** définissent respectivement le logo sur la page de connexion et sur l'interface principale. Remplacez les chemins d'accès des fichiers de logo dans la propriété d'**arrière-plan** par les nouveaux chemins d'accès.

```
/* Logos */
.header .header-logo {
    background: url("../resources/images/logo_main_interface.png") no-repeat -29px -12px;
    margin-left: 0;
    margin-top: 0;
    width: 123px;
    height: 43px;
}
.login-header-logo {
    background: url("../resources/images/logo_login_page.png") no-repeat 0px -12px;
    margin-left: -26px;
    margin-top: 0;
    width: 154px;
    height: 43px;
}
```

- b. Si la taille d'un logo diffère des valeurs recommandées, effectuez l'une des actions suivantes :
- Ajustez sa position en modifiant les valeurs des propriétés d'**arrière-plan**.
 - Ajustez sa position et la taille du conteneur qui stocke le logo (en modifiant les propriétés de **largeur**, **hauteur**, **marge gauche**, et de **marge du haut**) dans les sélecteurs de classe correspondants.
- c. Si nécessaire, vous pouvez aligner le nom du produit et le logo en modifiant les valeurs des propriétés de **marge du haut** et de **remplissage à gauche** dans le sélecteur de classe **.header-product-name**. Pour déplacer le nom du produit encore plus à droite, créez un sélecteur de classe **.login-header-text.prefix_2** avec la propriété de **remplissage à gauche**.
- d. Enregistrez le fichier.
4. Pour modifier l'image affichée dans l'onglet de navigateur, remplacez le fichier **/opt/acronis/vcd-agent/client/favicon.ico** par le nouveau fichier.

Il n'est pas nécessaire de redémarrer le serveur Web pour que les modifications prennent effet. Pour visualiser les modifications dans les pages Web actuellement ouvertes, appuyez sur CTRL+F5 dans le navigateur (ou effacez le cache du navigateur).

2 Guide de l'utilisateur

2.1 À propos du service de sauvegarde

Ce service permet la sauvegarde et la restauration de machines virtuelles gérées par VMware vCloud Director.

Il est disponible par le biais d'une interface Web. Pour vous connecter au service de sauvegarde, utilisez vos accréditations vCloud Director.

Les opérations que vous pouvez effectuer après connexion dépendent des paramètres configurés par un administrateur système pour votre organisation. En fonction de ces paramètres, certaines des opérations décrites dans ce guide risquent de ne pas être disponibles.

2.2 Navigateurs Web pris en charge

- Google Chrome 12 ou plus récent
- Mozilla Firefox 12 ou plus récent
- Windows Internet Explorer 9 ou plus récent
- Safari 5 ou plus récent s'exécutant sur les systèmes d'exploitation Mac OS X et iOS

Les autres navigateurs (dont les navigateurs Safari s'exécutant sur d'autres systèmes d'exploitation) peuvent ne pas afficher correctement l'interface utilisateur ou ne pas proposer l'ensemble des fonctions disponibles.

JavaScript doit être activé dans le navigateur.

Pour afficher l'interface graphique, la résolution de l'écran doit être au minimum de 1 024x768.

2.3 Installation de VMware Tools

Nous recommandons d'installer VMware Tools sur toutes les machines virtuelles en cours d'exécution que vous prévoyez de sauvegarder.

L'installation de VMware Tools est une exigence commune pour la sauvegarde au niveau hyperviseur. Le service de sauvegarde utilise VMware Tools pour créer une sauvegarde temporelle cohérente de la machine. Toutes les données seront sauvegardées dans l'état dans lequel elles se trouvaient lorsque la sauvegarde a démarré, même si elles ont été modifiées pendant la sauvegarde.

Pour installer VMware Tools sur une machine virtuelle

1. Connectez-vous à vCloud Director.
2. Dans la liste des machines virtuelles, contrôlez la colonne **VMware Tools** correspondant à votre machine virtuelle. Cette colonne est masquée par défaut.
3. Si elle indique **Non installé**, installez la version la plus récente comme suit :
 - a. Démarrez la machine.
 - b. Cliquez avec le bouton droit de la souris sur la machine, puis cliquez sur **Installer VMware Tools**.
 - c. Suivez les instructions affichées à l'écran.

Pour obtenir des informations sur l'installation de VMware Tools sur un système d'exploitation spécifique, veuillez consulter l'article suivant de la base de connaissances VMware : http://pubs.vmware.com/vcd-51/topic/com.vmware.vcloud.users.doc_51/GUID-F0826E73-7F9F-489C-B0DB-17C7D742B1AF.html.

2.4 Opérations de base

Cette section décrit l'utilisation courante du service de sauvegarde.

2.4.1 Connexion au service

Vous pouvez vous connecter au service de sauvegarde dans les conditions suivantes :

- Un administrateur système a autorisé l'utilisation du service pour votre organisation.
- [Pour les utilisateurs non-administrateurs] L'administrateur de votre organisation a autorisé l'utilisation du service pour votre compte.

Pour vous connecter au service de sauvegarde

1. Accédez à la page de connexion du service de sauvegarde. L'URL de la page de connexion se présente ainsi : **<https://backup.example.com/org/<nom de l'organisation>>**
En cas de doute sur l'adresse de la page de connexion, contactez l'administrateur système ou l'administrateur de l'organisation.
2. Saisissez le nom d'utilisateur et le mot de passe de votre compte vCloud Director.
3. Cliquez sur **Connex..**

2.4.2 Sauvegarde des machines virtuelles

Les machines virtuelles que vous pouvez sauvegarder sont répertoriées dans l'onglet Organisation.

Orga2_Cluster02 Stock. de sauv. Plans de sauv. Param. Journaux

Toutes les MV

vApps

- vApp1
- vApp_Sally
- vApp_without network

	Nom	Nom vApp	Dernière sauv.	État de protection
<input type="checkbox"/>	VM1	vApp1	27/09/2013 05:09	Non protégé
<input type="checkbox"/>	VM1-1	vApp1		Non protégé
<input type="checkbox"/>	VM2	vApp1		Non protégé
<input type="checkbox"/>	XPP3_ENU	vApp_without network	27/09/2013 04:34	Non protégé

La liste **vApps** répertorie toutes les vApps qui vous appartiennent. La liste **Toutes les MV** répertorie toutes les machines virtuelles pour ces vApps. (Un administrateur d'organisation voit toutes les vApps et machines virtuelles de l'organisation.)

Démarrage d'une sauvegarde

Sélectionnez une ou plusieurs machines virtuelles que vous souhaitez sauvegarder, puis cliquez sur **Sauv. maint.**

Orga2_Cluster02 [Stock. de sauv.](#) [Plans de sauv.](#) [Param.](#) [Journaux](#)

Toutes les MV

vApps

- vApp1
- vApp_Sally
- vApp_without network

Appli. plan sauv. **Sauv. maint.** Restaurer Retirer plan de sauv. Rafraîchir

	Nom	Nom vApp	Dernière sauv.	État de protection	Plan de sauv.
<input type="checkbox"/>	VM1	vApp1		⊙ Non protégé	
<input type="checkbox"/>	VM1-1	vApp1		⊙ Non protégé	
<input type="checkbox"/>	VM1-11	vApp1		⊙ Non protégé	
<input type="checkbox"/>	VM2	vApp1		⊙ Non protégé	
<input checked="" type="checkbox"/>	XPP3_ENU	vApp_without network	27/09/2013 04:34	⊙ Non protégé	

Détails machine

XPP3_ENU

Nom de l'ordi. -

SE Microsoft Windows XP Professional (32-bit)

Adresses IP -

Adresses IP externes -

Si vous souhaitez planifier l'exécution des sauvegardes, appliquez plutôt un plan de sauvegarde (p. 47).

Surveillance d'une sauvegarde

Le démarrage d'une sauvegarde peut être différé, selon la charge du service de sauvegarde.

Lorsque la sauvegarde démarre, sa progression s'affiche à droite, dans la zone de détails de la machine.

Orga2_Cluster02 [Stock. de sauv.](#) [Plans de sauv.](#) [Param.](#) [Journaux](#)

Toutes les MV

vApps

- vApp1
- vApp_Sally
- vApp_without network

Appli. plan sauv. **Arrêter sauv.** Restaurer Retirer plan de sauv. Rafraîchir

	Nom	Nom vApp	Dernière sauv.	État de protection	Plan de sauv.
<input checked="" type="checkbox"/>	VM1	vApp1		Sauvegarde...	
<input type="checkbox"/>	XPP3_ENU	vApp_without network	27/09/2013 04:34	⊙ Non protégé	
<input type="checkbox"/>	XPP3_ENU	vApp_Sally		⊙ Non protégé	

Détails machine

VM1

Sauvegarde... 63 % terminé...

Nom de l'ordi. -

Le service de sauvegarde définit le nombre de machines qui sont sauvegardées simultanément et l'ordre dans lequel elles sont sauvegardées.

Si vous devez arrêter la sauvegarde sur une machine en particulier, sélectionnez la machine, puis cliquez sur **Arrêter sauv.** ou cliquez sur le bouton Arrêter (■) à côté de la barre de progression.

Affichage du résultat

Une fois qu'une machine virtuelle est sauvegardée avec succès, la sauvegarde nouvellement créée s'affiche dans la colonne **Sauvegardes** sous l'onglet **Stock. de sauv.**

MyOrganization [Stock. de sauv.](#) [Plans de sauv.](#) [Param.](#) [Journaux](#)

Restaurer Restaurer fich. Suppr. Rafraîchir

	Nom machine	Nom vApp	Utilis. stock.	Données sauv.
<input checked="" type="checkbox"/>	VM1	vApp2	854 Ko	45,1 Mo

Détails machine

VM1

Sauv.

25/07/2014 07:48

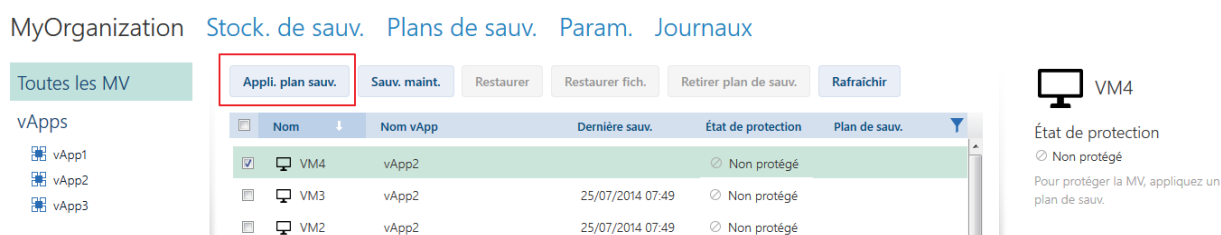
2.4.3 Application d'un plan de sauvegarde

L'application d'un plan de sauvegarde à une machine virtuelle vous permet d'automatiser la création et la suppression des sauvegardes de la machine.

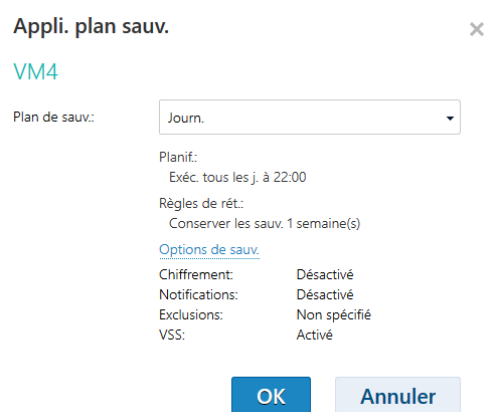
Selon la façon dont le service de sauvegarde est configuré, vous pouvez créer vos propres plans de sauvegarde ou appliquer des plans de sauvegarde partagés par l'administrateur système, voire effectuer ces deux opérations.

Pour appliquer un plan de sauvegarde à des machines virtuelles

1. Sélectionnez une ou plusieurs machines virtuelles dans la liste **Toutes les MV**, ou sélectionnez une vApp entière dans la liste **vApps**. Si vous sélectionnez une vApp entière, le plan de sauvegarde sera appliqué à toutes les machines figurant dans celle-ci, ainsi qu'à toute nouvelle machine qui y apparaîtra ultérieurement.
2. Cliquez sur **Appli. plan sauv.**.



3. Sélectionnez le plan de sauvegarde que vous désirez appliquer aux machines. Par exemple, sélectionnez **Journ.**.



Un plan de sauvegarde contient les instructions suivantes pour le service de sauvegarde :

- **Planification** : conditions et fréquence d'exécution des sauvegardes.
- **Règles de rétention** : durée de stockage des sauvegardes.
- **Options de sauv.** (p. 57).

4. Cliquez sur **OK**.

Le nom du plan de sauvegarde appliqué figure dans la colonne **Plan de sauvegarde**. Si un autre plan de sauvegarde a déjà été appliqué à la machine, il est retiré.

Conseils d'utilisation

- La colonne **État de protection** indique si la dernière sauvegarde a été réalisée avec succès (**OK**) ou si elle a échoué (**Erreur**).
- Si vous avez besoin de redémarrer une sauvegarde ayant échoué, sélectionnez une machine et cliquez sur **Sauv. maint.**. La machine sera sauvegardée conformément aux paramètres du plan de sauvegarde. Cependant, les règles de rétention ne s'appliqueront pas cette fois-ci.
- Uniquement si cela est vraiment nécessaire, remplacez un plan de sauvegarde par un autre dont le paramètre **Chiffrement** est différent (avec un mot de passe différent). Cette opération est autorisée mais peut causer certains désagréments. Pour plus de détails, veuillez vous référer à

« Conséquences du changement du chiffrement » dans « Modification d'un plan de sauvegarde » (p. 59).

2.4.4 Écrasement d'une machine virtuelle avec sa version sauvegardée

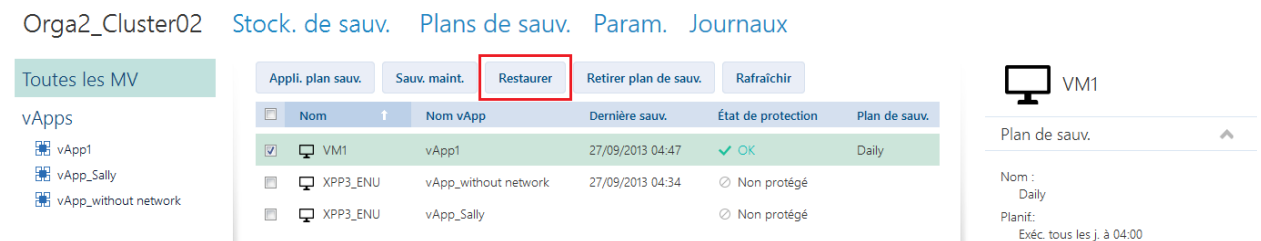
Cette procédure de restauration est facilement exécutable dans l'onglet de l'organisation.

En cas d'écrasement d'une machine, seul le contenu de ses disques d'origine est remplacé. Le contenu des disques durs ajoutés suite à la sauvegarde reste tel quel. Les paramètres de la machine (CPU, mémoire, etc.) et les adresses MAC des adaptateurs réseau, aussi appelées adresses physiques, sont également conservés.

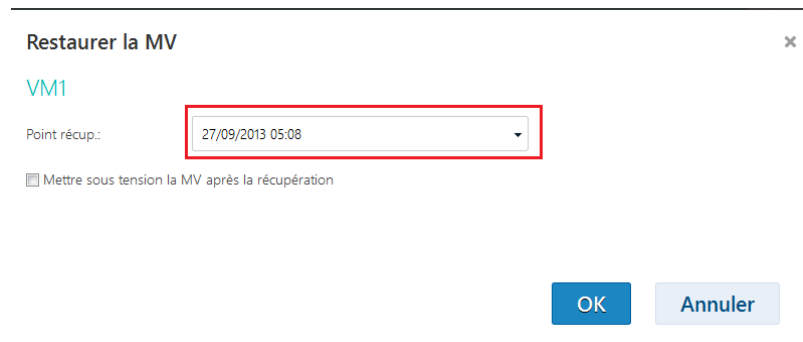
Une machine qui a été renommée ou déplacée vers une vApp différente est considérée comme nouvelle. Pour l'écraser, vous avez besoin d'une sauvegarde qui a été créée après le renommage ou le déplacement de la machine. Si vous avez besoin d'utiliser une sauvegarde plus ancienne, procédez comme décrit dans « Restauration d'une machine virtuelle » (p. 50).

Paramétrage de la restauration

1. Dans l'onglet Organisation, sélectionnez la machine à restaurer, puis cliquez sur **Restaurer**.



2. Dans **Point de récupération**, sélectionnez la date et l'heure à laquelle la machine sera restaurée. Par défaut, le dernier point de récupération sera sélectionné.



Si un ou plusieurs réseaux préalablement utilisés par la machine sauvegardée ne font plus partie de la vApp, il vous est demandé de mapper les adaptateurs réseau de la machine virtuelle aux réseaux de la vApp.

3. [Option] Activez la case **Mettre sous tension la MV après la restauration**.
4. Cliquez sur **OK**.

Surveillance de la restauration

Une fois la restauration lancée, la machine présente l'état de protection **Restauration**. La progression de la restauration s'affiche dans la zone de détails de la machine, à droite.

Orga2_Cluster02 Stock. de sauv. Plans de sauv. Param. Journaux

Toutes les MV

vApps

- vApp1
- vApp_Sally
- vApp_without network

	Nom	Nom vApp	Dernière sauv.	État de protection	Plan de sauv.
<input checked="" type="checkbox"/>	VM1	vApp1	27/09/2013 05:09	Restauration...	Daily
<input type="checkbox"/>	VM2	vApp1		Non protégé	
<input type="checkbox"/>	XPP3_ENU	vApp_without netwo...	27/09/2013 04:34	Non protégé	

VM1

Restauration... 2 % terminé...

Plan de sauv.

Nom :

Pour interrompre la restauration, cliquer sur le bouton **Arrêt. restaur.** ou sur le bouton d'arrêt (■) placé à proximité de la barre de progression. La machine d'origine risque d'être corrompue.

Une fois la restauration terminée, les informations concernant sa réussite ou son échec s'affichent dans la zone de détails de la machine.

2.4.5 Restauration d'une machine virtuelle

Il s'agit d'une procédure de restauration ordinaire. Contrairement à l'écrasement d'une machine virtuelle existante, elle vous permet de restaurer une machine virtuelle supprimée, de créer une nouvelle machine virtuelle en la restaurant à partir d'une sauvegarde, ainsi que de modifier les paramètres réseau de la machine.

Paramétrage de la restauration

1. Ouvrez l'onglet **Stock. de sauv.**.

MyOrganization Stock. de sauv. Plans de sauv. Param. Journaux

Restaurer Restaurer fich. Suppr. Rafraîchir

	Nom machine	Nom vApp	Utilis. stock.	Données sauv.
<input checked="" type="checkbox"/>	VM1	vApp2	854 Ko	45,1 Mo

VM1

Sauv.

25/07/2014 07:48

2. Dans la liste des machines sauvegardées, sélectionnez la machine à restaurer, puis cliquez sur **Restaurer**.

Restaurer la MV

VM1

Point récup.: 27/09/2013 03:52

vApp cible: vApp1

Nom de la machine restaurée: VM1-2

☐ Afficher les paramètres suppl.

☐ Mettre sous tension la MV après la récupération

OK Annuler

3. Dans **Point de récupération**, sélectionnez la date et l'heure à laquelle la machine sera restaurée. Par défaut, le dernier point de récupération est sélectionné.
4. Dans **vApp cible**, indiquez la vApp dans laquelle sera restaurée la machine. Par défaut, la vApp d'origine est sélectionnée.

Si la vApp d'origine n'existe plus dans l'organisation, vous pouvez la recréer et restaurer la machine dans celle-ci. Pour cela, sélectionnez **Recréer la vApp d'origine**. La vApp est créée avec les paramètres qui lui étaient associés lorsque la machine a été sauvegardée.

5. Dans **Nom de la machine restaurée**, saisissez le nom qui sera attribué à la machine restaurée dans la vApp. Par défaut, le nom d'origine de la machine est sélectionné.

Si une machine existe déjà sous ce nom dans cette vApp, le logiciel contrôle l'identifiant unique de la machine dans vCloud Director. Toute machine possédant le même identifiant unique sera écrasée. Si la machine possède un identifiant unique différent, le logiciel crée une nouvelle machine virtuelle et ajoute un suffixe de type **(1)** à son nom.

6. Dans **Afficher les paramètres suppl.**, les actions suivantes sont disponibles :

[Masquer les paramètres suppl.](#)

Nom de l'ordi.:

Adaptateurs réseau

Les paramètres d'adaptateur réseau des MV sont introuvables dans la sauvegarde.

NIC	Connecté	Réseau	NIC princ.	Mode IP	Adresse IP
0	<input checked="" type="checkbox"/>	VM Network	<input checked="" type="radio"/>	DHCP	Obtenir du serveur D...

[+ Ajouter carte réseau](#)

☐ Mettre sous tension la MV après la récupération

- Dans **Nom de l'ordi.**, modifier ou spécifier le nom de la machine sur le réseau. Il s'agit du nom défini dans le système d'exploitation invité (**Panneau de configuration > Système > Propriétés système > Nom de l'ordinateur**).
- Dans **Adaptateurs réseau**, modifiez ou indiquez les paramètres des adaptateurs existants, ou ajoutez ou supprimez des adaptateurs réseau.
Détails. Pour ajouter un adaptateur réseau, cliquez sur **Ajouter carte réseau**, et précisez ses paramètres. Pour supprimer un adaptateur réseau, cliquez sur le bouton **Supprimer** () qui lui est associé.
- Dans **Conserver les adresses MAC**, indiquez si les adaptateurs réseau de la machine (à l'exception de ceux que vous venez d'ajouter) posséderont les mêmes adresses MAC que ceux de la machine d'origine. Pour prévenir tout conflit d'adresses MAC, n'activez pas cette case si la machine d'origine existe et ne sera pas écrasée.

7. [Option] Activez la case **Mettre sous tension la MV après la restauration**.

8. Cliquez sur **OK**.

Surveillance de la restauration

La progression de la restauration s'affiche dans la zone de détails de la machine, à droite.

MyOrganization Stock. de sauv. Plans de sauv. Param. Journaux

Arrêt. récup. Suppr. Rafraichir

<input type="checkbox"/>	Nom machine	Nom vApp	Utilis. stock.	Données sauv.
<input checked="" type="checkbox"/>	VM1	vApp2	854 Ko	45,1 Mo

VM1

Restauration... 58% terminé...

Sauv.

23/07/2014 22:20

Pour interrompre la restauration, cliquer sur le bouton **Arrêt. restaur.** ou sur le bouton d'arrêt () placé à proximité de la barre de progression.

Une fois la restauration terminée, les informations concernant sa réussite ou son échec s'affichent dans la zone de détails de la machine.

2.4.6 Restauration de fichiers à partir d'une sauvegarde de machine virtuelle

Cette procédure vous permet de restaurer des fichiers et dossiers à partir de la sauvegarde d'une machine virtuelle, mais sans restaurer la machine virtuelle elle-même.

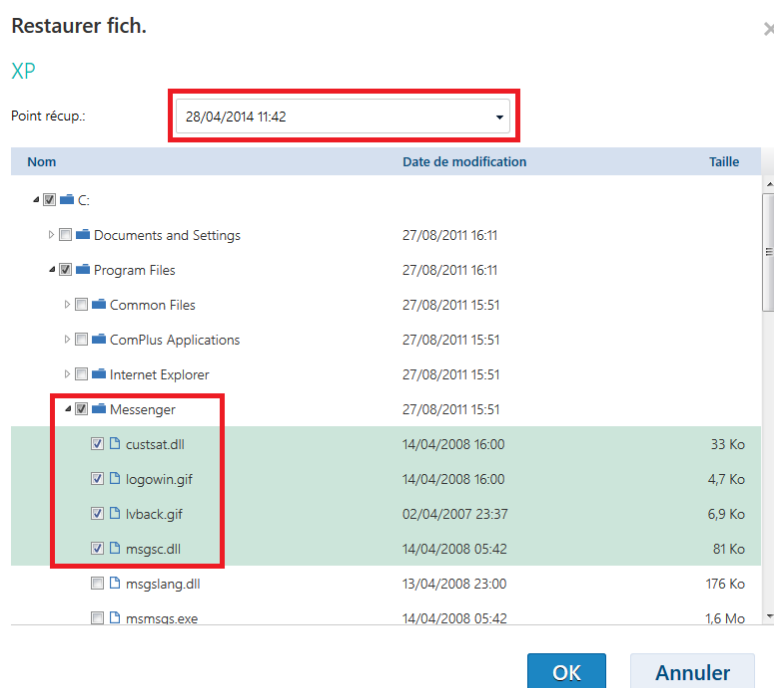
Les fichiers et dossiers que vous sélectionnez peuvent être téléchargés sous la forme d'un fichier .zip.

Vous pouvez restaurer des fichiers à partir de volumes associés aux systèmes de fichiers suivants : FAT, FAT32, NTFS, Ext2, Ext3 et Ext4. Indépendamment du système de fichiers, vous ne pouvez pas restaurer de fichiers à partir de volumes gérés par le gestionnaire de volumes logiques Linux (LVM), également appelés volumes logiques, ni à partir de périphériques MD (à disques multiples), également appelés RAID logiciels Linux.

Pour restaurer les fichiers d'une machine virtuelle

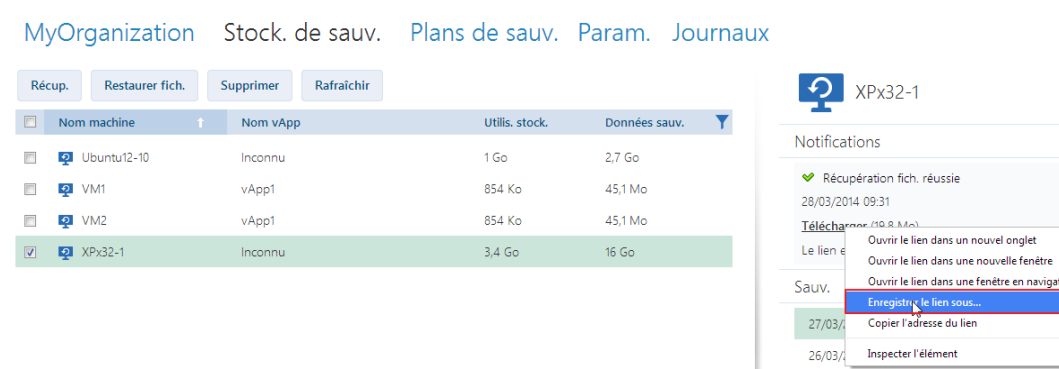
1. Ouvrez l'onglet de l'organisation ou l'onglet **Stockage de sauvegarde**.
2. Sélectionnez la machine virtuelle dont vous souhaitez restaurer les fichiers, puis cliquez sur **Restaurer fich..**
3. Dans **Point récup.**, sélectionnez la date et l'heure de la restauration des fichiers.

Le service montre les volumes, fichiers et dossiers qui étaient présents sur la machine à ce moment. Les volumes à partir desquels vous ne pouvez pas restaurer les fichiers ne s'affichent pas.



Sélectionnez les fichiers et dossiers que vous souhaitez restaurer, puis cliquez sur **OK**.

Lorsque la restauration est terminée, le lien de téléchargement du fichier .zip s'affiche dans l'onglet **Stockage de sauvegarde** de la zone de détails de la machine, sur la droite.



Ce lien est valide 24 heures. Vous ne pouvez utiliser ce lien que lorsque vous êtes connecté au service.

Les fichiers sont stockés dans le fichier .zip avec leur structure de dossier complète. Le fichier **C:\Documents\Report.doc** sera par exemple stocké dans le fichier .zip au sein du dossier **Drive(C)\Documents**.

Restauration de fichiers vers la machine d'origine

Pour restaurer les fichiers directement vers la machine virtuelle d'origine, respectez l'une des méthodes suivantes :

- **Extraction des fichiers sur un partage réseau système.** Une fois le fichier .zip téléchargé vers votre machine, mettez la machine virtuelle d'origine sous tension et extrayez le fichier vers un partage réseau tel que **\\VM1\c\$** (ce partage réseau correspond au volume C de la machine virtuelle **VM1**). Cette méthode de restauration ne fonctionne que pour une machine virtuelle exécutant Windows. Vous devez, sur cette machine virtuelle, fournir les accréditations d'un administrateur local.
- **Connectez-vous au service sur la machine virtuelle.** Démarrez la machine virtuelle, lancez le navigateur, connectez-vous au service, puis téléchargez le fichier .zip et extrayez les fichiers.

2.4.7 Surveillance des états de protection

La colonne **État de protection** de l'onglet de l'organisation indique si une machine virtuelle ou une vApp est bien protégée.

États de protection des machines

Le tableau ci-dessous indique les états de protection d'une machine par ordre croissant de *gravité*.

État	Signification
Non protégé	Aucun plan de sauvegarde n'est appliqué à la machine.
Jamais sauvegardé	Un plan de sauvegarde est appliqué à la machine, mais aucune sauvegarde n'a été effectuée.
OK	Un plan de sauvegarde est appliqué à la machine et la dernière sauvegarde a été réalisée avec succès.
Erreur	Un plan de sauvegarde est appliqué à la machine, mais la dernière sauvegarde a échoué.

Les états **Sauvegarde...** ou **Restauration...** s'affichent lorsqu'une opération de sauvegarde ou de récupération est en cours d'exécution.

Remarque L'opération Sauvegarder maintenant n'affecte l'état de protection que si un plan de sauvegarde est appliqué à la machine.

États de protection des vApps

L'état de protection d'une vApp est déterminé par l'état *le plus grave* parmi les machines de la vApp. Il ne dépend pas du fait qu'une sauvegarde ou une restauration soit en cours sur une machine.

2.5 Opérations avec des sauvegardes

L'onglet **Stock. de sauv.** affiche la liste des machines virtuelles sauvegardées. Chaque machine possède une ou plusieurs sauvegardes, également appelées points de récupération. Les sauvegardes sont répertoriées dans la zone **Sauvegardes** à droite.

Une fois que vous avez sélectionné une sauvegarde, la zone **Détails machine** affiche le nom de l'ordinateur, le système d'exploitation invité et les adresses IP de la machine *au moment de la sauvegarde*.

Il est possible d'effectuer les opérations suivantes avec les sauvegardes :

- **Pour restaurer une machine à partir d'une sauvegarde**, sélectionnez la machine et cliquez sur **Restaurer**. Veuillez vous référer à « Restauration d'une machine virtuelle » (p. 50).
- **Pour supprimer une ou plusieurs sauvegardes d'une machine**, sélectionnez la machine et cliquez sur **Supprimer**. Dans la fenêtre ouverte, sélectionnez les sauvegardes que vous désirez supprimer, puis cliquez sur **Supprimer**.
- **Pour supprimer toutes les sauvegardes de plusieurs machines**, sélectionnez les machines et cliquez sur **Supprimer**.

Utilis. stock./Total des données sauvegardées

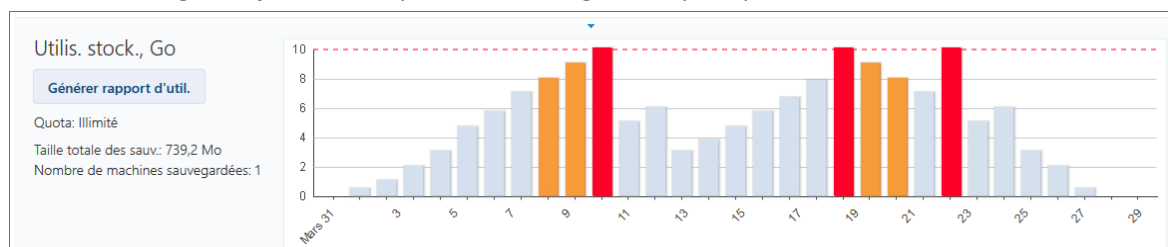
Cette zone contient des informations relatives à l'utilisation du stockage ou aux données sauvegardées, selon les paramètres de quota du service de sauvegarde (p. 33).

Cette zone est disponible uniquement pour les administrateurs. Elle contient les paramètres suivants :

- Le quota de stockage pour l'organisation (s'il est défini par l'administrateur système).
- La taille totale des sauvegardes stockées dans le stockage de sauvegarde ou la quantité totale de données sauvegardées.
- Le nombre de machines virtuelles sauvegardées.
- Les alertes concernant un quota quasiment atteint (80 % ou plus) ou un quota dépassé (100 % ou plus).

Pour afficher les données d'historique de l'utilisation du stockage, développez cette zone.

- Le graphique en colonnes représente l'utilisation du service au cours des 30 derniers jours. Dans le graphique, les colonnes rouges affichent les jours où le quota de stockage a été dépassé et les colonnes orange, les jours où le quota de stockage a été presque atteint.



- Pour générer un rapport exhaustif sur l'utilisation du stockage pour une période spécifique, cliquez sur **Générer rapport d'util.** (p. 60).

2.6 Opérations avec les plans de sauvegarde

L'onglet **Plans de sauv.** affiche les plans de sauvegarde que vous pouvez appliquer à vos machines virtuelles.

Les plans de sauvegarde suivants sont répertoriés :

- **Plans de sauvegarde système** (🔧). Ils sont partagés par l'administrateur système avec votre organisation. Leurs règles de rétention et de planification ne peuvent être modifiées qu'à l'aide de l'interface de l'administrateur système. Cependant, vous pouvez activer des options de sauvegarde pour ces plans, telles que le chiffrement ou les notifications. Pour ce faire, cliquez sur **Définir des options**. Ces options ne sont effectives qu'au sein de votre organisation.
- **Plans de sauvegarde créés au sein de l'organisation** (👤). Si vous êtes un administrateur de l'organisation, vous pouvez effectuer toutes les opérations que vous souhaitez avec ces plans de sauvegarde. Les utilisateurs non-administrateurs ont accès à l'ensemble des opérations pour les plans de sauvegarde qu'ils ont créés. La colonne **Prop.** affiche le créateur du plan de sauvegarde. Le propriétaire des plans de sauvegarde créés par un administrateur système est **Système**.

2.6.1 Création d'un plan de sauvegarde

Vous pouvez non seulement utiliser les plans de sauvegarde existants mais aussi créer vos propres plans de sauvegarde.

Pour créer un plan de sauvegarde

1. Ouvrez l'onglet **Plans de sauv.**.
2. Cliquez sur **Créer**.
3. Saisissez le nom du plan de sauvegarde. Le nom doit être différent des noms des autres plans de sauvegarde répertoriés dans la liste.
4. Indiquez le type de planification : **Journ.**, **Hebdo.**, **GFS (Grand-père/père/fils)** ou **Par heure**.
5. Dans les onglets **Planification** et **Règles de rétention**, indiquez les paramètres de planification et de règles de rétention (p. 55) pour le plan de sauvegarde.
6. Dans l'onglet **Options**, indiquez les options de sauvegarde (p. 57).
7. Cliquez sur **OK**.

Après avoir créé le plan de sauvegarde, vous pouvez l'appliquer à vos machines virtuelles (p. 47).

2.6.1.1 Planification et règles de rétention

L'opération de sauvegarde s'exécute selon la planification que vous avez spécifiée. Les sauvegardes correspondantes sont conservées et supprimées conformément aux règles de rétention.

L'horaire planifié correspond au fuseau horaire défini sur la machine vous connectant au service de sauvegarde. Par exemple, si vous planifiez vos sauvegardes à 07:00, elles s'exécuteront lorsque l'horloge de votre machine atteindra 07:00, quel que soit le fuseau horaire où est située l'infrastructure vCloud physique. Toute modification des paramètres de fuseau horaire de votre machine aura un impact sur l'heure de démarrage mais pas sur la planification elle-même.

Les types de planification et les règles de rétention suivants sont disponibles :

Sauvegarde par heure

Planification. Sélectionnez les jours de la semaine pendant lesquels exécuter des sauvegardes, ainsi que l'intervalle de temps entre chaque sauvegarde. Dans les champs **De** et **À**, spécifiez le début et la fin de la période d'exécution des sauvegardes.

Règles de rétention. Spécifiez la durée de conservation des sauvegardes.

Les sauvegardes auront lieu par défaut toutes les quatre heures pendant les jours ouvrables. Les sauvegardes sont conservées pendant une semaine.

Sauvegarde journalière

Planification. Sélectionnez l'heure et les jours de la semaine pour l'exécution des sauvegardes.

Règles de rétention. Spécifiez la durée de conservation des sauvegardes.

Par défaut, les sauvegardes seront exécutées du lundi au vendredi à 22:00. Les sauvegardes créées seront conservées pendant une semaine.

Sauvegarde hebdomadaire

Cette planification permet d'exécuter les sauvegardes à une fréquence définie en nombre de semaines.

Planification

1. Sélectionnez le nombre de semaines.
2. Sélectionnez l'heure et le jour de la semaine d'exécution des sauvegardes.

Par défaut, les sauvegardes seront exécutées toutes les semaines à 22:00, le jour de la semaine où le plan de sauvegarde a été créé.

Règles de rétention

Spécifiez la durée de conservation des sauvegardes.

Par défaut, les sauvegardes seront conservées pendant quatre semaines.

GFS (Grand-père - père - fils)

Cette planification est utile pour le stockage à long terme des sauvegardes.

Avec cette planification, vous disposez d'une sauvegarde pour chaque jour récent et chaque semaine récente. En ce qui concerne les périodes plus anciennes, vous disposez d'une sauvegarde unique pour chaque mois.

Planification

1. Sélectionnez les jours de la semaine et l'heure auxquels les sauvegardes sont exécutées.
2. Parmi ces jours de la semaine, choisissez celui où vous allez **Effectuer des sauv. hebdo. et mens. le**. Les sauvegardes réalisées ce jour-là seront considérées comme des *sauvegardes hebdomadaires* et des *sauvegardes mensuelles*. Les sauvegardes réalisées les autres jours seront considérées comme des *sauvegardes journalières*.

Par défaut, les sauvegardes auront lieu à 22:00 du lundi au vendredi. Le vendredi est choisi pour les sauvegardes hebdomadaires/mensuelles.

Règles de rétention

Spécifiez la durée de conservation des sauvegardes journalières, hebdomadaires et mensuelles.

Les paramètres par défaut sont les suivants :

- Sauvegardes journalières : 5 jours (minimum recommandé)
- Sauvegardes hebdomadaires : 7 semaines
- Sauvegardes mensuelles : 12 mois

Exemple

Supposons que vous utilisiez les paramètres par défaut (sauvegardes journalières du lundi au vendredi, sauvegardes hebdomadaires/mensuelles le vendredi, règles de rétention par défaut), et que vous appliquiez le plan de sauvegarde le lundi 1er mars.

Le tableau suivant indique les sauvegardes journalières (J), hebdomadaires (H) et mensuelles (M) qui auront été préservées à la date du vendredi 30 avril. Les sauvegardes figurant sur un fond gris auront été supprimées une fois cette date atteinte.

	Lun	Mar	Mer	Jeu	Ven	Sam	Dim
Du 1er au 7 mars	J	J	J	J	H	–	–
Du 8 au 14 mars	J	J	J	J	H	–	–
Du 15 au 21 mars	J	J	J	J	H	–	–
Du 22 au 28 mars	J	J	J	J	M	–	–
Du 29 mars au 4 avril	J	J	J	J	H	–	–
Du 5 au 11 avril	J	J	J	J	H	–	–
Du 12 au 18 avril	J	J	J	J	H	–	–
Du 19 au 25 avril	J	J	J	J	H	–	–
Du 26 avril au 2 mai	J	J	J	J	M	–	–

2.6.1.2 Options de sauvegarde

Dans l'onglet **Options**, configurez les paramètres de l'opération de sauvegarde.

Chiffrement

Spécifiez le mot de passe à utiliser pour le chiffrement des sauvegardes. L'invite de mot de passe apparaîtra lorsque quelqu'un tentera de supprimer une sauvegarde ou de restaurer des données à partir d'une sauvegarde.

Les sauvegardes sont chiffrées à l'aide de l'algorithme de chiffrement AES-256.

Le mot de passe n'est stocké ni sur le disque ni dans le fichier de sauvegarde. Vous devez vous souvenir du mot de passe. Il est impossible de récupérer un mot de passe qui a été perdu.

Si vous modifiez le plan de sauvegarde (p. 59) et que vous modifiez ou supprimez le mot de passe, les règles de rétention ne s'appliqueront plus aux sauvegardes concernées par l'ancien paramètre de chiffrement. De plus, des enregistrements séparés seront affichés pour les jeux de sauvegarde possédant des paramètres de chiffrement différents. Durant la restauration, vous devrez sélectionner l'enregistrement approprié et indiquer le mot de passe requis.

Notifications

Indiquez si vous souhaitez qu'un courrier électronique de notification soit envoyé après une sauvegarde réussie, un échec ou les deux.

Indiquez l'adresse d'envoi des notifications. Séparez les adresses e-mail par un point-virgule. Par exemple : **utilisateur1@exemple.com; utilisateur2@exemple.com**

Les notifications seront envoyées depuis l'adresse électronique indiquée par l'administrateur système.

Exclusions

Saisissez un ou plusieurs critères. Les fichiers et dossiers correspondant à l'un des critères spécifiés ne seront pas sauvegardés.

Cette option ne s'applique qu'aux fichiers et dossiers stockés dans les systèmes de fichiers suivants :

- FAT
- NTFS
- Ext3
- Ext4

Indépendamment du système de fichiers, cette option ne s'applique pas aux volumes gérés par Linux Logical Volume Manager (LVM), également appelés volumes logiques, ni aux périphériques MD (à disques multiples), également appelés Linux Software RAID.

Comment spécifier des critères

Vous pouvez utiliser les critères suivants :

- **Le chemin d'accès complet au fichier ou dossier**, en commençant par la lettre du lecteur (lors de la sauvegarde de Windows) ou le répertoire racine (lors de la sauvegarde de Linux).
Sous Windows et Linux, vous pouvez utiliser une barre oblique dans le chemin du dossier ou du fichier (par exemple : **C:/Temp** et **C:/Temp/File.tmp**). Dans Windows, vous pouvez aussi utiliser la barre oblique inverse (par exemple : **C:\Temp** et **C:\Temp\File.tmp**).
- **Le nom d'un fichier ou d'un dossier** ; par exemple : **Document.txt**. Tous les fichiers et dossiers portant ce nom seront exclus.

Séparez les critères les uns des autres avec des points-virgules (;).

Les critères *ne sont pas* sensibles à la casse. Par exemple, si vous choisissez d'exclure tous les fichiers **.tmp** et le dossier **C:\Temp**, seront également exclus tous les fichiers **.tmp**, tous les fichiers **.TMP** et le dossier **C:\TEMP**.

Caractères génériques

Vous pouvez utiliser un ou plusieurs caractères génériques * et ? dans un critère. Ces caractères peuvent être utilisés dans le chemin d'accès complet et le nom du fichier ou du dossier.

L'astérisque (*) remplace zéro ou plusieurs caractères dans un nom de fichier. Par exemple, le critère **Doc*.txt** englobe les fichiers tels que **Doc.txt** et **Document.txt**.

Le point d'interrogation (?) remplace exactement un seul caractère dans un nom de fichier. Par exemple, le critère **Doc?.txt** englobe les fichiers tels que **Doc1.txt** et **Docs.txt**, mais pas les fichiers **Doc.txt** ou **Doc11.txt**.

VSS

Indiquez si le service de cliché instantané des volumes (VSS) doit être utilisé pendant la sauvegarde.

Cette option ne s'applique qu'aux machines sur lesquelles VMware Tools est installé (p. 45).

Cette option garantit que le système de fichiers est sauvegardé dans un état cohérent. Pour les machines exécutant Windows, cette option assure également l'état cohérent de toutes les données utilisées par les applications compatibles VSS, telles que Microsoft SQL Server.

Sans cette option, le processus de sauvegarde est plus rapide, mais la cohérence des données ne peut pas être garantie.

2.6.2 Modification d'un plan de sauvegarde

Important : les modifications que vous apportez à un plan de sauvegarde affectent toutes les machines virtuelles (vos machines et celles des autres utilisateurs) auxquelles le plan de sauvegarde est appliqué.

Pour modifier un plan de sauvegarde

1. Ouvrez l'onglet **Plans de sauv..**
2. Sélectionnez le plan de sauvegarde que vous désirez modifier, puis cliquez sur **Modifier**.
3. Affichez ou modifiez le nom, la planification, les règles de rétention (p. 55) et les options de sauvegarde (p. 57).
4. Cliquez sur **OK**.

Conséquences du changement du chiffrement

Si vous devez modifier le paramètre **Chiffrement** (pour activer ou désactiver le chiffrement ou pour modifier le mot de passe), considérez ce qui suit :

- **Les règles de rétention ne s'appliqueront plus** aux sauvegardes concernées par l'ancien paramètre de chiffrement. Vous pourrez uniquement supprimer ces sauvegardes manuellement (p. 59).
- **Des enregistrements séparés seront affichés** pour les jeux de sauvegarde possédant des paramètres de chiffrement différents. Durant la restauration, vous devrez sélectionner l'enregistrement approprié et indiquer le mot de passe requis.

La même situation se produit lorsque vous appliquez un plan de sauvegarde à une machine à laquelle un autre plan de sauvegarde avec un paramètre **Chiffrement** est appliqué.

2.6.3 Retrait d'un plan de sauvegarde

Lorsque vous retirez un plan de sauvegarde d'une machine, toute sauvegarde en cours d'exécution est interrompue. La machine ne sera plus sauvegardée, à moins qu'un plan soit de nouveau mis en œuvre. Les sauvegardes de la machine sont conservées dans le stockage de sauvegarde jusqu'à ce que vous les supprimiez manuellement (p. 54).

Pour retirer un plan de sauvegarde

1. Ouvrez l'onglet contenant le nom de l'organisation.
2. Sélectionnez la ou les machines devant faire l'objet du retrait.
3. Cliquez sur **Retirer un plan de sauvegarde**.

2.6.4 Suppression d'un plan de sauvegarde

Lorsque vous supprimez un plan de sauvegarde, il est retiré (p. 59) de toutes les machines auxquelles il est appliqué (sur vos machines et sur celles des autres utilisateurs) et il est retiré de la liste des plans de sauvegarde.

Pour supprimer un plan de sauvegarde

1. Ouvrez l'onglet **Plans de sauv.**.
2. Sélectionnez le plan de sauvegarde que vous désirez supprimer, puis cliquez sur **Supprimer**.
3. Confirmez la suppression du plan de sauvegarde.

2.7 Génération de rapports d'utilisation

Cette fonctionnalité n'est disponible que pour les administrateurs.

Les rapports d'utilisation fournissent des données d'historique sur l'utilisation du service de sauvegarde dans votre organisation. Ces rapports peuvent vous être utiles pour calculer le montant que votre organisation déboursa pour l'utilisation du service.

Paramètres de rapport

Les valeurs de tous les paramètres sont contrôlées tous les jours à 23 h 55, conformément aux réglages horaires de vCloud Director. Le rapport utilise les valeurs existant à ce moment-là.

Le rapport comprend les paramètres suivants pour l'organisation :

- **Nombre de MV protégées** : Nombre total de machines protégées (c'est-à-dire les machines auxquelles des plans de sauvegarde sont appliqués), que des sauvegardes de ces machines existent ou non.
- **Utilis. stock.** : Taille totale de toutes les sauvegardes dans le stockage de sauvegarde (exprimée en giga-octets). Ce paramètre peut être exclu du rapport, en fonction des paramètres du service de sauvegarde.
- **Total des données sauvegardées** : Quantité totale des données sauvegardées. Cette quantité comprend le contenu initial des disques de la machine virtuelle et les modifications incrémentielles ultérieures apportées à ce contenu.
- **Excédent de quota** : Quantité de données qui dépasse le quota défini pour l'organisation (exprimée en giga-octets).
- **Taille disque MV protégées** : Taille totale des disques durs des machines protégées (exprimée en giga-octets), indépendamment de l'espace occupé sur ces disques.
- **Taille mém. RAM MV protégées** : Taille totale de la mémoire des machines protégées (exprimée en giga-octets).
- **Nombre de CPU des MV protégées** : Nombre total de CPU des machines protégées.

Pour générer un rapport d'utilisation

1. Ouvrez l'onglet **Stock. de sauv.**.
2. Développez la zone **Utilis. stock.** en bas, puis cliquez sur **Générer rapport d'util.**.
3. Dans **Période**, sélectionnez la période couverte par le rapport :
 - **Mois en cours** : le rapport comprendra des données entre le premier jour du mois en cours et le jour actuel (si vous générez le rapport après 23:55) ou jusqu'au jour précédent (si vous générez le rapport avant 23:55).

- **Mois précédent** : Le rapport comprendra des données de tous les jours du mois précédent. Par exemple, en avril, vous obtiendrez un rapport pour la période comprise entre le 1er mars et le 31 mars.
 - **Période personnalisée** : le rapport comprendra des données pour l'intervalle que vous spécifiez.
4. Dans **Type**, sélectionnez le type de rapport :
 - **Statistiques journ.** : le rapport comprendra les valeurs des paramètres de rapport pour chaque jour de la période visée. Le rapport comprend également le *résumé* : les valeurs minimale, maximale et moyenne de chaque paramètre de rapport pour la période visée.
 - **Rapport synthèse** : le rapport comprendra uniquement le résumé (voir option précédente).
 5. Cliquez sur **OK**. Le rapport s'affiche dans une fenêtre ou un onglet de navigateur distinct.
 6. [Facultatif] Pour imprimer le rapport, cliquez sur **Imprimer**. Pour enregistrer le rapport en tant que fichier .csv (valeurs séparées par des virgules), cliquez sur **Enreg. au form. .csv**.

2.8 Autoriser les non-administrateurs à utiliser le service

L'utilisation du service de sauvegarde comprend la connexion à celui-ci, les opérations de sauvegarde et de restauration, ainsi que la gestion des sauvegardes et des plans de sauvegarde. Un administrateur système peut être amené à créer un rôle vCloud Director dédié pour l'accès au service de sauvegarde.

Les administrateurs d'organisation peuvent autoriser les membres de tout rôle vCloud Director à utiliser le service.

Pour autoriser les membres d'un rôle vCloud Director à utiliser le service

1. Connectez-vous au service de sauvegarde.
2. Cliquez sur l'onglet **Paramètres**.
Le logiciel affiche une liste des rôles vCloud Director.
3. Cochez la case **Service activé** pour le rôle.

Tout membre de ce rôle sera en mesure d'utiliser le service de sauvegarde. Si vous avez besoin de conseils sur la façon d'attribuer un rôle vCloud Director à un utilisateur, lisez la section suivante.

2.8.1 Attribution d'un rôle vCloud Director à un utilisateur

La procédure ci-après peut s'appliquer aux deux types d'utilisateurs suivants :

- **Utilisateurs locaux** : utilisateurs dont les comptes ont été créés dans vCloud Director
- **Utilisateurs LDAP** : utilisateurs dont les comptes ont été importés dans vCloud Director à partir d'un annuaire Lightweight Directory Access Protocol (LDAP), tel qu'Active Directory

Pour attribuer un rôle à un utilisateur

1. Connectez-vous à vCloud Director.
2. Cliquez sur **Administration > Utilisateurs**.
3. Attribuez le rôle en autorisant l'accès au service de sauvegarde à l'utilisateur.

L'utilisateur peut commencer à employer le service dès que vous avez attribué le rôle.

Autre méthode pour les utilisateurs LDAP

Si votre organisation possède un grand nombre d'utilisateurs LDAP non-administrateurs, vous pouvez suivre une procédure différente pour leur permettre d'employer le service.

Pour attribuer un rôle à un groupe LDAP

1. Connectez-vous au serveur LDAP (tel qu'un contrôleur de domaine Active Directory) depuis lequel les comptes d'utilisateurs sont importés dans vCloud Director.
2. Créez un groupe dans l'annuaire LDAP (par exemple : **Utilisateurs du service de sauvegarde vCloud**).
3. Ajoutez tous les utilisateurs que vous voulez autoriser à accéder au groupe créé à l'étape 2. Vous pouvez à présent vous déconnecter du serveur LDAP.
4. Connectez-vous à vCloud Director.
5. Dans la page **Groupes**, recherchez le groupe que vous avez créé à l'étape 2.
6. Attribuez au groupe le rôle disposant de l'accès aux services de sauvegarde.

En ajoutant ou en retirant des membres de groupe sur le serveur LDAP, vous pouvez modifier la liste des utilisateurs autorisés à employer le service.

2.9 Affichage des journaux d'audit

Le service de sauvegarde comprend un journal d'audit qui enregistre les opérations effectuées par les utilisateurs.

Les administrateurs système et de l'organisation peuvent voir le journal dont la portée se trouve dans leur zone de contrôle.

Pour afficher le journal d'audit

1. Connectez-vous au service.
2. Cliquez sur l'onglet **Paramètres**.

3 Références terminologiques

Agent pour vCloud

Composant de l'infrastructure de service de sauvegarde qui s'exécute sur une machine virtuelle dédiée au sein d'un cluster de gestion vCloud Director.

Administrateur de l'organisation

Utilisateur possédant le rôle Administrateur de l'organisation dans vCloud Director.

Un administrateur d'organisation peut sauvegarder et restaurer n'importe quelle machine virtuelle dans l'organisation.

Administrateur système

Utilisateur possédant le rôle Administrateur système dans vCloud Director.

Un administrateur système peut sauvegarder et restaurer n'importe quelle machine virtuelle dans n'importe quelle organisation. Un administrateur système peut autoriser les utilisateurs d'organisation à sauvegarder les machines virtuelles de leur organisation.

Cluster de gestion

Cluster ESX(i) qui contient les composants de l'infrastructure vCloud Director.

Groupe de ressources

Un ou plusieurs clusters ESX(i) contenant des machines virtuelles d'organisations vCloud Director.

Machine protégée

Machine virtuelle à laquelle un plan de sauvegarde est appliqué.

Plan de sauvegarde

Ensemble de règles qui définit la méthode de protection des machines virtuelles.

Ces règles incluent la planification de sauvegarde, les règles de rétention et les options de sauvegarde telles que la protection par mot de passe. Par exemple : réaliser une sauvegarde chaque jour à minuit, supprimer les sauvegardes datant de plus d'un mois, protéger les sauvegardes avec un mot de passe.

Plan de sauvegarde système

Plan de sauvegarde prêt à l'emploi prédéfini par l'administrateur système afin de le rendre disponible dans de nombreuses organisations. Les utilisateurs d'organisation peuvent appliquer des plans de sauvegarde système à leurs machines virtuelles.

Les modifications apportées aux règles de rétention ou de planification d'un plan de sauvegarde système concernent toutes les organisations pour lesquelles celui-ci est disponible.

Propriétaire du plan de sauvegarde

Utilisateur d'organisation qui a créé le plan de sauvegarde.

Les plans de sauvegarde système ont un propriétaire spécial nommé **Système**. **Système** est également propriétaire des plans de sauvegarde créés par l'administration système au sein de l'organisation.

Quota de stockage (quota)

Espace de stockage affecté à une organisation.

Si le quota est dépassé, des alertes s'affichent dans l'interface du service de sauvegarde à l'attention de l'administrateur système et des utilisateurs de l'organisation. À moins d'être appliquées manuellement par l'administrateur système, les restrictions d'utilisation du service de sauvegarde ne s'appliquent pas.

Règles de rétention

Partie d'un plan de sauvegarde indiquant la durée de conservation des sauvegardes.

Restauration

Opération de création ou d'écrasement d'une machine virtuelle à l'aide de données enregistrées précédemment dans une sauvegarde. Si la machine sauvegardée est sélectionnée pour restauration, elle est écrasée. Autrement, une machine virtuelle est créée.

Sauvegarde (opération)

Opération qui enregistre des informations sur une machine virtuelle sous une forme compacte, à des fins de restauration.

Sauvegarde (point de récupération)

Résultat d'une opération de sauvegarde unique.

Une sauvegarde est un point dans le temps jusqu'auquel l'utilisateur peut restaurer la machine virtuelle. Les données nécessaires à la restauration sont stockées à deux emplacements. Le contenu des disques virtuels et la configuration de la machine virtuelle sont stockés dans le stockage de sauvegarde. Les métadonnées qui reflètent l'appartenance de la machine dans vCloud (configuration des cartes réseau virtuelles, nom de l'ordinateur, vApp dont la machine fait partie) sont stockées dans l'agent pour vCloud.

Stockage de sauvegarde

Dossier qu'alloue un administrateur système pour le stockage des sauvegardes d'une organisation.

Utilisateur

Personne possédant un compte d'utilisateur dans vCloud Director.

Selon les permissions affectées à son compte utilisateur dans vCloud Director, l'utilisateur peut être administrateur système, administrateur de l'organisation ou utilisateur non-administrateur.

vApp

Ensemble de machines virtuelles créé dans vCloud Director et pouvant être géré dans vCloud Director comme une entité unique.

Déclaration de copyright

Copyright © Acronis International GmbH, 2002-2014. Tous droits réservés.

“Acronis” et “Acronis Secure Zone” sont des marques enregistrées de Acronis International GmbH.

« Acronis Compute with Confidence », « Acronis Startup Recovery Manager », « Acronis Active Restore », « Acronis Instant Restore » et le logo Acronis sont des marques enregistrées de Acronis International GmbH.

Linux est une marque déposée de Linus Torvalds.

VMware et VMware Ready sont des marques et/ou des marques déposées de VMware, Inc. aux États-Unis et/ou dans d'autres pays.

Windows et MS-DOS sont des marques déposées de Microsoft Corporation.

Toutes les autres marques de commerce ou autres droits d'auteurs s'y référant appartiennent à leurs propriétaires respectifs.

La distribution de versions de ce document dont le contenu aurait été modifié est interdite sans la permission explicite du détenteur des droits d'auteur.

La distribution de ce travail ou d'une variante sous forme imprimée (papier) standard à des fins commerciales est interdite à moins que l'on ait obtenu des autorisations de la part du détenteur des droits d'auteur.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTES CONDITIONS, DÉCLARATIONS ET GARANTIES, IMPLICITES OU EXPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE CONFORMITÉ, D'USAGE POUR UN EMPLOI PARTICULIER OU DE NON-TRANSGRESSION, SONT DÉNIÉES, SOUS RÉSERVE QUE CES DÉNIS DE RESPONSABILITÉ NE SOIENT PAS LÉGALEMENT TENUS POUR NULS.

Certains codes tiers peuvent être fournis avec le logiciel et/ou le service. Les termes de la licence de tiers sont détaillés dans le fichier license.txt situé dans le répertoire d'installation racine. Vous pouvez toujours rechercher la dernière liste du code tiers mise à jour et les termes de la licence associés utilisés avec le logiciel et/ou le service à l'adresse <http://kb.acronis.com/content/7696>.

Technologies Acronis brevetées

Les technologies utilisées dans ce produit sont couvertes et protégées par un ou plusieurs numéros de brevet aux États-Unis (7,047,380 ; 7,275,139 ; 7,281,104 ; 7,318,135 ; 7,353,355 ; 7,366,859 ; 7,475,282 ; 7,603,533 ; 7,636,824 ; 7,650,473 ; 7,721,138 ; 7,779,221 ; 7,831,789 ; 7,886,120 ; 7,895,403 ; 7,934,064 ; 7,937,612 ; 7,949,635 ; 7,953,948 ; 7,979,690 ; 8,005,797 ; 8,051,044 ; 8,069,320 ; 8,073,815 ; 8,074,035 ; 8,145,607 ; 8,180,984 ; 8,225,133 ; 8,261,035 ; 8,296,264 ; 8,312,259 ; 8,347,137 ; 8,484,427 ; 8,645,748 ; 8,732,121) et plusieurs demandes de brevet.