Les 10 meilleures pratiques de sauvegarde pour vSphere

Date : 30 juillet 2019

Veeam Backup & Replication 9.5 Update 4b

VMware version 6.7

Hannes Kasparick
Analyste en chef, équipe de gestion des produits

Synthèse

La virtualisation des serveurs est une pratique largement répandue à travers le monde. En 2019, VMware reste leader sur ce marché et les clients Veeam® sont nombreux à avoir fait le choix de VMware vSphere comme plateforme de virtualisation. Ce livre blanc décrit les meilleures pratiques de sauvegarde et de disponibilité pour VMware vSphere avec Veeam Backup & Replication™ 9.5. Il n'aborde pas les meilleures pratiques générales propres à Hyper-V et Veeam Agent.

Introduction

La virtualisation des serveurs est une pratique largement répandue à travers le monde. En 2019, VMware reste leader sur ce marché et les clients Veeam sont nombreux à avoir fait le choix de VMware vSphere comme plateforme de virtualisation. La sauvegarde des VM (machines virtuelles) sur vSphere constitue une partie seulement de la disponibilité des services. Sans sauvegarde, pas de restauration. C'est pourquoi il est essentiel de disposer à tout moment de sauvegardes accessibles pour être restaurées dans les délais requis. Parmi les meilleures pratiques d'ordre général, la règle la plus importante est celle du 3-2-1.

La règle du 3-2-1 implique de disposer d'au moins trois copies : les données de production et deux lignes de sauvegarde. Il est également recommandé de stocker les copies de sauvegarde sur au moins deux types de support indépendants. On ne saurait trop insister sur cette indépendance qui doit se comprendre du point de vue technologique. Enfin, une autre copie doit être conservée hors site et hors ligne, à l'abri des catastrophes naturelles, des logiciels malveillants et des personnes non autorisées. Par exemple, Veeam Backup & Replication 9.5 Update 3a incluait la protection de Veeam Cloud Connect contre les pirates internes. Évidemment, le stockage des sauvegardes hors site peut toujours s'effectuer sur bande.

Avec Veeam Backup & Replication la règle du 3-2-1 devient celle du 3-2-1-0, zéro représentant l'absence de problème de restauration rendue possible grâce aux tests de restauration automatisés de Veeam SureBackup®. SureBackup a pour principale vocation de détecter les problèmes logiques dans les sauvegardes. Par exemple, si quelqu'un installe des mises à jour sans jamais redémarrer, un écran bleu ou une panique du noyau se produira après un redémarrage.

Ce document décrit plusieurs meilleures pratiques avec Veeam Backup & Replication et VMware vSphere. Celles-ci concernant exclusivement Veeam et VMware, elles ne portent pas sur les autres hyperviseurs.

Ces meilleures pratiques d'ordre général abordent les sujets suivants :

- mettre en place une stratégie de sauvegarde et de restauration adaptée aux besoins de votre activité,
- dimensionner correctement les équipements,
- s'assurer que VSS fonctionne sur les machines Windows,
- disposer d'un espace de sauvegarde suffisant.

Ces principes s'appliquent dans tous les cas, qu'il s'agisse de sauvegarder VMware, Hyper-V, un fournisseur de cloud ou un serveur physique. Avant de planifier ou mettre en œuvre une solution, il est primordial d'en déterminer les exigences.

Dans un monde idéal, celles-ci sont définies par les opérationnels qui indiquent à l'équipe IT les délais optimaux de reprise d'activité (RPO) et les objectifs de temps de restauration (RTO) attendus. La sauvegarde est-celle suffisante ou faut-il également prévoir une reprise après incident (DR) ?

Ces informations permettent de dimensionner les équipements, notamment le nombre de cœurs de CPU, la quantité de mémoire et la bande passante requise sur les réseaux (WAN, LAN et SAN). Il faut enfin disposer d'un stockage de la source et de la sauvegarde qui soit suffisamment rapide.

L'étape suivante concerne la sauvegarde elle-même. Veeam traite les images prenant en charge les applications en s'appuyant sur Microsoft VSS pour réaliser des sauvegardes des VM Windows cohérentes au niveau des applications. Ce mécanisme n'utilise pas la mise en suspension par les outils VMware. Pour que le traitement des images prenant en charge les applications soit fiable, il est indispensable que les VSS Writers des VM fonctionnent correctement.

Nº 1 : Utiliser les versions actuelles de Veeam et vSphere

Grâce aux toutes dernières versions de Veeam Backup & Replication et VMware vSphere, vous optimisez les performances. En effet, les performances de Veeam Backup & Replication 9.5 sont bien meilleures que celles des précédentes versions, en particulier dans les environnements vSphere. Leurs améliorations les plus notables concernent le service Broker de Veeam et les méthodes de sauvegarde non-VADP : ajout à chaud, accès direct NFS et sauvegarde à partir de snapshots de baie de stockage.

De con côté, VMware a amélioré la consolidation des snapshots de VM dans ESXi version 6.x, limitant le gel des VM en cas d'E/S intensives pendant la validation des snapshots à l'issue d'une sauvegarde.

Meilleure pratique : Tirez parti des améliorations apportées aux toutes nouvelles versions de Veeam Backup & Replication et de vSphere.

Nº 2 : Choisir son mode de sauvegarde avec soin

Veeam Backup & Replication offre trois modes de transport différents des VM sur vSphere, qui présentent tous des avantages et des inconvénients. Il n'existe pas de règle générale pour déterminer lequel est le mieux adapté. Vous choisirez donc l'un de ces trois modes en fonction de votre environnement et de ses exigences :

1. Mode réseau ou NBD
2. Accès direct au stockage
3. Appliance virtuelle/ajout à chaud

Les propriétés de chaque proxy permettent de configurer ces options dans la section du mode de transport, comme l'illustre la figure 1.

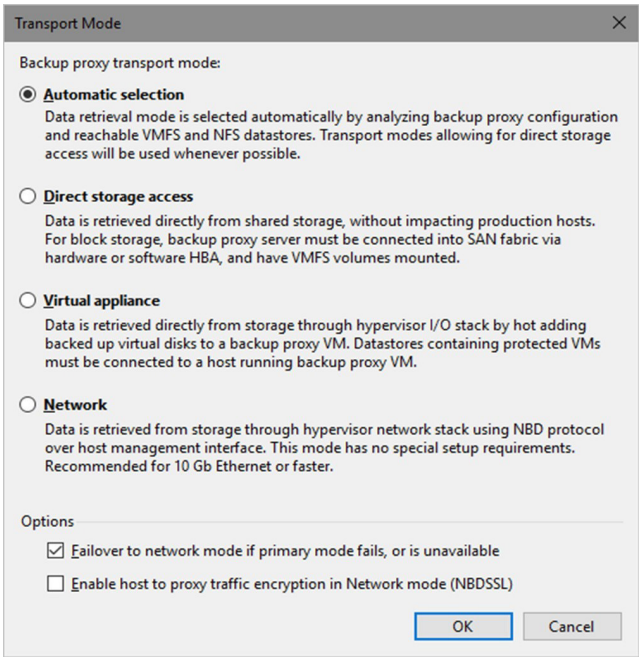

Figure 1 : Options de mode de transport

Le mode réseau ou NBD est le plus simple pour exécuter les sauvegardes VMware. Le serveur proxy Veeam utilise le port de gestion ESXi de chaque hôte ESXi pour transférer les données de sauvegarde. L'installation est donc simplifiée à l'extrême : elle ne nécessite pas de configuration supplémentaire des stockages ou des VM. Autre atout : une surcharge administrative très faible. Il représente un gain de temps par rapport au mode d'ajout à chaud, car il ne nécessite aucune opération de montage supplémentaire. Il ne crée pas non plus de snapshots de baie de stockage supplémentaires comme la sauvegarde à partir de snapshots de baie de stockage avec systèmes de stockage intégrés. Comme la coordination des VM et des snapshots de baie de stockage prend du temps, le mode réseau peut se révéler encore plus rapide pour les sauvegardes incrémentielles dans les environnements constitués de nombreuses VM avec un faible taux de modification des données.

Le port de gestion ESXi peut constituer un goulet d'étranglement, surtout s'il s'agit d'une interface réseau de seulement 1 Gbit. Toutefois, le problème ne se pose généralement pas avec des cartes d'interface réseau de 10 Gbits ou plus.

Si vous utilisez ESXi 6.5, sachez que cette version chiffre le trafic de sauvegarde via NBD-SSL. Auparavant, ce chiffrement était un paramètre en option. Cela ralentit sensiblement les sauvegardes. De nouveau autorisé dans les versions suivantes par VMware, le trafic NBD non chiffré est pris en charge depuis Veeam Backup & Replication 9.5 Update 3.

Le trafic de sauvegarde en mode d'accès direct au stockage est acheminé directement depuis le système de stockage vers le proxy de sauvegarde Veeam.

Il ne nécessite pas le passage par l'hyperviseur ESXi et le protocole dépend de l'environnement de stockage. Ce protocole est généralement FibreChannel ou iSCSI. L'accès direct au stockage présente le même avantage que le mode réseau en évitant les longues opérations de l'ajout à chaud. En contrepartie, ces deux modes utilisent l'API VADP

officielle de VMware pour la sauvegarde des VM. Or, celle-ci ayant un impact sur les performances de sauvegarde, Veeam Backup & Replication ne l'utilise pas dans trois configurations particulières :

- Sauvegarde à partir de snapshots de baie de stockage
- Accès direct NFS (semblable à l'accès direct au stockage)
- Appliance virtuelle/ajout à chaud

Éviter l'API VADP permet d'améliorer les performances de manière significative, ce qui explique le gain de popularité de l'ajout à chaud. Celui-ci présente en outre un autre avantage : en mode d'ajout à chaud, le proxy de sauvegarde Veeam s'exécute comme une VM supplémentaire pour les sauvegardes. Il monte les snapshots des VM à sauvegarder et achemine le trafic sur le réseau normal des VM, sans utiliser l'interface de gestion ESXi. C'est ce qui fait de l'ajout à chaud une solution performante sur les réseaux de 1 Gbit ne permettant pas les modes de sauvegarde avec accès direct au stockage.

Le mode de sauvegarde avec ajout à chaud n'est généralement pas recommandé avec les datastores NFS. Avec NFS, il est recommandé d'utiliser l'accès direct au stockage qui se traduit par le mode d'accès direct NFS. Celui-ci n'est pas proposé sous forme d'option dans l'interface graphique. Il s'agit simplement d'une déclinaison de l'accès direct au stockage. Cette recommandation est justifiée par le fait que l'ajout à chaud produit souvent un gel des VM si le proxy Veeam ne s'exécute pas sur le même hôte ESXi que la VM. Vous trouverez plus d'informations sur les environnements avec datastores NFS dans la base de connaissances Veeam KB 1681. Si vous prévoyez néanmoins d'utiliser le mode d'ajout à chaud sur les datastores NFS, appliquez la règle et le paramètre suivants :

- Prévoyez un proxy d'ajout à chaud par hôte proxy
- Paramétrez l'option EnableSameHostHotAddMode = 1 dans HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\ Veeam Backup and Replication

Les possibilités de sauvegarde étant nombreuses, vous pouvez utiliser le tableau ci-dessous pour évaluer les résultats de chaque mode et déterminer lequel convient le mieux à votre situation.

Mode	Operation	Time	Speed
Direct Storage Access	Full backup		
Direct Storage Access	Incremental backup		
Backup from Storage Snapshots	Full backup		
Backup from Storage Snapshots	Incremental backup		
Virtual Appliance	Full backup		
Virtual Appliance	Incremental backup		
Network	Full backup		
Network	Incremental backup		

Meilleure pratique : *Testez les modes de sauvegarde pour déterminer le mieux adapté à votre environnement.*

Nº 3 : Prévoir le mode de restauration

Une fois le mode de sauvegarde optimal identifié, il est important de s'intéresser au mode de restauration. Veeam propose 57 scénarios de restauration de VM, fichiers et objets applicatifs.

Tout d'abord, il est essentiel de savoir que la restauration des fichiers et des objets est différente de celle des VM et des disques. Veeam restaure les fichiers et les objets (e-mails Microsoft Exchange ou objets Microsoft Active Directory, par exemple) sur le réseau. Cela implique une connexion RPC (Windows) ou SSH (Linux) pour transférer les données à restaurer vers la VM.

La sauvegarde étant basée sur les snapshots de VM, comme la sauvegarde au niveau des blocs, la sauvegarde de VM entières ou de disques virtuels est également basée sur les blocs. Selon le mode de restauration, il existe une différence entre le provisionnement statique ou dynamique de la VM. Les modes de restauration sont les mêmes que ceux de sauvegarde (c'est-à-dire accès direct au stockage, appliance virtuelle et réseau), auxquels s'ajoute la fonctionnalité Instant VM Recovery™ associée à Storage VMotion ou à Quick Migration.

Les modes d'ajout à chaud et réseau peuvent restaurer des VM à provisionnement statique ou dynamique. Comme précisé précédemment, le mode appliance virtuelle/ajout à chaud ajouté introduit dans la version 9.5 améliore les performances de sauvegarde. C'est également le cas des restaurations de VM entières ou de disques en mode d'ajout à chaud. Dans la plupart des scénarios, il est logique de disposer d'au moins un proxy d'ajout à chaud pour les restaurations de VM ou de disques.

Le mode réseau est habituellement le mode de restauration le plus lent, car il ne peut pas exploiter l'intégralité de la bande passante.

L'accès direct au stockage n'est pas limité en termes de bande passante, mais il ne peut restaurer que les disques provisionnés statiquement. Ceux provisionnés dynamiquement sont convertis en disques statiques à la volée. Comme le mode d'accès direct au stockage utilise VADP pour les restaurations, il ne s'agit généralement pas de l'option la plus rapide. Il existe une exception : la restauration en mode d'accès direct NFS lorsque Veeam Backup & Replication n'utilise pas VADP.

Pour restaurer une VM ou un disque virtuel, il n'est pas nécessaire de transférer l'intégralité des données. Si les informations de suivi des blocs modifiés (CBT) sont correctes sur le stockage de production, il est possible d'exécuter une restauration sur cette base. Cette option peut accélérer la restauration. Pour ce faire, l'option de de restauration rapide Quick Rollback doit être activée manuellement pendant la restauration, comme l'illustre la figure 2.

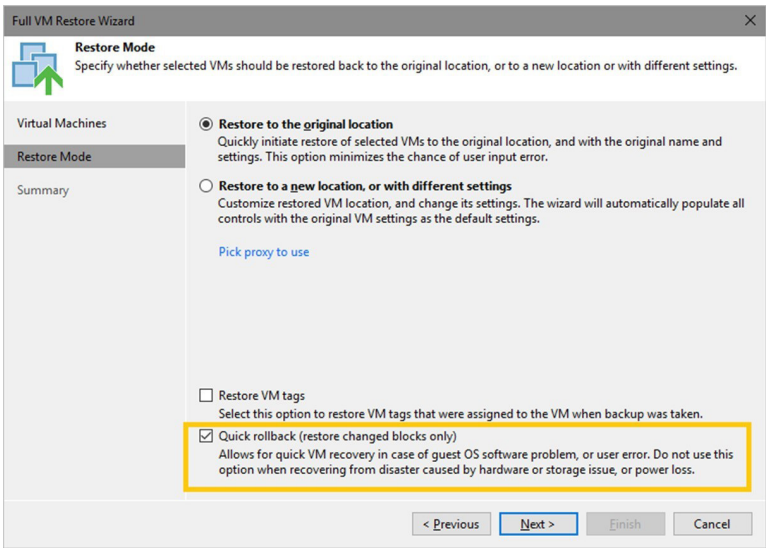

Figure 2 : Restauration rapide basée sur les informations de suivi des blocs modifiés (CBT)

La fonctionnalité Instant VM Recovery est une autre solution pour restaurer des VM entières. Elle permet de démarrer instantanément une VM directement depuis la cible de sauvegarde. Celle-ci agit comme un datastore NFS monté sur un hôte ESXi. Il existe deux possibilités pour transférer les données des VM depuis le datastore NFS cible vers le datastore de production :

- Veeam Quick Migration
- VMware Storage VMotion

Les possibilités de restauration de VM entières étant nombreuses, vous pouvez utiliser le tableau ci-dessous pour évaluer les résultats de chaque mode et déterminer lequel convient le mieux dans votre situation.

Mode	Operation	Time	Speed
Direct Storage Access	Full VM restore		
Direct Storage Access	Full VM restore CBT		
Virtual Appliance	Full VM restore		
Virtual Appliance	Full VM restore CBT		
Network	Full VM restore		
Network	Full VM restore CBT		
Instant VM recovery + Storage Vmotion	Full VM restore		
Instant VM recovery + Quick Migration	Full VM restore		

Meilleure pratique : Planifiez et testez les options de restauration en fonction des modes de stockage et de transport. Si vous n'utilisez pas de datastores NFS, prévoyez d'installer au minimum un proxy d'ajout à chaud comme solution de rechange.

Nº 4 : Installer les outils VMware

Dans de nombreuses situations, Veeam Backup & Replication s'appuie sur la présence d'outils VMware exécutés sur les VM. Sans ceux-ci, il ne peut pas trouver les adresses IP ni la version du système d'exploitation, par exemple. Le résultat : le traitement d'images prenant en charge les applications échouera.

La raison en est que Veeam Backup & Replication ne peut pas détecter les adresses IP indispensables pour se connecter aux VM sur le réseau. De même, l'API VIX ou vSphere qui sert de mécanisme de rechange pour interagir avec les SE invités ne fonctionnera pas en l'absence d'outils VMware (se reporter à la meilleure pratique nº 10 pour en savoir plus sur VIX). La figure 3 illustre l'échec d'un test de connexion au SE invité en l'absence d'outils VMware :

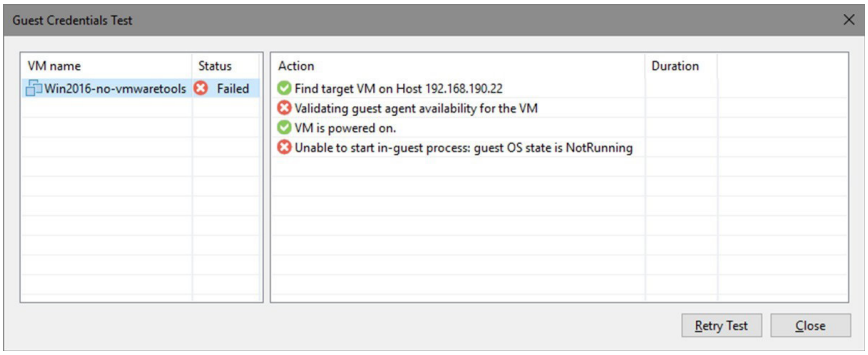

Figure 3 : Échec d'un test de traitement prenant en charge les applications

Les tests SureBackup constituent un deuxième exemple : en l'absence d'outils VMware, les tests heartbeat et ping échoueront. Sinon, la meilleure pratique nº 1 s'applique à ces outils : veillez donc à ce qu'ils soient toujours à jour.

Meilleure pratique : Installez les outils VMware et veillez à ce qu'ils soient toujours à jour.

Nº 5 : Intégrer des snapshots de baie de stockage dans son concept de disponibilité

Si les snapshots de baie de stockage ne sont certainement pas aussi efficaces qu'une sauvegarde, ils permettent de minimiser les pertes de données dans de nombreuses situations. Veeam Backup & Replication s'intègre avec différents fournisseurs de stockage, conjointement avec VMware vSphere. L'intégration aux stockages offre un nombre plus important de possibilités de protection des données.

La première consiste pour Veeam Backup & Replication à ouvrir les snapshots de baie de stockage et les fichiers de restauration directement depuis les snapshots de baie de stockage. Cela vous permet ainsi de planifier des snapshots de baie de stockage toutes les 15 minutes sans devoir créer de snapshot de VM. Certes, ces snapshots réalisés toutes les 15 minutes ne constituent pas réellement des sauvegardes puisqu'ils ne respectent pas la règle du 3-2-1, mais ils permettent de réduire les RPO.

La figure 4 illustre ce concept avec Veeam Explorer™ pour snapshots de baie de stockage. Les snapshots de baie de stockage apparaissent sur la gauche où sont affichés les LUN et les snapshots de l'un d'entre eux. Sur la droite sont affichées les VM de chaque snapshot de baie de stockage. À partir de là, il est possible de restaurer des VM avec Instant VM Recovery ou des fichiers et des objets applicatifs. Imaginez maintenant que des snapshots des LUN ou des volumes stratégiques soient réalisés toutes les 15 minutes et supprimés au bout de quatre heures. Cela rend possible la restauration des données remontant à 15 minutes plutôt que celles de la sauvegarde nocturne précédente.

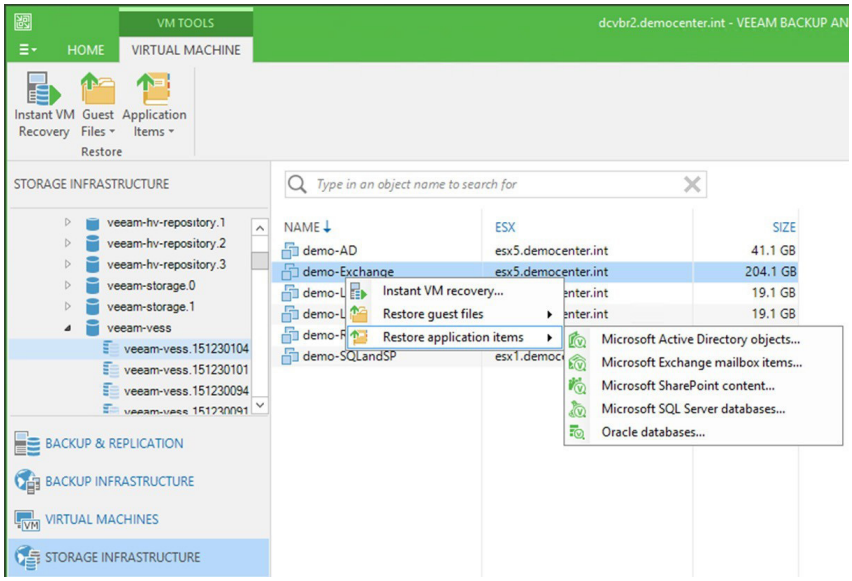

Figure 4 : Restauration d'objets à partir de snapshots de baie de stockage

Autre avantage de l'intégration aux stockages avec Veeam Backup & Replication : il est désormais possible de sauvegarder des VM importantes par la taille ou par le nombre de transactions — comme des serveurs de base de données — sans risquer leur gel pendant la consolidation des snapshots VMware. Bien que la situation se soit nettement améliorée avec les versions actuelles de vSphere, cela justifie toujours le recours aux snapshots de baie de stockage.

Enfin, Veeam Backup à partir de snapshots de baie de stockage permet l'utilisation par Veeam de ses mécanismes propriétaires d'extraction des données pour surclasser les sauvegardes VADP classiques. Cet avantage est particulièrement sensible pour les sauvegardes entières et toute sauvegarde en cas de taux de modifications élevé.

Meilleure pratique : Utilisez l'intégration aux stockages si votre stockage prend en charge les snapshots pour Veeam Backup & Replication.

Nº 6 : Anticiper la sauvegarde VMware vSAN

Étant donné la popularité croissante de VMware vSAN, il est logique de préciser certaines de ses caractéristiques. Comme VMware vSAN n'utilise pas les protocoles de stockage traditionnels, l'accès direct au stockage et l'option de sauvegarde à partir de snapshots de baie de stockage ne sont pas disponibles.

Les modes de sauvegarde pris en charge sont les modes appliance virtuelle/ajout à chaud et réseau. En mode ajout à chaud, Veeam Backup & Replication sauvegarde les VM en fonction de la proximité de leurs données. Cela signifie que les sauvegardes s'effectuent à travers un proxy sur l'hôte où résident les données les plus spécifiques des VM. Pour que ce mode fonctionne correctement, il faut disposer d'un proxy d'ajout à chaud par hôte ESXi. Les règles d'affinité des hôtes pour les VM proxy empêchent VMware DRS (Distributed Resource Scheduler) de déplacer ces VM vers d'autres hôtes ESXi.

Le résultat : des fenêtres de sauvegarde plus courtes grâce à un trafic et une latente moins importants sur le réseau. En effet, avec une VM et un proxy sur des hôtes différents, le trafic est plus important sur le réseau, ce qui augmente la latence et réduit la vitesse.

Veeam Backup & Replication est certifié VMware Ready pour vSAN dans la catégorie protection des données. Pour plus d'informations, consultez l'article de la base de connaissances VMware 2149874 et le guide de compatibilité VMware vSAN.

Meilleure pratique : Installez un proxy d'ajout à chaud par hôte ESXi si vous utilisez le mode appliance virtuelle avec VMware vSAN.

Nº 7 : Effectuer un suivi de son infrastructure (vSphere)

« Cela fonctionne, tout simplement » a été le slogan de Veeam pendant de nombreuses années. C'est une vérité pour la plupart des clients, car les paramètres par défaut sont très efficaces. Il est toutefois judicieux de planifier dans le détail le déploiement de Veeam Backup & Replication pour les installations de grande envergure.

vCenter est l'un des composants les plus stratégiques pour le fonctionnement de Veeam Backup & Replication. Si vCenter est en panne, les sauvegardes échoueront. Les fenêtres de maintenance de vCenter doivent donc être planifiées en dehors des fenêtres de sauvegarde. Il est également conseillé de surveiller la charge et le nombre de connexions sur vCenter. Sans oublier la stabilité du réseau entre le serveur de sauvegarde Veeam et vCenter !

En fonction de votre environnement, la sauvegarde peut peser de manière importante sur votre stockage de production. Il n'est pas inhabituel de constater des charges de plusieurs Go/s, ce qui peut augmenter la latence des E/S sur les baies de disques classiques. La fonctionnalité de contrôle des E/S de sauvegarde de Veeam Backup & Replication limite la vitesse de sauvegarde et de restauration (voir figure 5).

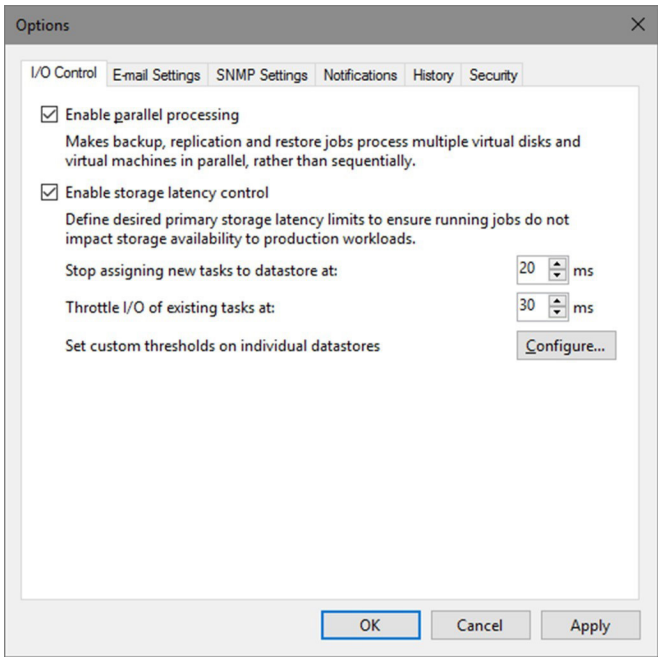

Figure 5 : Contrôle de latence du stockage

Le contrôle de latence du stockage attribue ou limite les tâches en fonction des valeurs de latence du datastore que Veeam récupère de vSphere. Cela se produit en deux étapes. D'abord, Veeam arrête d'attribuer de nouvelles tâches de sauvegarde à un datastore. Si la latence continue d'augmenter, il limite ensuite les tâches de sauvegarde existantes. Le résultat : la sauvegarde durera plus longtemps, mais avec un impact moindre sur les VM en cours d'exécution. Ce mécanisme permet d'effectuer des sauvegardes pendant les heures de production en impactant au minimum les VM, les applications et les utilisateurs.

Le contrôle de latence du stockage désactive le paramétrage par défaut de quatre snapshots de VM par datastore au maximum. Cela peut aussi améliorer les performances.

Meilleure pratique : Le fonctionnement de Veeam Backup & Replication étant fortement dépendant de vCenter, assurez-vous que celui-ci s'exécute efficacement, supervisez la charge au cours de la fenêtre de sauvegarde et procédez à des ajustements si nécessaire.

Nº 8 : Prévoir la sécurité

Veeam Backup & Replication se connecte à vCenter pour gérer la sauvegarde et la restauration des VM. Du point de vue de la sécurité, il est toujours judicieux d'utiliser les privilèges les plus bas. VMware vCenter offre des autorisations granulaires fines pour permettre les sauvegardes.

La page consacrée aux autorisations requises détaille celles à configurer selon le mode de sauvegarde. En effet, les différents modes de sauvegarde nécessitent des autorisations différentes. Il sera ainsi pertinent de disposer de l'autorisation de suppression de disque en mode appliance virtuelle.

Ces considérations de sécurité peuvent déterminer le choix du mode de sauvegarde. Il est en outre possible de limiter des serveurs de sauvegarde particuliers (si vous en disposez de plusieurs) à des emplacements ou objets spécifiques dans vCenter.

Meilleure pratique : Travaillez dans les limites du privilège le plus bas.

Nº 9 : Planifier son déploiement Veeam Backup & Replication avec Veeam ONE

Veeam Availability Suite™ comprend un puissant outil de planification pour les déploiements Veeam Backup & Replication : Veeam ONE™.

La fonctionnalité de supervision de Veeam ONE affiche l'état réel et les problèmes en cours de l'environnement vSphere. Les problèmes de sauvegarde peuvent notamment relever d'une latente élevée du stockage ou de snapshots de VM anciens, volumineux, nombreux ou orphelins.

La fonctionnalité de reporting de Veeam ONE produit le rapport d'évaluation de la configuration qui révèle les problèmes de sauvegarde potentiels. Il s'agit typiquement des problèmes suivants :

- outils VMware non installés,
- matériel version 4 ou antérieure,
- disques impossible à sauvegarder (des disques indépendants, par exemple),
- datastores disposant de moins de 10 % d'espace libre,
- mappages de périphériques bruts dans les VM.

Résoudre ces problèmes avant l'exécution des sauvegardes permet d'éviter qu'ils en créent d'autres par la suite.

Meilleure pratique : Utilisez Veeam ONE pour planifier l'installation de Veeam Backup & Replication.

Nº 10 : Effectuer les sauvegardes prenant en charge les applications via l'API VIX

La meilleure pratique nº 4 recommande de toujours disposer de la dernière version des outils VMware. Grâce à ces outils, l'administrateur Veeam peut effectuer des sauvegardes prenant en charge les applications pour les VM Windows, sans passer par une connexion réseau directe.

Le moyen de prédilection pour effectuer ce type de sauvegarde consiste à connecter le proxy des applications aux VM via RPC. C'est aussi le plus rapide. Si la communication réseau vers les VM est empêchée par la segmentation du réseau ou par des pare-feux, Veeam peut interagir avec les SE clients au moyen de l'API VIX ou vSphere (à partir de la version 6.5 de vSphere). La figure 6 illustre la connexion via VIX (encadré orange).

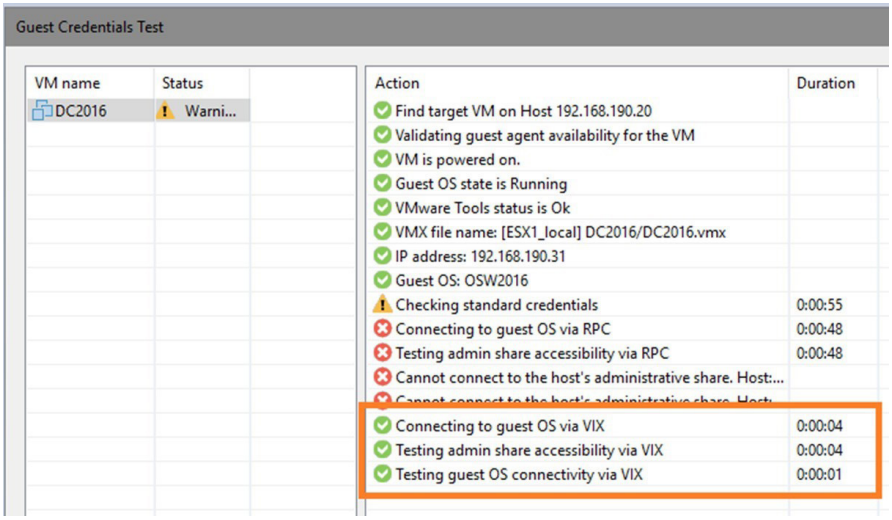

Figure 6 : Test des informations d'identification sur le SE client via l'API VIX

L'interaction avec les SE clients via l'API VIX ou vSphere ne fonctionne pas telle quelle. Les exigences sont détaillées dans l'article de la base de connaissances Veeam KB 1788. Celles-ci sont au nombre de deux :

- le compte utilisateur utilisé par Veeam doit être membre du groupe local des administrateurs ;
- si le nom du compte n'est pas « administrator », le contrôle de compte d'utilisateur Windows doit être désactivé.

Si la connexion RPC ne fonctionne pas, le mode de rechange est l'interaction avec les SE clients via l'API VIX ou vSphere. De fait, dans les environnements où la plupart des VM ne peuvent pas être atteintes via RPC, les sauvegardes prendront plus de temps, car Veeam commence toujours par tenter une connexion RPC. Dans ce cas, il est possible de modifier l'ordre pour commencer par l'API VIX en utilisant la clé de registre suivante sur le serveur de sauvegarde ou le proxy d'interaction avec le SE invité :

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Veeam\Veeam Backup and Replication\ DWORD: InverseVssProtocolOrder
Value = 1
La valeur pour désactiver cet ordre est 0 (comportement par défaut).

Il est important de noter que l'utilisation de l'API VIX ou vSphere pour interagir avec les SE invités limite les opérations de restauration. Il est ainsi possible de restaurer des fichiers, mais pas des objets applicatifs comme ceux d'Active Directory ou d'Exchange, par exemple. Pour ce faire, une connexion réseau est nécessaire. En outre, la restauration des fichiers est bien plus lente via le réseau.

En parlant de vitesse, le service VeeamLogShipper qui achemine les journaux SQL peut également utiliser l'API VIX comme mécanisme de rechange s'il n'arrive pas à atteindre la cible via le réseau. Si cela peut s'avérer trop lent dans la plupart des environnements, il est néanmoins recommandé d'acheminer les journaux SQL via le réseau.

Meilleure pratique : Prenez les limites en considération pour interagir avec les SE invités via l'API VIX ou vSphere.

Conclusion

Veeam Backup & Replication et VMware vSphere sont généralement prêts à fonctionner ensemble. Il existe toutefois quelques meilleures pratiques qui rendent leur association encore plus efficace. Celles-ci sont faciles et rapides à configurer.

Meilleure pratique : Consultez le guide des meilleures pratiques Veeam Backup & Replication Best Practices si vous envisagez un déploiement complexe ou de plus grande envergure.

À propos de l'auteur

Hannes Kasparick est un professionnel du secteur de l'IT depuis 2004. Il fait actuellement partie de l'équipe de gestion des produits Veeam. Par le passé, il a géré des environnements Linux et Windows, ainsi que des services d'infrastructure comme des serveurs, des stockages, des réseaux et des pare-feux.

À propos de Veeam Software

Veeam® est le leader des solutions de sauvegarde pour la gestion des données dans le cloud « Cloud Data Management™ ». Veeam offre une plateforme unique qui permet de moderniser la sauvegarde, d'accélérer le cloud hybride et de sécuriser les données. Avec plus de 365 000 clients dans le monde, dont 81% d'entreprises du Fortune 500 et 66% des Forbes Global 2000, les scores de satisfaction client de Veeam sont 3,5 fois supérieurs à la moyenne du secteur d'activité. Son écosystème compte plus de 70 000 partenaires de distribution dans le monde, dont HPE, NetApp, Cisco et Lenovo comme revendeurs exclusifs. Veeam, dont le siège social est situé à Baar, en Suisse, possède des bureaux dans plus de 30 pays. Pour en savoir plus, visitez https://www.veeam.com/fr ou suivez @veeam_fr sur Twitter.