

# Chapitre 3

## Veeam Backup & Replication

### 1. Les composants de Veeam Backup & Replication

Veeam Backup & Replication permet la sauvegarde et la restauration de ressources virtuelles (Hyper-V, VMware, Nutanix) ou de ressources physiques (au travers des agents Veeam) exécutant un système d'exploitation Windows ou Linux. Il est capable de protéger les données ou de proposer une solution de récupération suite à un sinistre (dégât des eaux, dégât matériel sur un serveur, etc.). La solution de réPLICATION offerte par Veeam Backup & Replication assure la fonctionnalité de PRA/PCA. Le PRA (Plan de reprise d'activité) consiste à redémarrer l'infrastructure (serveurs, données) sur un environnement de secours en cas de perte d'un ou plusieurs serveurs. Le PCA (Plan de continuité d'activité) permet de poursuivre l'activité de l'entreprise, et ce, même en cas de sinistre impactant gravement le système d'information.

#### 1.1 Prérequis de Veeam Backup & Replication

Le serveur (virtuel ou physique) qui héberge Veeam Backup & Replication peut être membre d'un domaine Active Directory. Pour plus de sécurité, ce serveur est souvent membre d'un groupe de travail et non d'un domaine. Les rôles **Backup proxy**, **Backup repositories**, **Wan Accelerator** ainsi que certains composants d'infrastructure peuvent être attribués à un serveur Windows Server Core (sans interface graphique). A contrario, il n'est pas possible d'installer Veeam Backup & Replication sur ce type de serveur.

Avant de mettre en place une infrastructure Veeam Backup & Replication, il est conseillé de vérifier les prérequis. Ces derniers sont accessibles sur le site web de Veeam ([https://helpcenter.veeam.com/archive/backup/100/vsphere/system\\_requirements.html](https://helpcenter.veeam.com/archive/backup/100/vsphere/system_requirements.html)). Les prérequis des principaux composants sont présents ci-dessous.

Le serveur de sauvegarde nécessite au moins quatre coeurs, son architecture peut être x86 ou x64. De plus, il doit avoir un minimum de 4 GB de Ram, et il est nécessaire d'ajouter 500 MB par job de sauvegarde concurrent. Ces valeurs sont une recommandation minimum, il est nécessaire de l'adapter à l'infrastructure cible. Un job de sauvegarde contenant un grand nombre de VM à sauvegarder nécessite évidemment plus de mémoire. L'utilisation d'un lecteur de bandes est également consommateur de ressource mémoire.

L'espace disque requis est un point critique dans une infrastructure de sauvegarde. Les fichiers nécessaires à l'exécution de Veeam Backup & Replication (hors fichiers de sauvegardes) sont stockés au niveau de la partition système. Les différents répertoires de cache et du catalogue peuvent, eux, être stockés sur une partition de données. Il est très important d'estimer la place nécessaire pour héberger les différents fichiers de sauvegarde. Une grande rétention nécessite de stocker les chaînes de sauvegardes (fichiers VBK et VIB - ce point est traité plus tard) plus longtemps. L'espace disque varie donc en fonction de la rétention mais également du type de sauvegarde (complète ou incrémentale).

Le serveur est installé sur un système d'exploitation Microsoft (Windows Server 2012 et ultérieure). Il est recommandé d'utiliser une des dernières versions de Windows Server (Windows Server 2019 ou 2022), ceci afin d'éviter de migrer l'infrastructure Veeam quelques mois/années après son installation. De plus, certaines fonctionnalités de Veeam, comme la déduplication, nécessitent d'utiliser un système d'exploitation (pour les serveurs Veeam) d'une version au moins égale à la version la plus haute des serveurs sauvegardés. Si vous sauvegardez des serveurs sous Windows Server 2012 et 2016, il est nécessaire d'installer Veeam sur un serveur Windows Server 2016 ou ultérieur.

Veeam Backup & Replication nécessite l'utilisation d'une base de données SQL. En production, il est préférable d'utiliser SQL Server Standard. La version Express peut être utilisée pour de très petites infrastructures de sauvegarde ainsi que pour les tests. À ce jour, SQL Server 2012 et les versions ultérieures sont supportés. Comme pour le système d'exploitation, il est fortement recommandé d'utiliser les dernières versions de SQL Server (2019 ou 2022). Depuis la version 12 de Veeam Backup & Replication, il est également possible d'utiliser PostgreSQL pour la base de données de Veeam Backup & Replication. Ce type de moteur de base de données étant open source.

Le .Net Framework 4.7.2 est utilisé par Veeam Backup & Replication. Dans le cas où ce dernier n'est pas présent sur le serveur, il est installé pendant la phase d'installation. La plateforme PowerShell est également nécessaire ; cette dernière doit être en version 5.1.

Les serveurs proxy et repositories sont des composants de l'infrastructure Veeam Backup & Replication. Ils peuvent être installés sur un serveur Microsoft (Windows Server 2012 et versions ultérieures) ou sur un serveur Linux. Les distributions suivantes sont supportées par Veeam pour l'hébergement du rôle Backup Proxy.

- CentOS 7–8.3
- CentOS Stream
- Debian 9.0–10.8
- Fedora 30–33
- openSUSE Leap 15.2, Tumbleweed
- Oracle Linux 6 to 8.3 (RHCK)
- RHEL 6.0–8.3
- SLES 11 SP4, 12 SP1–SP5, 15 SP0–SP2
- Ubuntu: 14.04 LTS, 16.04 LTS, 18.04 LTS, 19.10, 20.04 LTS

## 1.2 Protection avec VBR

Veeam Backup & Replication est capable de protéger un grand nombre de ressources internes et externes. Les ressources hébergées sous VMware vSphere, Microsoft Hyper-V ou Nutanix AHV peuvent être sauvegardées et restaurées. Il est également possible de protéger les VM (*Virtual Machine* - Machine virtuelle) présentes dans une instance AWS EC2 ou Microsoft Azure. Différentes ressources physiques (Windows, Linux et macOS) sont également prises en charge par Veeam Backup & Replication. Néanmoins ce type de workload nécessite l'utilisation d'agent. Ce point est traité plus loin dans le chapitre Nas et serveurs physiques. Les fichiers et dossiers sauvegardés sur un NAS peuvent être sauvegardés et restaurés.

Outre les ressources de type machine physique ou virtuelle, les applications et les données qu'elles hébergent sont également protégées par Veeam. Les applications de base de données SQL server, Oracle et PostgreSQL sont prises en charge. Il en est de même pour l'annuaire Active Directory et le serveur de messagerie Microsoft Exchange. Enfin, il est possible de sauvegarder les données présentes dans OneDrive et SharePoint.

Au-delà du système d'exploitation, Veeam Backup & Replication s'attache à sauvegarder la donnée et ce quel que soit son emplacement (système d'exploitation, application, etc.).

## 1.3 Permissions requises

De nos jours, les aspects sécurité sont très importants. Il est donc nécessaire d'accorder un minimum de droits.

### Veeam Backup & Replication

Lors de l'installation de Veeam Backup & Replication, un compte utilisateur est configuré. Afin de respecter la politique de moindre privilège, le compte utilisateur Active Directory utilisé doit être ajouté dans le groupe administrateur local du serveur. Il est possible de configurer le service Veeam afin qu'il s'exécute en tant que système local. Microsoft SQL Server nécessite quelques permissions. Le compte utilisateur configuré lors de l'installation de Veeam Backup & Replication doit avoir la permission **CREATE ANY DATABASE**. Configurée au niveau de Microsoft SQL Server, elle permet la création de la base de données. Par la suite, il est nécessaire d'octroyer au compte le rôle db\_owner. Cette opération doit être effectuée depuis SQL Management Studio.

### Serveur et Repository

Lors de l'ajout d'un ESXi / vCenter, un compte utilisateur possédant des permissions root doit être utilisé. Il en est de même pour les Repositories Linux, qui nécessiteront le compte root ou un compte possédant des permissions équivalentes. Les Repositories SMB ne nécessitent, eux, qu'une autorisation de modifier au niveau du dossier partagé.

### Applications Microsoft et autres

Les différentes applications telles que Microsoft Exchange, Active Directory, etc. nécessitent des permissions particulières.

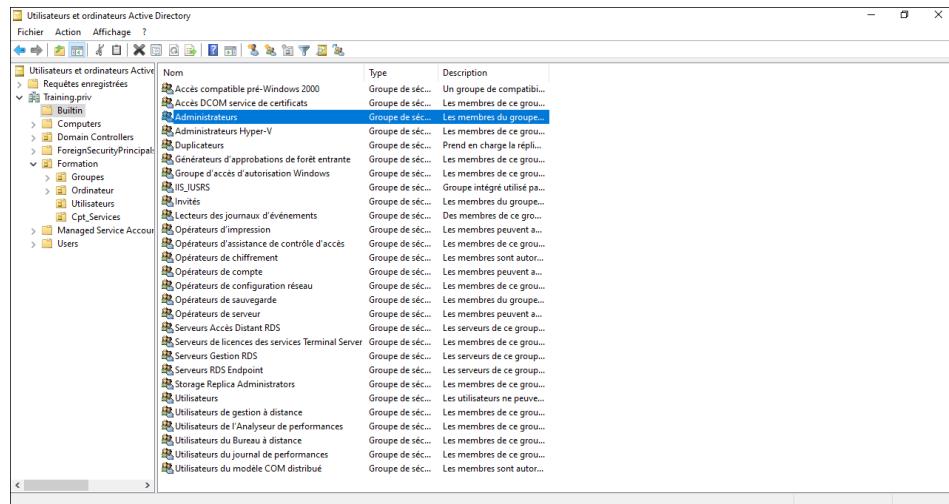
Afin de pouvoir procéder à la sauvegarde de Microsoft SQL Server, le compte utilisateur doit posséder le droit d'administrateur du serveur SQL. Il doit également être Sysadmin au niveau des autorisations de SQL Server. Il est néanmoins possible de minimiser les autorisations. Dans ce cas bien précis, l'utilisateur doit posséder le rôle public et dbcreator au niveau de l'instance SQL. Les droits suivants doivent être positionnés au niveau de la base de données.

- db\_backupoperator
- db\_denydatareader
- public

Des droits supplémentaires doivent être ajoutés pour l'utilisateur au niveau des bases de données master, model, msdb : il est nécessaire d'ajouter db\_backupoperator, db\_datareader et public. Concernant le droit db\_datawriter, il doit être positionné au niveau de la base de données msdb.

## Chapitre 3

La sauvegarde de l'annuaire Active Directory nécessite des droits plus élevés. En effet, le compte utilisateur doit être membre du groupe Administrateurs présent dans-Built-in. L'ajout dans ce groupe consiste à octroyer à l'utilisateur de service le droit d'admin du domaine. Ce droit est néanmoins requis pour pouvoir effectuer une restauration granulaire des objets AD.



The screenshot shows the Windows Active Directory Users and Computers snap-in. The left pane displays a tree view of organizational units: Utilisateurs et ordinateurs Active, Built-in, and several other OUs. The right pane lists objects with columns for Nom (Name), Type (Type), and Description (Description). The 'Administrateurs' group is highlighted with a blue selection bar. Other groups listed include Accès compatible pré-Windows 2000, Accès DCOM service de certificats, Administrateurs Hyper-V, Administrateurs locaux, Applicatrices, Générateurs d'applications de forêt entrante, Groupe d'accès d'autorisation Windows, IIS\_IUSRS, Invités, Lecteurs des journaux d'événements, Opérateurs d'impression, Opérateurs d'assistance de contrôle d'accès, Opérateurs de chiffrement, Opérateurs de compte, Opérateurs de configuration réseau, Opérateurs de sauvegarde, Opérateurs de serveur, Serveurs Accès Distant RDS, Serveurs de licence des services Terminal Server, Serveurs Gestion RDS, Serveurs RDS EndPoint, Storage Replica Administrators, Utilisateurs, Utilisateurs de gestion à distance, Utilisateurs de l'Analyseur de performances, Utilisateurs du Bureau à distance, Utilisateurs du journal de performances, and Utilisateurs du modèle COM distribué.

La sauvegarde de Microsoft Exchange et Microsoft SharePoint nécessite des droits d'administrateur local pour Exchange et d'administrateur de la ferme pour SharePoint. La sauvegarde de la base de données SQL pour SharePoint nécessite les mêmes droits que ceux listés précédemment.

Enfin, dans les applications pouvant être sauvegardées, Oracle et PostgreSQL sont également présents. Concernant Oracle installé sur un serveur Windows, le compte utilisateur doit être membre du groupe administrateur local ainsi que du groupe ORA\_DBA. Concernant Oracle sous Linux, un utilisateur possédant un droit root est nécessaire.

Pour PostgreSQL, il est nécessaire de procéder à la création d'un compte utilisateur et de lui octroyer les droits de superuser. Ce compte est utilisé par le job de sauvegarde pour se connecter à la base de données et sauvegarder cette dernière.

## 1.4 Vue d'ensemble des différents composants

Avant de pouvoir administrer et configurer Veeam Backup & Replication, il est nécessaire de connaître les différents composants présents dans une infrastructure Veeam.

### 1.4.1 Serveur de sauvegarde

Le serveur de sauvegarde (Backup server) est un serveur fonctionnant sur Microsoft Windows Server. Il peut être physique ou virtuel. Veeam Backup & Replication est installé sur ce serveur. Au centre de l'infrastructure Veeam, il permet d'effectuer différentes opérations d'administration telles que la coordination des sauvegardes et de la réplication ainsi que les tâches de vérification et restauration.

Il peut également contrôler la planification des différents travaux de sauvegarde ainsi que des ressources allouées à ce travail.

Il utilise différents composants.

Le **Veeam Backup Service** est un service Windows. Il a pour fonction de coordonner les différentes opérations effectuées par Veeam Backup & Replication (sauvegarde, restauration, etc.).

Le **Veeam Broker Service** permet de gérer l'interaction avec les différentes infrastructures virtuelles. Il assure la collecte de la topologie de l'infrastructure virtuelle. Il a également pour fonction de fournir aux travaux de sauvegarde les informations nécessaires à cette topologie, dans le but d'améliorer les performances.

Le **Veeam Guest Catalog Service** assure l'indexation, au niveau du système d'exploitation, des différentes VM. Il est ainsi plus aisément de procéder à une recherche de fichier au niveau de l'OS (*Operating System* - Système d'exploitation) invité. Ces index sont stockés dans le dossier Veeam Backup Catalog. Son emplacement est défini lors de l'installation du serveur de sauvegarde.

Le **Mount Service** permet d'effectuer le montage des sauvegardes ainsi que des répliques. Il assure, grâce à ce montage, la restauration des fichiers du système d'exploitation au niveau de la VM ainsi que des éléments d'application.

La **Veeam Backup & Replication Configuration Database** (base de données de configuration de VBR) contient les données de configuration. On y trouve les travaux de sauvegarde, les sessions, etc. Depuis la version 12 de Veeam Backup & Replication, il est possible d'utiliser une base de données de type PostgreSQL. Lors de l'installation de Veeam, un choix entre SQL et PostgreSQL doit être effectué. Pour rappel la version Express de SQL Server doit être utilisé pour des lab, en production il est nécessaire d'utiliser la version Standard. Les licences pour cette dernière ne sont pas fournies avec la licence Veeam.

### 1.4.2 Hôtes et serveurs

Après avoir configuré Veeam Backup & Replication, il est nécessaire de procéder à l'ajout des différents serveurs. Ces derniers peuvent être utilisés pendant la sauvegarde ou la réPLICATION. Les hôtes ESXi ou le vCenter Server peuvent être utilisés en tant qu'hôte source (sauvegarde ou réPLICATION des VM) ou en tant que cible. Dans ce cas, l'hôte de destination contient les réPLICAS de VM.

Il est également possible d'ajouter des serveurs Windows Server et Linux en tant que Backup Proxy et/ou Backup Repository.

### 1.4.3 Backup Proxy

Le serveur possédant le rôle de Backup Proxy est situé entre le serveur de sauvegarde et les autres composants présents dans l'infrastructure Veeam. Il assure le traitement des travaux de sauvegarde et effectue également la délivrance du trafic de sauvegarde.

Il a pour fonction la récupération des données des différentes machines virtuelles à partir du stockage de production. Il assure également la compression et la déduplication. Il procède aussi au chiffrage de la sauvegarde afin de sécuriser les données qu'elle contient.

Différents modes sont disponibles. Lors de la configuration d'un travail de sauvegarde, il est possible d'en sélectionnez un ou de laisser en mode automatique (sélection par Veeam du mode le plus approprié).

- **Direct Storage Access** : ce mode est sélectionné si le serveur Veeam a un accès direct au stockage de production.
- **Virtual Appliance** : une VM exécutant le système d'exploitation Windows Server est créée dans l'ESX. Lors de la sauvegarde, les disques de la VM sauvegardés sont ajoutés à cette VM. Elle transfère les données contenues dans la VM directement dans le stockage de production.
- **Réseau** : les sauvegardes sont effectuées au travers du réseau local. Cela consomme plus de ressource au niveau du réseau local.

Le Backup Proxy utilise des services dont le déploiement est entièrement automatisé par Veeam Backup & Replication.

Il est également intéressant de noter que les trois modes de transport ci-dessus sont fournis par VMware, mais Veeam a développé des modes de transport supplémentaires (Backup from Storage Snapshots et Direct NFS) et de nombreuses améliorations aux modes de transport mis en œuvre par VMware.

Le **Veeam Installer Service** est un service Windows installé et démarré automatiquement sur l'ensemble des serveurs Microsoft ajoutés en tant que serveurs gérés. Il assure l'analyse du système et permet l'installation et la mise à jour des différents composants Veeam nécessaires.

Le **Veeam Data Mover** est un composant qui permet le traitement des données (récupération des données au niveau de la source, déduplication, compression de la donnée). Il permet également de stocker les données sauvegardées au niveau du stockage cible.

#### 1.4.4 Backup Repository

Un repository Veeam consiste en un espace de stockage où Veeam Backup & Replication positionne ses fichiers de sauvegarde (vbk, vib). Dans le cas d'une réPLICATION, il stocke les metadata de la ou des machines virtuelles. Différents types de repositories sont disponibles.

Le *direct attached storage* consiste à ajouter un serveur Microsoft ou Linux comme Backup Repositories. Dans le cas d'une très petite infrastructure Veeam, cela peut être la partition de données du serveur Veeam. Il est fortement recommandé de ne pas le stocker sur une partition système.

Depuis la version 11 de Veeam Backup & Replication, il est possible d'activer le stockage immuable. Ainsi, pendant une durée de temps déterminée par l'administrateur, les fichiers de sauvegarde ne peuvent être modifiés. C'est une excellente protection contre les ransomwares. Il est de plus en plus fréquent de voir des systèmes d'information et des sauvegardes cryptés par ce genre de menace. La version 12 a facilité la configuration d'un repository immuable, l'assistant de création a été modifié afin de faciliter la configuration de ce type de repository.

Le *network attached storage* permet l'ajout d'un partage SMB (CIFS) et/ou NFS. Cela peut être un NAS local ou un partage directement dans Azure ou autre provider.

Les appliances de stockage dédupliquées peuvent être ajoutées dans Veeam. Elles assurent la déduplication des données et ainsi un gain en espace disque. Les appliances Dell EMC Data Domain, Exagrid, HPE StorageOnce et Quantum DXi peuvent être ajoutées et configurées dans Veeam.

Le stockage objet permet l'externalisation de la sauvegarde et le stockage des éléments sauvegardés dans un service de stockage cloud (exemple S3, blob azure, etc.).

Dans les bonnes pratiques, il est recommandé, quand cela est possible, d'utiliser un repository physique. Veeam recommande pour les serveurs hébergeant ce rôle un minimum de deux coeurs au niveau processeur et 8 Go de mémoire RAM.

#### **1.4.5 Gateway server**

Le gateway server est un composant de l'infrastructure qui a pour but de faire "le relais" entre le serveur de sauvegarde et le repository. Il est requis dans le cas où l'un des repositories suivants est utilisé :

- Repository sur un partage réseau
- Appliance de déduplication Dell EMC Data Domain
- Appliance de déduplication HPE StoreOnce

Ces repositories n'ont pas la possibilité d'héberger le service data mover, nécessaire à l'établissement d'une connexion entre le Backup Proxy et son repository.

Le *gateway server* héberge donc le Veeam Data Mover cible. À la suite de la connexion entre les Veeam Data Mover source et cible, Veeam Backup & Replication effectue le transport des données vers le repository via le gateway server.

Le composant peut être ajouté à un serveur Microsoft ou linux virtuel ou physique.

#### **1.4.6 Scale-out Repository**

Le *Scale-out Repository* est un repository avec une mise à l'échelle horizontale. Il est composé d'un ou plusieurs repositories aussi appelés "*capacity extents*". Il peut être étendu à des repositories objets sur site accessible par l'intermédiaire d'un fournisseur cloud.

Ce type de repository offre l'avantage de pouvoir être extensible. En cas de manque d'espace, il est possible d'ajouter un nouveau repository "*capacity extent*". L'espace libre du système de stockage ajouté vient s'ajouter à la capacité du scale-out repository.

Cela permet d'éviter de déplacer des fichiers de sauvegarde d'un repository à un autre. L'ensemble des cibles de sauvegarde (*backup targets*) est supporté par le Scale-out Repository.

- Serveur Windows ou Linux
- Serveur avec stockage local ou DAS
- Partage réseau

Il est également possible d'effectuer une libération des extents vers un stockage froid dans le cloud (archivage des données, par exemple).

#### **1.4.7 Tape server**

De nos jours, il est important d'externaliser sa sauvegarde ou d'avoir un média hors ligne. Les pirates informatiques et ransomwares s'attaquent au système d'information mais également aux sauvegardes. Dans le cas des cryptages des sauvegardes, le rétablissement du système d'information peut être difficile, voire impossible.