Votre parcours vers la résilience avec Veeam Kasten

Une feuille de route pour les 100 premiers jours et au-delà.

Ce guide accompagne les administrateurs IT dans le déploiement, la configuration et la mise en œuvre de Veeam Kasten *pour Kubernetes*. Qu'il soit installé via Helm ou Marketplace, le chemin de déploiement est conçu pour être rapide, sécurisé et accessible. Au jour 100, vous disposez d'un environnement de sauvegarde natif Kubernetes avec des exportations hors site inaltérables intégrées à vos outils et applications, ainsi que d'un runbook de restauration documenté.

Votre parcours de 100 jours

PHASE 1 **Fondation** **Jours 1 à 14**	**PHASE 2** **Renforcer les bases** **Jours 15 à 45**	**PHASE 3** **Optimiser et durcir** **Jours 46 à 75**	**PHASE 4** **Démontrer la valeur** **Jours 76—100**
M1 : Dimensionnement et planification	M4 : Gestion centralisée	M7 : Intégration de l'observabilité	M10 : Test de restauration
M2 : Déployer Veeam Kasten	M5 : Traitement prenant en charge les applications	M8 : Résilience améliorée	M11 : Documentation et reporting
M3 : Premières tâches de sauvegarde	M6 : Meilleures pratiques en matière de politiques	M9 : Combler les lacunes de couverture	M12 : Hygiène continue

Feuille de route en bref

Phase	Nom	Chronologie	Objectif
PHASE 1	Fondation	Jours 1 à 14	Planification de l'environnement, déploiement de Veeam Kasten et exécution des premières tâches de sauvegarde.
PHASE 2	Renforcer les fondamentaux	Jours 15 à 45	Gestion centralisée, traitement prenant en charge les applications et meilleures pratiques en matière de politiques.
PHASE 3	Optimiser et renforcer	Jours 46 à 75	Observabilité, résilience et reprise après sinistre (DR), et comblement des écarts de couverture.
PHASE 4	Prouver la valeur	Jours 76 à 100	Tests de restauration, documentation et hygiène continue.

Comment utiliser ce guide

Les jours sont des lignes directrices, pas des délais stricts. Les petits environnements peuvent réduire la Phase 1 à une semaine, tandis que les environnements complexes peuvent prolonger la Phase 3.

Chaque étape s'appuie sur la précédente ; il est donc recommandé de suivre les étapes dans l'ordre.

Des encadrés tout au long du guide mettent en avant les points de décision, les options d'architecture et les pièges courants qui méritent d'être pris en compte.

Sommaire

PHASE 1 • Jours 1 à 14

Fondation

Objectif : infrastructure dimensionnée, déployée et premiers workloads protégés.

Étape 1 : dimensionnement et planification

Avant de déployer quoi que ce soit, investissez du temps dans la planification. La plupart des difficultés liées au déploiement d'un environnement stable et bien protégé peuvent être évitées en accordant une attention particulière à cette étape.

Inventaire des workloads

- Documentez le workload total et le nombre de machines virtuelles (VM), l'empreinte des données (par exemple, taille des volumes ou nombre de fichiers) et le taux de modification quotidien estimé.
- Identifiez vos workloads stratégiques. Ces éléments déterminent vos objectifs de restauration (délai optimal de reprise d'activité et objectif de temps de restauration (RPO/RTO)).
- Recensez les bases de données et les workloads qui pourraient bénéficier d'un traitement prenant en charge les applications.

Dimensionnement et planification du déploiement Veeam Kasten

- Veeam Kasten présente une configuration requise minimale configuration requise et les valeurs par défaut sont généralement suffisantes.
- Choisissez votre méthode de déploiement, soit Marketplace/Operator (recommandé si possible), soit Helm. Il est possible de changer de méthode après l'installation si nécessaire.
- Vérifiez que votre version de Kubernetes est compatible avec la dernière version de Veeam Kasten. Si ce n'est pas le cas, vous devrez d'abord effectuer la mise à niveau ou utiliser une version plus ancienne.
- Déterminez si cet environnement est entièrement isolé. Si tel est le cas, il faudra peut-être transférer les images Veeam Kasten vers un registre local disponible hors ligne via la place de marché de votre fournisseur, ou demander que notre registre soit ajouté à la liste blanche.
- Planifiez votre réseau de sauvegarde en isolant le trafic de sauvegarde sur un VLAN dédié constitue une meilleure pratique de sécurité, et elle est possible avec Kubernetes en fonction de votre CNI.

Helm VS marketplace

Helm : c'est l'option la plus flexible et la plus compatible avec toutes les distributions Kubernetes.

Marketplace/Operator : le cycle de vie de déploiement et de mise à niveau est plus simple et prend en charge les mêmes paramètres de personnalisation que Helm. Il est aussi fréquemment utilisé avec Red Hat OpenShift.

Le compromis : il existe un délai potentiel dans la réception des nouvelles versions via la place de marché. Les mises à jour sont disponibles immédiatement sur Helm, mais les fournisseurs de la place de marché retardent souvent les nouvelles versions d'un ou plusieurs jours pour validation.

Architecture de stockage des workloads

- **Stockage compatible avec les snapshots :** Veeam Kasten est compatible avec pratiquement tous les pilotes de stockage CSI prenant en charge les snapshots, ainsi qu'avec les intégrations de stockage directes.
- **Autres stockages (par exemple, NFS générique, disque local, etc.) :** Veeam Kasten peut tout de même protéger ces workloads, mais l'absence de véritable fonctionnalité de snapshot affecte la fiabilité et la performance des sauvegardes. Nous vous recommandons fortement d'effectuer une mise à niveau vers l'utilisation de volumes avec des fonctionnalités de snapshot, mais GSB **ou** NFS tar peuvent être utilisés si vous acceptez leurs limitations inhérentes.

Architecture du stockage de sauvegarde : aperçu des options

Le choix du stockage façonne la résilience et la disponibilité de vos données de sauvegarde. Voici un aperçu général des avantages et inconvénients de chaque type de stockage de sauvegarde que vous pouvez configurer en tant que profil d'emplacement.

Veeam Kasten + Veeam Vault

Les snapshots sont exportés vers un stockage objet immuable, logiquement entièrement isolé, hors site, via Veeam Vault. Aucune configuration avancée ni maintenance n'est nécessaire.

Veeam Kasten + cible Veeam Backup & Replication

Les snapshots sont exportés vers l'infrastructure gérée par Veeam Backup & Replication, y compris les Veeam Hardened Repositories et les Scale-out Backup Repositories (SOBRs). Le mode bloc est requis. **Remarque :** Les versions antérieures à la version 9.x requièrent également un petit profil d'emplacement supplémentaire (Vault/Object/NFS/CIFS) pour les métadonnées.

Veeam Kasten + Stockage objet

Les snapshots sont exportés vers un stockage objet (S3, cloud, par exemple) qui doit être configuré pour être hors site et inaltérable.

Veeam Kasten + NFS/CIFS

Les snapshots exportés directement vers NFS/CIFS ne sont généralement pas immuables, même sur des dispositifs compatibles WORM, car une gestion des versions serait nécessaire pour fonctionner. Cette option est entièrement prise en charge, mais n'est conseillée que si vous disposez également de duplications ou de copies immuables hors site.

Veeam Kasten + plusieurs profils de localisation

Les snapshots sont exportés vers 2 emplacements ou plus. Si elle est conçue correctement, en utilisant au moins une option immuable, cette solution peut s'avérer la plus résiliente. **Remarque :** Pour les versions antérieures à la 9.x, plusieurs politiques sont nécessaires, avec un profil d'emplacement par politique.

Les modes de stockage déterminent les fonctionnalités.

Selon votre type de stockage, les options suivantes sont disponibles :

Mode Volume : fichier ou Bloc. Les deux sont compatibles avec Veeam Kasten (par ex. Ceph FS ou RBD).

Mode d'exportation : fichier ou bloc. Les deux sont possibles avec Veeam Kasten.

Si un volume est en mode bloc, vous pourrez peut-être exporter vos snapshots en mode bloc. Cela offre des fonctionnalités spéciales, comme le CBT (lorsqu'il est disponible) et l'exportation vers une cible Veeam Backup & Replication.

Utilisation de Veeam Backup & Replication + Veeam Infrastructure Appliance (VIA) comme cible renforcée

Pour ceux qui ne disposent pas d'un stockage inaltérable existant, intégrer Veeam Kasten à Veeam Backup & Replication et déployer VIA peut constituer une approche raisonnable pour atteindre l'immutabilité locale.

Une cible renforcée fournit des sauvegardes locales immuables, ce qui empêche les ransomwares de les chiffrer ou de les supprimer pendant la période de rétention. Le SE est renforcé contre les accès non autorisés et devrait idéalement s'exécuter sur un serveur physique protégé plutôt que sur une VM.

Traditionnellement, une cible renforcée nécessite d'installer et de renforcer manuellement une distribution Linux. VIA supprime entièrement cet obstacle puisqu'il est renforcé à l'avance et se déploie via une image ISO amorçable. Elle peut également être déployée par l'utilisateur sur du matériel compatible ou achetée auprès d'un fournisseur en tant qu'appliance certifiée.

Étape 2 : déployer Veeam Kasten

Déployer Veeam Kasten

- Utilisez l'outil de pré-vérification pour vérifier que les prérequis sont remplis (facultatif).
- Méthode Marketplace/opérateur : consultez les instructions détaillées ici.
- Méthode Helm : consultez les instructions détaillées ici.

Intégration de l'accès au tableau de bord et de l'authentification

- Pour accéder au tableau de bord en externe, ajoutez un ingress ou une route à Veeam Kasten.
- Il est conforme aux meilleures pratiques d'intégrer le fournisseur d'authentification de votre distribution (par exemple, OpenShift Auth), mais d'autres options comme l'utilisation directe de LDAP sont également possibles.
- Une fois le tableau de bord Veeam Kasten visible, vous pouvez passer aux étapes ci-dessous.

Connecter l'infrastructure à Veeam Kasten

- Le cas échéant, (vSphere/cloud/autres) ajoutez un profil d'infrastructure pour une intégration de stockage directe.
- Ajoutez un profil d'emplacement pour définir la destination de votre sauvegarde.

Étape 3 : premières tâches de sauvegarde

Sauvegardes dans les environnements Kubernetes

Les snapshots de baie de stockage sont une fonctionnalité puissante que Kubernetes comprend et peut gérer nativement, à condition que votre provisionneur de stockage les prenne en charge.

Veeam Kasten exploite cette fonctionnalité ou une intégration directe pour déclencher des snapshots qui résident localement sur le périphérique de stockage. Veeam Kasten peut alors utiliser ces snapshots pour exporter de manière fiable les données vers un profil d'emplacement externe (par exemple, NFS, S3, dépôt VBR, coffre-fort, etc.).

Cette méthode offre une rapidité et une cohérence maximales, tout en tirant parti des fonctionnalités et des API natives de Kubernetes pour une compatibilité optimale.

Ce dont vous avez besoin pour démarrer

Veeam Kasten, en tant qu'application native Kubernetes, nécessite que l'utilisateur chargé de l'installation dispose d'un accès kubectl à l'environnement cible, de privilèges d'administrateur du cluster et, idéalement, d'un accès à l'interface de gestion de votre distribution, si elle existe.

Conseil : si vous rencontrez des erreurs, des solutions sont disponibles sur notre Communauté et Base de connaissances.

- En savoir plus sur la protection des VMs KubeVirt, le cas échéant dans votre environnement.
- Créez votre première stratégie de sauvegarde et ciblez votre profil d'emplacement.
- Définissez une stratégie de rétention pertinente pour démarrer : 1 snapshot local quotidien, avec exportation vers le profil d'emplacement selon une rétention de 1 quotidien, 4 hebdomadaires et 3 mensuelles.
- Planifiez la tâche pour qu'elle s'exécute pendant les heures creuses et vérifiez qu'elle n'entre pas en conflit avec d'autres fenêtres de maintenance.
- Exécutez la tâche manuellement lors de la première exécution et surveillez-la jusqu'à son terme.
- Vérifiez que la tâche s'est achevée sans avertissement ni erreur avant de passer à la phase 2.

Votre premier test de restauration : ne sautez pas cette étape !

Avant de passer à la phase 2, effectuez une restauration sur une application non critique afin de confirmer la capacité de restauration.

Vous n'êtes pas protégé tant que vous n'avez pas vérifié votre capacité à restaurer. Cela ne prend que quelques minutes et peut vous éviter des jours de problèmes par la suite.

Local vs exportation

N'oubliez pas que les snapshots sont locaux uniquement sur votre périphérique de stockage. Cela signifie que :

- Ce ne sont pas de véritables sauvegardes.
- Plus de snapshots locaux sont conservés, plus de stockage principal est consommé.

Ainsi, il est important d'exporter les snapshots vers un profil d'emplacement, qui peut avoir une stratégie de rétention configurée indépendamment.

Lors de l'exportation des snapshots, toutes les données sont automatiquement dédupliquées, compressées, chiffrées et enregistrées de façon incrémentale.

PHASE 2 • Jours 15 à 45

Renforcer les bases

Objectif : protection constante, copie hors site et visibilité dans l'ensemble de votre environnement.

Étape 4 : gestion centralisée (MCM)

Le gestionnaire multicluster (MCM) permet une visibilité et une gestion centralisées de plusieurs clusters. Dans chaque cluster, Veeam Kasten sera installé pour protéger les workloads et les instances pourront être reliées entre elles.

- Une fois qu'un autre cluster exécutant Veeam Kasten a été déployé, définissez une instance Kasten comme Primary et utilisez un jeton d'association pour les relier (instructions). Assurez-vous que les certificats auto-signés sont approuvés pour éviter les erreurs.
- Affichez tous les clusters joints via le MCM « tableau de bord ».
- Définissez des politiques globales et des profils globaux si vous souhaitez disposer d'une configuration cohérente dans l'ensemble de votre environnement.
- Ajoutez votre clé de licence d'entreprise au cluster MCM principal. Les licences seront distribuées de manière transparente à tous les autres clusters, sans qu'aucune autre configuration ne soit nécessaire.

Étape 5 : traitement prenant en charge les applications

Le traitement prenant en charge les applications à l'aide des Blueprints Kanister garantit que les sauvegardes cohérentes en cas d'incident deviennent cohérentes au niveau des applications ou sont exportées logiquement. Ceci est essentiel pour les bases de données telles que PostgreSQL, MongoDB, MySQL, Elastic, et autres.

- Discutez des exigences de l'application et de l'accès à l'application avec votre équipe d'application.
- Trouvez des exemples de schéma préconçus que vous pouvez personnaliser, ou créez votre propre schéma.
- Ajoutez le schéma à Veeam Kasten.
- Associez le schéma aux workloads manuellement ou en créant une liaison de schéma.
- Testez une sauvegarde et une restauration au moyen de votre schéma pour vérifier la restauration des applications de bout en bout.

Types de sauvegardes

Cohérence en cas d'incident (par défaut) : ce type de sauvegarde capture le système de fichiers entier à un instant précis, généralement via des snapshots du fournisseur de stockage. C'est plus cohérent sur le plan des données que la simple copie de fichiers, mais des écritures en cours de transfert ou des transactions non vidées peuvent néanmoins être ignorées.

Cohérence au niveau des applications : ce type de sauvegarde suspend en principe brièvement l'application au moyen des outils natifs de celle-ci pour que toutes les données soient écrites sur le volume avant la création du snapshot.

Logique : ce type de sauvegarde utilise les outils natifs de l'application pour créer un vidage logique ou une exportation de ses données sous forme de fichier. Celle-ci est souvent transférée vers un emplacement externe tel que S3 au lieu du volume lui-même.

Les schémas sont puissants et infiniment flexibles. De plus, grâce à sa nature open source, vous pouvez créer un schéma pour n'importe quelle application ou flux de travail s'il n'en n'existe pas.

Étape 6 : meilleures pratiques en matière de politiques

- Dans cette étape, vous allez créer des jobs supplémentaires pour protéger tous vos workloads et utiliser des paramètres avancés pour garantir leur fiabilité.

Meilleures pratiques (pour la plupart des scénarios)

- Utilisez plusieurs jobs avec des étiquettes pour sélectionner les applications, au lieu d'une politique générique protégeant tout.
- Utilisez des stratégies basées sur les VM plutôt que sur les espaces de noms lorsque vous protégez des VM KubeVirt.
- Si vous souhaitez sauvegarder des ressources à l'échelle du cluster, créez une politique distincte pour ces sauvegardes uniquement.
- Définissez une fenêtre de sauvegarde pour garantir que les workloads de production ne soient pas impactés pendant les heures critiques.
- Envisagez de planifier les tâches de manière échelonnée pour améliorer les performances.
- Configurez la protection de la sauvegarde inaltérable.
- Exclusions / filtres de ressources si nécessaire.
- (Facultatif) ressources globales, préréglages de stratégie

Autres conseils

Pour les tâches exécutées manuellement, à moins qu'un délai d'expiration ne soit spécifié, tous les artefacts devront être supprimés manuellement.

Même si la tâche a été configurée à l'aide de l'heure locale, toutes les heures sont converties en UTC et les programmations de politique ne changent pas pour l'heure d'été.

Vérifiez vos calculs ! Le calcul de la rétention n'est pas toujours évident. Par exemple, conserver 24 snapshots à l'heure (au total) à des intervalles de 15 minutes ne permettra de conserver que 6 heures de snapshots, et non 24 heures.

PHASE 3 • Jours 46 à 75

Optimisation et renforcement

Objectif : combler les lacunes de protection, optimiser le RTO/RPO et renforcer la visibilité.

Étape 7 : intégration de l'observabilité

- Activez l'intégration Red Hat ACM Observability, le cas échéant.
- Exportez les métriques vers des systèmes de supervision externes (p. ex., Grafana, Datadog, Thanos, etc.).
- Créez des alertes et des tableaux de bord au sein de vos systèmes de supervision (exemple : Grafana).
- Activez le reporting.

Étape 8 : résilience et DR améliorée

La sauvegarde de tous les workloads doit également inclure une sauvegarde de Veeam Kasten lui-même, ce qui peut être réalisé par Kasten Disaster Recovery (KDR). Il ne faut pas assimiler cela à la mise en place d'un environnement DR ou d'un PRA ; ces éléments devraient être considérés en fonction du niveau de résilience nécessaire.

KDR (sauvegarde du catalogue Veeam Kasten)

- Activez Kasten DR : cela permet de sauvegarder le catalogue de sauvegarde Veeam Kasten afin que les restaurations soient possibles même si l'installation Kasten n'est plus accessible. C'est important, car les fichiers de sauvegarde Veeam Kasten ne sont pas autonomes et nécessitent le catalogue ainsi que la clé de chiffrement pour être restaurés.
- Configurez Kasten DR sur « Export local catalog snapshots » et sauvegardez les informations suivantes dans un emplacement sécurisé : phrase secrète, ID du cluster, détails du profil d'emplacement KDR et informations d'identification.

DR pour vos workloads

- Déterminez le niveau de résilience nécessaire en fonction de vos RTO/RPO souhaités.
- Si un RTO/RPO de plus d'un jour est acceptable, disposer uniquement de sauvegardes et reconstruire l'environnement selon les besoins peut constituer une solution raisonnable.
- Si les RTO/RPO doivent se mesurer en heures ou en minutes, il faut porter une attention particulière à la conception du plan. Quelques exemples sont donnés ci-dessous.

Exemples de configurations DR (en fonction des RTO/RPO requis)

- **Application non protégée :** aucun point de restauration (c'est-à-dire pas de snapshots ou d'exportations locaux).

  Résultat : pas de restauration possible.

- **Exportation uniquement :** les exportations de KDR et les points de restauration exportés existent dans un profil d'emplacement hors site.

  Résultat : pour restaurer, reconstruisez d'abord un environnement Kubernetes, installez Veeam Kasten, restaurez le catalogue Kasten, puis restaurez les applications à partir des points de restauration exportés.

- **Environnement DR + importation :** Veeam Kasten est installé et une stratégie d'importation s'exécute régulièrement pour importer les points de restauration dans un catalogue local.

  Résultat : les points de restauration sont visibles à l'emplacement secondaire et prêts à être restaurés. Des ressources minimales sont consommées jusqu'à ce qu'elles soient nécessaires.

- **Environnement de DR + Importation + Restauration, échelle à zéro :** Veeam Kasten est installé, la politique d'importation et de restauration s'exécute régulièrement pour importer les points de restauration dans un catalogue local, puis restaurer les applications dans l'environnement Kubernetes. Les applications sont alors restaurées, mais avec Transforms mettant tous les réplicas à 0 pour chaque workload.

  Résultat : les applications sont restaurées dans Kubernetes (via les pods, les PV, tout ce qui a été sélectionné). Cependant, le nombre de réplicas est égal à 0, donc seules des ressources minimales sont consommées jusqu'à ce qu'elles soient nécessaires, hormis le stockage.

- **DR environnement + Importation + restauration, complet :** Veeam Kasten est installé, la politique d'importation et de restauration s'exécute régulièrement pour importer les points de restauration dans un catalogue local, puis restaurer les applications dans l'environnement Kubernetes.

  Résultat : les applications sont restaurées dans Kubernetes (via les pods, les volumes persistants, tout ce qui a été sélectionné), fonctionnant exactement comme en production et prêtes à être pleinement utilisées.

Planification des catastrophes

Veeam Kasten est indépendant de toute distribution, ce qui signifie qu'il peut restaurer vers et depuis n'importe quelle distribution Kubernetes, y compris entre des distributions complètement différentes comme Tanzu et Azure. Cependant, les restaurations nécessitent qu'un environnement Kubernetes fonctionnel soit en place ; Kasten ne peut pas s'auto-amorcer. Veillez à établir un plan de reprise d'activité afin d'être prêt en cas d'incident et vérifiez régulièrement qu'il répond à vos objectifs.

Étape 9 : ajustement fin

- **Consultez le tableau de bord Veeam Kasten :** traitez tous les workloads non protégés avant d'effectuer tout autre paramétrage.
- **Examinez les plannings des tâches pour détecter les conflits :** échelonnez les heures de démarrage afin d'éviter la contention des ressources.
- Vérifiez que toutes les tâches s'effectuent dans les limites de la fenêtre de sauvegarde définie.
- **Validez la conformité RPO :** tous les workloads stratégiques génèrent-ils des points de restauration dans votre fenêtre de restauration cible ?
- Confirmez que tous les workloads sont exportés vers au moins un emplacement immuable.
- Activez Garbage collection pour supprimer les anciennes actions peut améliorer les performances du catalogue.
- Testez votre processus de mise à niveau ! De nouvelles versions de Veeam Kasten sont publiées environ toutes les deux semaines.

PHASE 4 • Jours 76 à 100

Démontrez la valeur et opérationnalisez

Objectif : vérifier la capacité de restauration, établir une hygiène continue et démontrer le ROI.

Étape 10 : tests de restauration

La seule sauvegarde qui compte est celle dont vous pouvez restaurer les données. La phase 4 est celle où vous démontrez, preuves documentées à l'appui, que votre environnement respecte ses engagements en matière de RTO et de RPO.

Tests de restauration granulaire et complète

- Testez la restauration d'un namespace complet ou d'une VM à partir d'un export. Simulez une perte totale sur site pour valider votre copie hors site.
- Testez la restauration d'objets applicatifs : restaurez une base de données et exécutez des requêtes pour vérifier que vos données sont intactes.
- Testez la restauration au niveau fichier (si souhaité) : restaurez des fichiers individuels depuis une exportation vers un emplacement de test.
- Testez votre PRA de bout en bout, notez les éventuels problèmes à améliorer et documentez en détail le processus afin de garantir que votre plan et son accès sont disponibles.
- Enregistrez les temps de restauration réels et comparez-les à vos objectifs de RTO. Documentez les résultats.

Meilleures pratiques pour les tests de restauration

Restaurez toujours vers une cible hors de production et n'écrasez jamais les workloads actifs pendant un test.

Documentez ce qui a été restauré, à partir de quel point de restauration, sur quelle cible et combien de temps cela a pris.

Ces résultats constituent la preuve de votre capacité de restauration. Conservez-les pour vos besoins d'examens de conformité, d'audits et de reporting de gestion.

De plus, si vous effectuez une restauration au sein du même environnement, même vers des espaces de noms différents, sachez que certaines ressources (notamment les services réseau) peuvent entrer en conflit. Assurez-vous d'examiner votre configuration avant de restaurer, restaurez vers un environnement différent, et/ou utilisez les Transforms pour éviter les conflits.

Restauration dans différents environnements

Si vous restaurez vers ou à partir de différents sites, distributions Kubernetes, plateformes ou autres, les Transforms peuvent être utiles pour modifier facilement votre configuration lors de la restauration. Par exemple, si vous modifiez les chemins réseau de la production vers la DR, ou si vous changez des classes de stockage. Aucun changement manuel n'est nécessaire pour que vos restaurations s'exécutent immédiatement avec une configuration modifiée ou dans un nouvel environnement.

Étape 11 : documentation et rapports

- Activez le reporting, si cela n'a pas déjà été fait.
- Documentez votre architecture de sauvegarde finale, y compris la liste des stratégies, les emplacements d'exportation, les planifications et les stratégies de rétention.
- Examinez la consommation de stockage Veeam Vault et confirmez que votre utilisation correspond à votre budget prévisionnel.
- Archivez les résultats des tests de restauration avec la documentation de l'architecture.

Étape 12 : établir une cadence d'hygiène continue

Au 100e jour, votre environnement devrait être stable et entièrement documenté. Ces habitudes permettent de maintenir cet état :

- **Chaque semaine :** passez en revue le tableau de bord Veeam Kasten et examinez les tâches ayant échoué ou signalées par un avertissement avant qu'elles ne s'accumulent.
- **Mensuel :** passez en revue les dernières versions de Kasten et effectuez des mises à jour régulières.
- **Chaque trimestre :** réalisez un test de restauration documenté et alternez les types de workload testés.
- **Annuellement :** évaluez votre architecture de sauvegarde au regard des besoins actuels de l'entreprise.
- **Avant le renouvellement :** vérifiez l'utilisation des licences dans votre tableau de bord Kasten (par exemple, le total via MCM ou dans chaque cluster individuellement) pour confirmer que vous êtes dans les limites de vos droits.

Prochaines étapes

Vous en voulez davantage ?

- Visitez Veeam University
- Découvrez les témoignages de réussite de vos homologues
- Contactez l'équipe Customer Success
- Partagez votre histoire de résilience des données avec Veeam

Annexe : référence rapide

Composants clés : intégration Veeam

- **Appliance logicielle Veeam (VSA) :** appliance durcie avec Veeam Backup & Replication préinstallé. Déploiement sous forme d'OVA (VM) ou d'ISO (physique). Peut lui-même servir de cible inaltérable limitée ou fonctionner avec d'autres appliances ou stockage de sauvegarde, y compris des VIA dédiés.
- **Veeam Infrastructure Appliance (VIA) :** une appliance pré-durcie déployée en tant que cible renforcée dédiée ou pour d'autres rôles. Fournit une inaltérabilité locale sans expertise Linux. Un rôle par appliance.
- **Veeam Backup & Replication :** moteur de sauvegarde principal, hébergé sur le VSA. Gère les tâches, les cibles, les proxys et les opérations de restauration.
- **Scale-Out Backup Repository :** structure logique associant un niveau de performance local (par exemple VIA) et un niveau de capacité (par exemple Vault/S3/NFS) pour former une seule cible de sauvegarde.
- **Veeam Vault :** stockage objet cloud immuable pour les copies hors site. Elle est gérée par Veeam, aucun compte cloud distinct n'est requis.

Termes clés

- **RPO :** pertes de données maximales acceptables, mesurées en temps. Détermine la fréquence des sauvegardes.
- **RTO :** temps d'arrêt maximal acceptable avant qu'un workload ne doive être restauré.
- **Inaltérabilité :** données de sauvegarde impossibles à modifier ou à supprimer pendant une période de rétention définie. Protège contre le chiffrement des fichiers de sauvegarde par les ransomwares.
- **Cible renforcée Veeam :** une cible de sauvegarde Linux avec immutabilité appliquée au niveau de l'OS. Fourni prêt à l'emploi par VIA sans administration Linux requise.
- **KubeVirt :** projet open source permettant à Kubernetes d'exécuter et de gérer des VM parallèlement à des workloads conteneurisés. Cela permet aux VM de s'exécuter sur des plateformes Kubernetes telles que OpenShift Virtualization et SUSE Harvester, qui peuvent être protégées par Veeam Kasten.
- **Traitement prenant en charge les applications :** traitement qui crée des points de sauvegarde cohérente de l'application, ce que Veeam Kasten peut réaliser en utilisant des schémas.
- **Schéma :** les schémas Kanister sont un mécanisme open source permettant de décrire des tâches personnalisées pour la gestion des données au niveau application sur Kubernetes.

Ressources utiles

- Centre d'assistance Veeam
- Portail client Veeam (téléchargements)
- Forums de la communauté Veeam
- Articles de la base de connaissances Veeam
- Documentation Veeam Kasten
- Documentation Kanister Blueprints

À propos de Veeam Software

Veeam, la référence en matière de confiance dans les données et l'IA, est une société spécialisée dans l'aide aux organisations pour garantir que leurs données et leur IA sont pleinement comprises, sécurisées et résilientes, afin de pouvoir accélérer leur innovation en matière d'IA sécurisée à grande échelle. En tant que leader du marché en matière de résilience des données et de gestion de la posture de sécurité des données, Veeam est conçu pour la convergence de l'identité, des données, de la sécurité et des risques liés à l'IA.

Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 82 % des entreprises du Fortune 500,

Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.