Commvault

Cloud Rewind™
Formerly Appranix

eBOOK

Atteignez la Résilience des Applications Cloud avec des Récupérations Hyper-rapides

Commvault

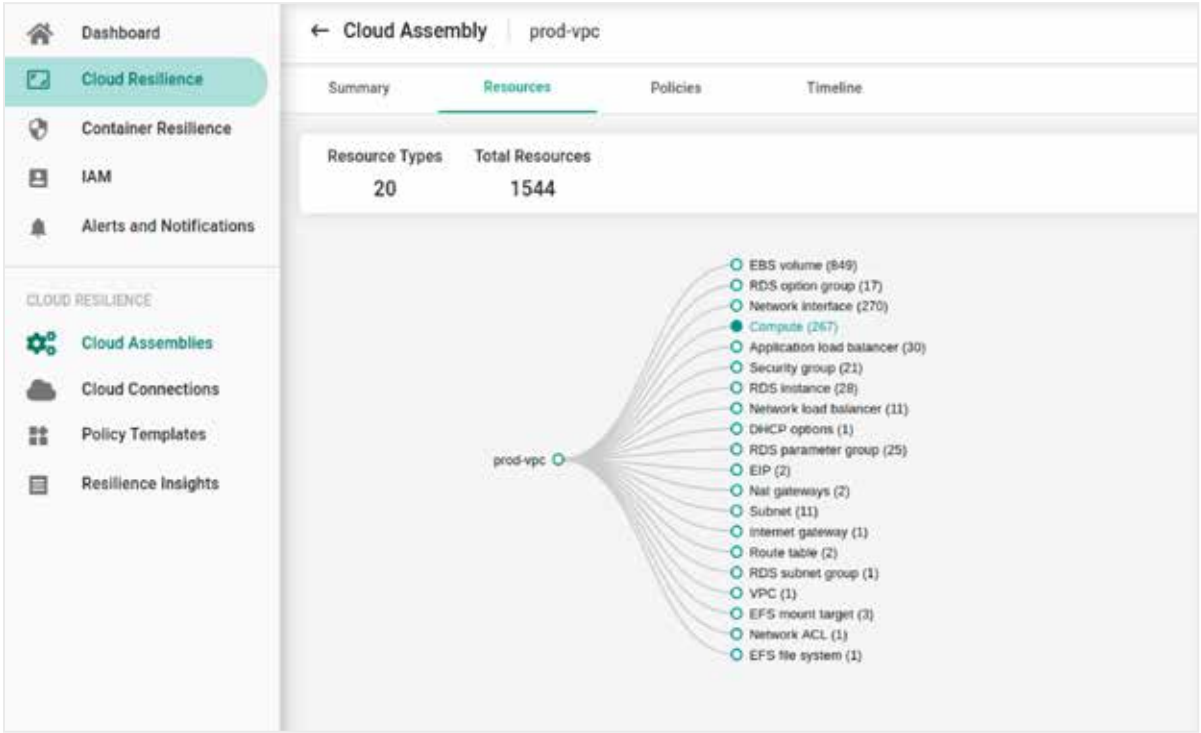
Table des matières

RÉCUPÉRATION HYPER-RAPIDE DES ENVIRONNEMENTS D'APPLICATIONS CLOUD

Les organisations cloud ont rapidement adopté un modèle d'exploitation décentralisé pour leurs applications et services. Les architectures logicielles sont également devenues plus distribuées, utilisant des ressources cloud facilement accessibles dans différentes zones cloud. Les ingénieurs de la fiabilité des sites ont adopté des cycles de publication plus dynamiques et rapides grâce aux pratiques DevOps, afin de répondre aux exigences croissantes des clients. De plus, les ressources cloud programmables ont permis aux environnements de s'adapter automatiquement pour répondre aux exigences de performance des applications métier critiques.

Cependant, tous ces changements ont également créé d'énormes défis pour les équipes de services opérationnels partagés qui gèrent la résilience, la sécurité et les coûts. La question la plus urgente aujourd'hui, surtout compte tenu de la vulnérabilité accrue des environnements cloud aux cyberattaques, est de savoir comment ces environnements d'applications dynamiques et auto-évolués peuvent se rétablir rapidement en cas de temps d'arrêt, en utilisant l'infrastructure cloud native, afin de maintenir les SLA promis aux entreprises.

POURQUOI UN MODÈLE BCDR TRADITIONNEL DE CENTRE DE DONNÉES N'EST PAS ADAPTÉ AUX APPLICATIONS CLOUD



Les applications ne dépendent plus de quelques serveurs ou d'une seule base de données critique. Considérons l'exemple suivant d'une application cloud simple à trois niveaux avec un auto-scaling, composée de deux machines virtuelles et d'une base de données. Elle est constituée d'au moins vingt (20) types et instances de ressources cloud distincts. Les systèmes de sauvegarde et de récupération traditionnels étaient conçus pour protéger uniquement les disques des machines virtuelles, les bases de données et les systèmes de fichiers. Pour assurer la résilience de l'application cloud complète, toutes les ressources cloud doivent être protégées afin de pouvoir récupérer à tout moment et dans n'importe quelle région du cloud. Les systèmes de sauvegarde et de récupération hérités n'ont pas été conçus pour protéger toutes ces ressources cloud utilisées par des applications dynamiques, distribuées et auto-évoluées qui s'appuient sur une infrastructure cloud définie par logiciel.

LA PROLIFÉRATION DES RANSOMWARES MODIFIE LA RÉCUPÉRATION DES APPLICATIONS

Alors que les attaques par ransomware se multiplient et deviennent de plus en plus sophistiquées, les récupérations d'environnements cloud deviennent de plus en plus difficiles. Ce qui est encore plus important, c'est que les nouvelles attaques de ransomware ciblent les solutions de sauvegarde et leurs consoles de gestion. Comme la plupart des produits BCDR sont installés dans le même compte cloud que celui des systèmes de production, si une attaque de ransomware prend le contrôle de l'ensemble du compte cloud, il n'est même pas possible d'accéder aux consoles des systèmes de sauvegarde et de récupération pour pouvoir restaurer les environnements d'application. C'est peut-être l'un des modèles critiques que les organisations doivent reconsidérer lorsqu'elles repensent l'architecture de résilience des applications, et non seulement la sauvegarde et la récupération des données.

Comme les systèmes d'applications cloud sont composés de multiples services d'infrastructure cloud, les utilisateurs effectuant des récupérations après des attaques de ransomware ont besoin d'une compréhension considérable pour pouvoir reconstituer les machines virtuelles, les bases de données, les réseaux, de nombreux services cloud et les configurations associées afin de les restaurer correctement. Généralement, des composants clés des environnements d'application, tels que les réseaux privés virtuels (VPC), les équilibreurs de charge, les passerelles, les groupes de sécurité, les groupes de paramètres de base de données, etc., doivent être assemblés manuellement à l'avance par les équipes d'opérations cloud avant même d'engager les systèmes BCDR pour la récupération des données.

LA DÉCOUVERTE CONTINUE DES RESSOURCES CLOUD EST LA CLEF D'UNE MEILLEURE RÉSILIENCE

Les environnements cloud dynamiques et auto-évolués présentent d'énormes défis pour les équipes d'opérations afin de les maintenir sécurisés et résilients. Comme de nombreuses équipes de développement gèrent la majorité des ressources d'infrastructure cloud de manière autonome, les environnements d'applications cloud s'élargissent à un rythme plus rapide que dans le modèle traditionnel de centre de données. Ces environnements programmables et en constante évolution nécessitent un système capable de découvrir continuellement toutes les ressources appartenant à une application. Les organisations disposent également de nombreux comptes cloud pour isoler leurs environnements de développement, de production et de test en fonction de leurs besoins métier. Il n'est pas rare de nos jours de voir des organisations disposer de centaines de comptes cloud.

La complexité de nombreux comptes cloud, associée à des environnements en constante évolution, rend difficile pour les équipes centralisées de s'appuyer sur des systèmes de protection et de récupération traditionnels et non centrés sur les applications. En effet, ces systèmes se contentent de compter sur les utilisateurs pour sélectionner les bonnes ressources et appliquer manuellement la protection pour leurs applications. De leur côté, les développeurs d'applications ne suivent pas toutes les ressources d'infrastructure cloud utilisées pour leurs applications, ce qui les empêche d'aider les SREs (Site Reliability Engineers) au moment critique de la récupération. Généralement, plusieurs pipelines DevOps modifient les environnements cloud centraux, rendant encore plus difficile pour les SREs de récupérer les applications au moment où c'est le plus urgent. Il est donc nécessaire d'avoir un système qui découvre continuellement les ressources cloud et est centré sur les applications, avec la capacité de comprendre les ressources système grâce à une cartographie des dépendances automatisée pour protéger correctement toutes les ressources cloud pertinentes. Cela permet ensuite de récupérer rapidement ou de basculer les applications, les données, les configurations, l'état et les dépendances afin de respecter les exigences de disponibilité des applications.

SAUVEGARDEZ L'ÉTAT DE VOTRE ENVIRONNEMENT CLOUD AVEC UN SYSTÈME EN APPRENTISSAGE CONTINU.

Gartner estime qu'un environnement cloud typique subit plus de 50 modifications de configuration par jour. Il est crucial de créer un dépôt de métadonnées de configuration cloud immuable pour tous les environnements d'applications cloud critiques. Il est également très important d'héberger ces métadonnées de configuration dans un système de résilience des applications cloud situé sur un cloud différent pour obtenir des niveaux

supplémentaires de résilience. Ces coffres de métadonnées de configuration doivent être segmentables par services d'application et être journalisés pour une récupération à un point précis dans le temps, dans n'importe quelle région du cloud. Ils doivent être suffisamment granulaires pour permettre aux équipes d'opérations de demander une seule ressource à un moment précis, afin de pouvoir récupérer rapidement une instance particulière d'un service cloud en cas de panne. Un système en apprentissage continu est essentiel pour suivre les modifications, de sorte que, en cas de panne, les systèmes d'applications cloud distribués puissent être recréés en fonction de ce qui existait dans l'environnement de production. Un système de découverte continue et d'apprentissage des métadonnées élimine complètement la nécessité d'une évaluation manuelle et les risques associés à des métadonnées disjointes lors du processus de récupération.

RÉCUPÉRATIONS HYPER-RAPIDES DE L'ENSEMBLE DE L'ENVIRONNEMENT AVEC LA DR-AS-CODE

La partie la plus complexe de la récupération consiste à identifier les ressources appropriées de calcul, de stockage, de PaaS et d'infrastructure réseau correspondant à un ensemble d'applications, puis à les séquencer pour une récupération orchestrée. Cela est appelé un "Plan Technique de Récupération après Sinistre", ou TDP pour faire court. Il existe également un aspect non technique du plan de récupération après sinistre (DR) qui concerne l'apport de ressources humaines et organisationnelles pour la validation des applications après les récupérations.

Les TDPs sont généralement composés de plusieurs pages et nécessitent la collaboration de plusieurs personnes opérationnelles pour identifier ce qui fonctionne en production, en termes de configurations, de dépendances, de séquencement et de scripts. Les organisations qui ont utilisé des produits BCDR traditionnels vous diront à quel point les TDPs sont complexes et pourquoi elles ne réalisent pas souvent des tests de récupération.

Il est maintenant possible d'éliminer complètement les TDPs manuels grâce à un modèle d'infrastructure-as-code (IaC) automatisé. En particulier, pour des récupérations garanties, il est important d'utiliser un IaC natif cloud, plutôt qu'un IaC neutre cloud, afin que la responsabilité de la récupération de grands systèmes soit transférée au fournisseur cloud, qui dispose de ressources dynamiquement évolutives pour réussir les récupérations pendant une panne.

GESTION DES COPIES DE DONNÉES NATIVE CLOUD

Les plateformes cloud disposent de suffisamment de capacités de gestion des données pour pouvoir réaliser des copies de données beaucoup plus rapides pour les sauvegardes, la réplication et la récupération. Il n'est pas nécessaire d'ajouter des capacités de gestion des données supplémentaires provenant de fournisseurs tiers. Il n'est pas non plus nécessaire de modifier le format de stockage des données de l'application native en un format de sauvegarde de données commun, ni de passer par le processus long d'importation et d'exportation dans le système de fichiers de sauvegarde neutre.

Il est possible de créer des copies de données incrémentielles et cohérentes à partir de machines virtuelles et de bases de données pour réduire les coûts de sauvegarde et de reprise d'activité après sinistre (DR). Les services serverless disposent de suffisantes capacités de gestion des données intégrées pour éviter des copies coûteuses vers et depuis des plateformes de gestion des données ajoutées à un environnement cloud.

Les plateformes cloud hyperscale ont vraiment ouvert la voie à une résilience bien meilleure par rapport au modèle d'infrastructure de centre de données. Les organisations mondiales peuvent littéralement répliquer les données incrémentielles d'une région cloud à une autre en quelques minutes. Cela non seulement augmente la résilience des données, mais permet également de créer des copies multiples moins coûteuses à travers le monde, offrant ainsi de bien meilleurs niveaux de résilience des applications en cas de panne.

MACHINE À REMONTER LE TEMPS POUR L'ENVIRONNEMENT DES APPLICATIONS CLOUD

La Machine à remonter le Temps pour l'Environnement d'Application Cloud est un concept simple dans lequel un système automatisé peut rassembler toutes les métadonnées des ressources cloud centrées sur l'application à partir d'un coffre-fort, l'application à partir d'un dépôt immuable, et les données de l'application à partir du stockage et des bases de données pour une récupération synchronisée à un point précis dans le temps. On peut imaginer ces machines du temps comme des CMDB journalisés qui sont automatiquement mis à jour d'une perspective centrée sur l'application en utilisant toutes les capacités natives du cloud.

Cependant, la différence la plus importante entre une Machine du Temps Cloud et les anciens CMDB est qu'elle connaît les copies de données à un point précis dans le temps pour les applications. Au fil du temps, une machine du temps cloud devient inestimable pour les organisations, car de multiples groupes au sein d'une organisation peuvent facilement y accéder pour diverses opérations de retour en arrière, de récupération et de basculement. Les systèmes traditionnels de BCDR (Business Continuity and Disaster Recovery) n'ont jamais collecté les métadonnées des systèmes de manière à être utiles au-delà des simples exigences de sauvegarde de données.

RÉSUMÉ

La nature dynamique, la complexité et la rapidité des changements apportés aux applications cloud nécessitent vraiment un nouveau modèle de résilience centré sur l'application, plutôt que les modèles de protection et de récupération ou de récupération après sinistre hérités de l'ère des centres de données. Que les applications aient été migrées vers le cloud ou créées de manière native sur les plateformes cloud, ce nouveau modèle non seulement permet une récupération rapide de l'ensemble des environnements d'application en cas de multiples temps d'arrêt, mais réduit également considérablement les cauchemars opérationnels, en particulier lorsque des équipes d'opérations moins nombreuses gèrent une quantité beaucoup plus importante de ressources par rapport à la dernière décennie.

À PROPOS DE CLOUD REWIND™

Cloud Rewind offre une résilience des applications cloud avec une sauvegarde et une récupération de l'ensemble de l'environnement cloud, incluant toutes les ressources, services et dépendances, à n'importe quel point précis dans le temps et dans n'importe quelle région cloud.

Pour en savoir plus, visitez **commvault.com**