Protection des charges de travail sur GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Sommaire

Protection des charges de travail sur GCP/GCVE

Reprise d'activité cohérente avec les applications avec NetApp SnapCenter et Veeam Replication

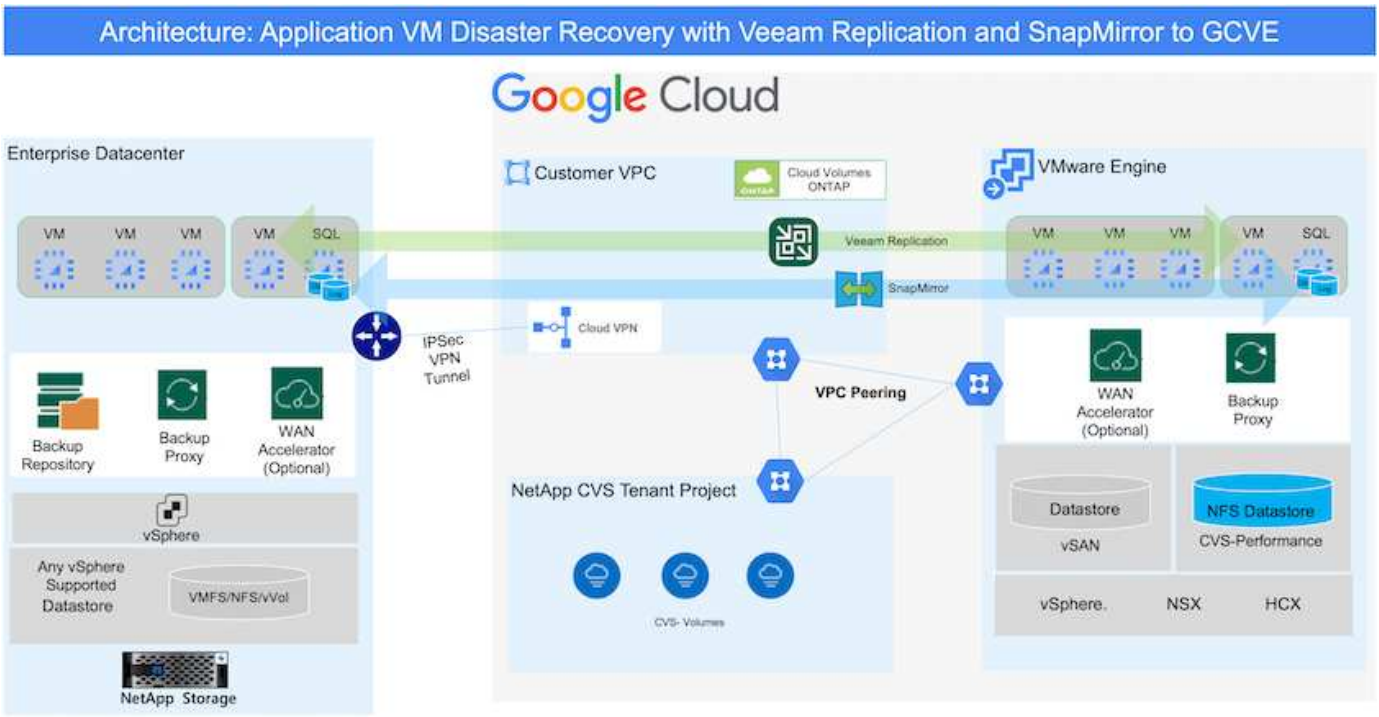
Auteurs : Suresh Thoppay, NetApp

Présentation

De nombreux clients recherchent une solution de reprise après incident efficace pour leurs machines virtuelles d'application hébergées sur VMware vSphere. La plupart d'entre eux utilisent leur solution de sauvegarde existante pour effectuer une restauration pendant les diaster.
La plupart du temps, cette solution augmente le RTO et ne répond pas à leurs attentes. Pour réduire les objectifs RPO et RTO, la réplication de machine virtuelle Veeam peut être utilisée même sur site vers GCVE dans la mesure où la connectivité réseau et l'environnement ne disposent pas des autorisations appropriées.
REMARQUE : Veeam VM Replication ne protège pas les dispositifs de stockage connectés invités d'une machine virtuelle, tels que les montages iSCSI ou NFS au sein de la machine virtuelle invitée. Ils doivent les protéger séparément.

Pour assurer une réplication cohérente avec les applications pour SQL VM et réduire l'objectif de durée de restauration, nous avons utilisé SnapCenter pour orchestrer les opérations snapmirror des volumes de bases de données et de journaux SQL.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des

sauvegardes cohérentes au niveau des applications.

> Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d'activité

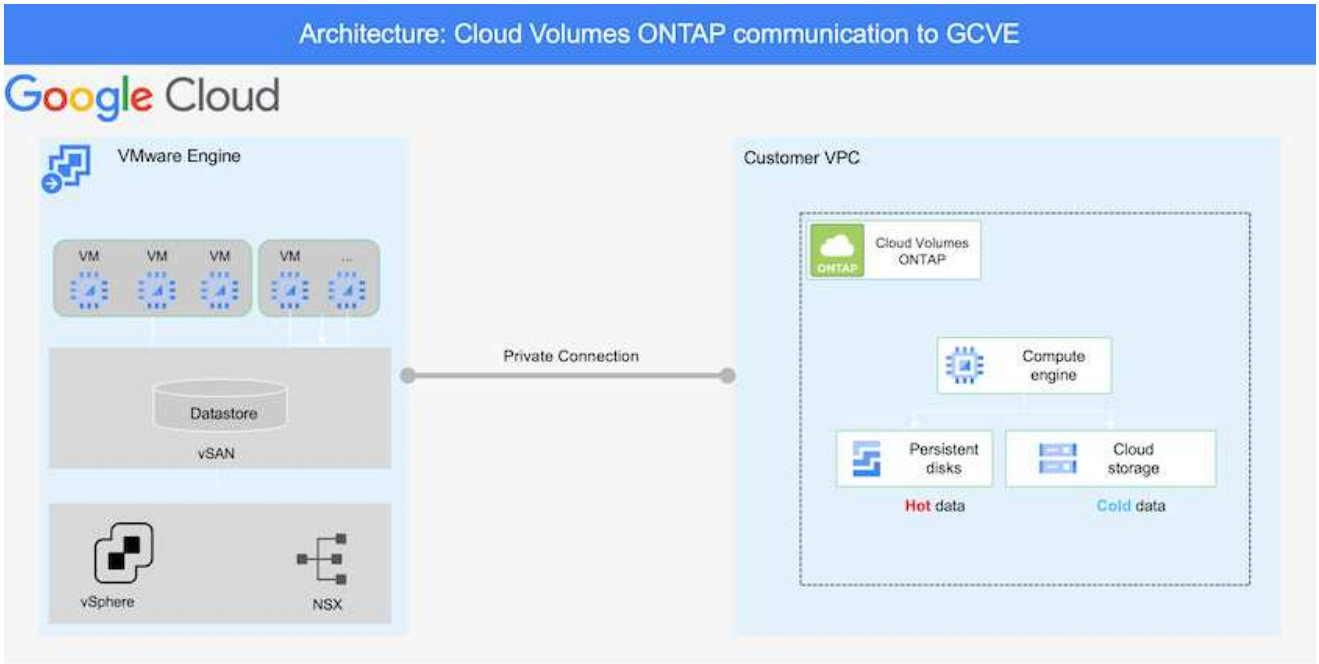
Présentation du déploiement de la solution

1. Assurez-vous que les données applicatives sont sauvegardées à l'aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d'instance appropriée à l'aide de BlueXP avec l'abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l'instance Google Cloud VMware Engine.
4. En cas d'incident, rompez la relation SnapMirror avec BlueXP et déclenchez le basculement des serveurs virtuels avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d'applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à "Configurez la réplication avec SnapCenter"

Révision de la protection de SQL VM avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et le temps de maintenance du SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d'exploitation globaux. Le SDDC peut héberger jusqu'à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

Le datastore NetApp Cloud Volume Service pour NFS et le journal et les bases de données Cloud Volumes ONTAP pour SQL peuvent être déployés sur n'importe quel VPC et GCVE doivent disposer d'une connexion privée à ce VPC pour monter le datastore NFS et se connecter aux LUN iSCSI par un VM.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.
"Se référer à la documentation Veeam pour la procédure d'installation"
Pour plus d'informations, reportez-vous à la section "Migration avec Veeam Replication"

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

Le basculement de la machine virtuelle Microsoft SQL Server

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.

Reprise après incident des applications avec SnapCenter, Cloud Volumes ONTAP et Veeam Replication

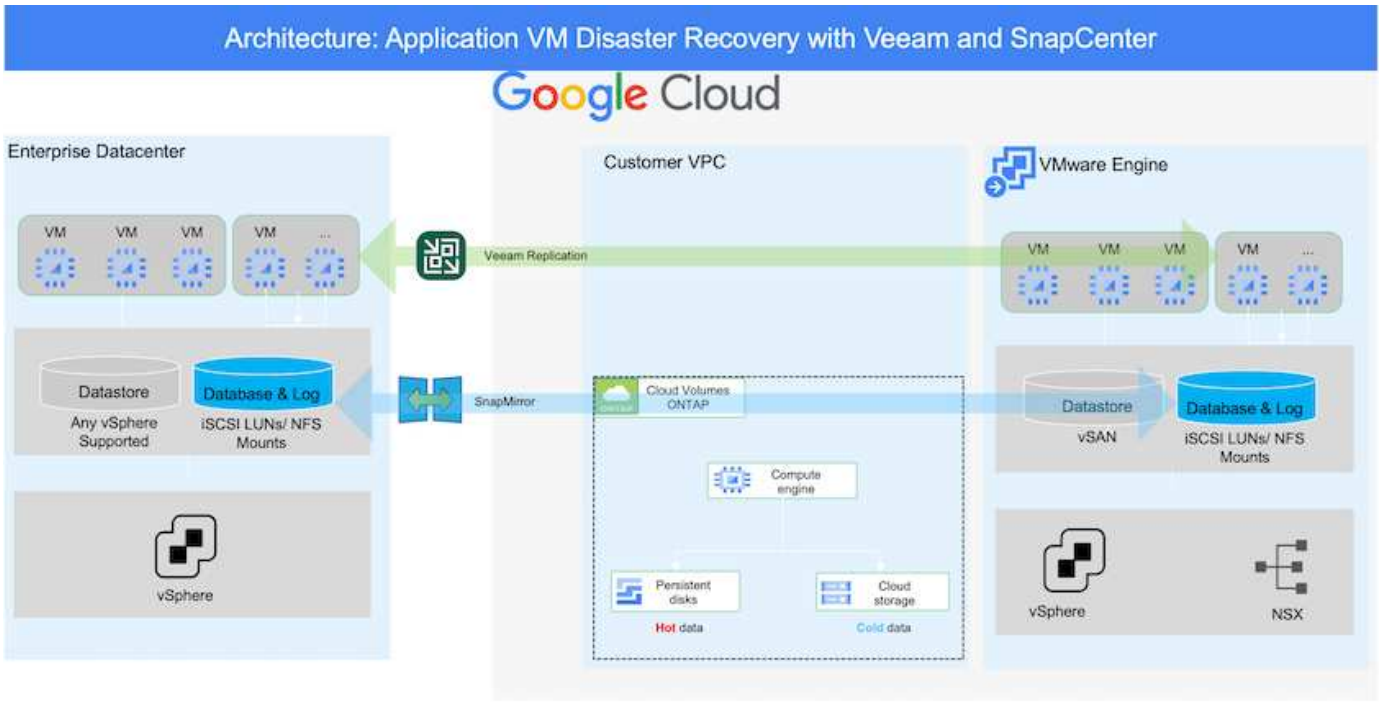
Auteurs : Suresh Thoppay, NetApp

Présentation

La reprise d'activité dans le cloud est une solution résiliente et économique qui protège les charges de travail

contre les pannes sur site et la corruption des données, comme les attaques par ransomware. NetApp SnapMirror permet de répliquer les charges de travail VMware sur site utilisant un stockage connecté à l'invité vers NetApp Cloud Volumes ONTAP exécuté dans Google Cloud. Il s'agit aussi des données applicatives, mais qu'en est-il des machines virtuelles elles-mêmes ? La reprise sur incident doit couvrir tous les composants dépendants, notamment les machines virtuelles, les VMDK ou les données d'application. Pour ce faire, SnapMirror et Veeam peuvent être utilisés pour restaurer de manière transparente les workloads répliqués depuis des sites sur Cloud Volumes ONTAP et en utilisant le stockage VSAN pour les VMDK de VM.

Ce document propose une approche détaillée de la configuration et de l'exécution d'une reprise d'activité à l'aide de NetApp SnapMirror, Veeam et Google Cloud VMware Engine (GCVE).



Hypothèses

Ce document est axé sur le stockage invité pour les données d'applications (également appelé « invité connecté »), et nous supposons que l'environnement sur site utilise SnapCenter pour assurer des sauvegardes cohérentes au niveau des applications.

> Ce document s'applique à toute solution de sauvegarde et de restauration tierce. En fonction de la solution utilisée dans l'environnement, suivez les bonnes pratiques pour créer des stratégies de sauvegarde conformes aux SLA de l'entreprise.

Pour la connectivité entre l'environnement sur site et le réseau Google Cloud, utilisez les options de connectivité telles que une interconnexion dédiée ou un VPN cloud. Les segments doivent être créés en fonction de la conception VLAN sur site.

> Plusieurs options de connexion des data centers sur site à Google Cloud sont possibles, ce qui évite de présenter un workflow spécifique dans ce document. Consultez la documentation Google Cloud pour connaître la méthode de connectivité appropriée, du site vers Google.

Déploiement de la solution de reprise d’activité

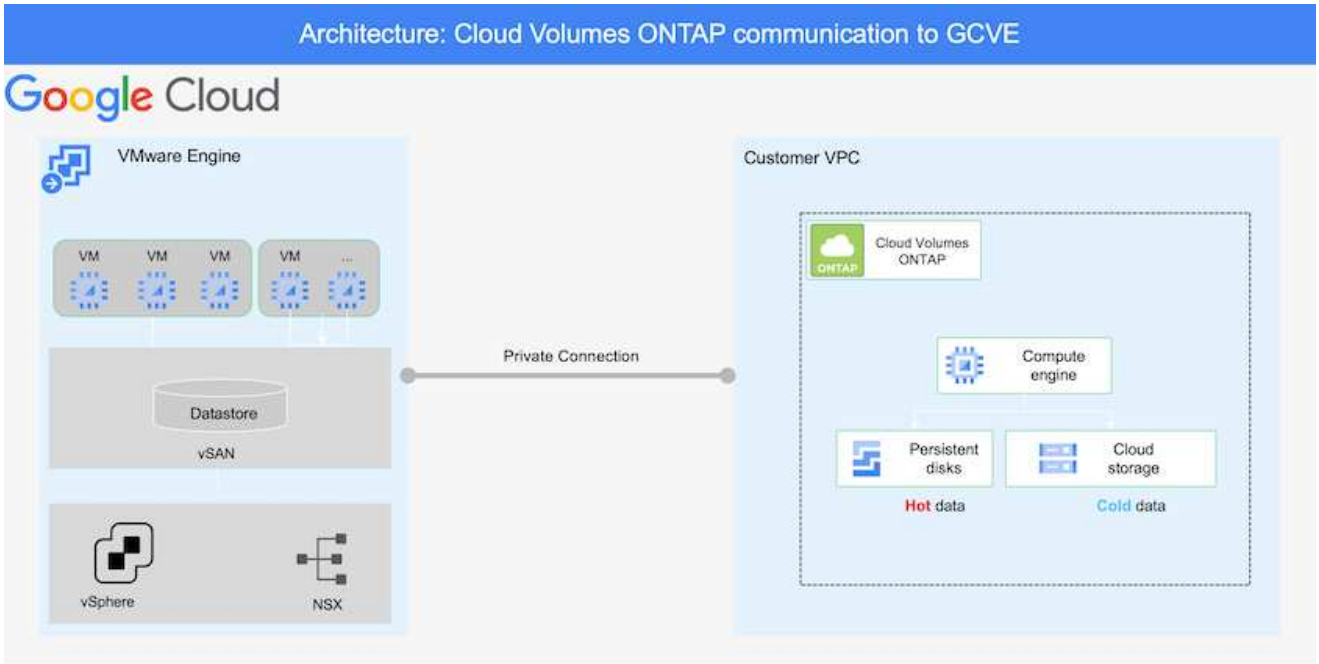
Présentation du déploiement de la solution

1. Assurez-vous que les données applicatives sont sauvegardées à l’aide de SnapCenter avec les exigences de RPO requises.
2. Provisionnez Cloud Volumes ONTAP avec la taille d’instance appropriée à l’aide de Cloud Manager dans l’abonnement et le réseau virtuel appropriés.
   a. Configurer SnapMirror pour les volumes applicatifs concernés.
   b. Mettez à jour les règles de sauvegarde dans SnapCenter pour déclencher des mises à jour SnapMirror après les tâches planifiées.
3. Installez le logiciel Veeam et commencez à répliquer des machines virtuelles sur l’instance Google Cloud VMware Engine.
4. En cas d’incident, interrompre la relation SnapMirror avec Cloud Manager et déclencher le basculement des machines virtuelles avec Veeam.
   a. Reconnectez les LUN ISCSI et les montages NFS pour les machines virtuelles d’applications.
   b. Permet de mettre les applications en ligne.
5. Annulez le rétablissement du site protégé après la restauration du site primaire.

Détails du déploiement

Configurez CVO pour Google Cloud et répliquez les volumes dans CVO

La première étape consiste à configurer Cloud Volumes ONTAP sur Google Cloud ("cvo") Et répliquez les volumes souhaités dans Cloud Volumes ONTAP avec les fréquences et les instantanés souhaités.



Pour obtenir des exemples d'instructions détaillées sur la configuration de SnapCenter et la réplication des données, reportez-vous à la section "Configurez la réplication avec SnapCenter"

Configurez la réplication avec SnapCenter

Configurez l'accès aux données des hôtes GCVE et CVO

Deux facteurs importants à prendre en compte lors du déploiement du SDDC sont la taille du cluster SDDC dans la solution GCVE et le temps de maintenance du SDDC. Ces deux considérations clés à prendre en compte dans une solution de reprise sur incident permettent de réduire les coûts d'exploitation globaux. Le SDDC peut héberger jusqu'à trois hôtes, tout comme un cluster multi-hôtes dans un déploiement à grande échelle.

Cloud Volumes ONTAP peut être déployé sur n'importe quel VPC et GCVE doit disposer d'une connexion privée à ce VPC pour que la VM se connecte aux LUN iSCSI.

Pour configurer GCVE SDDC, voir "Déploiement et configuration de l'environnement de virtualisation sur Google Cloud Platform (GCP)". Avant cela, vérifiez que les VM invités résidant sur les hôtes GCVE peuvent consommer des données de Cloud Volumes ONTAP une fois la connectivité établie.

Une fois que Cloud Volumes ONTAP et GCVE ont été correctement configurés, commencez à configurer Veeam pour automatiser la restauration des workloads sur site vers GCVE (machines virtuelles avec VMDK d'application et VM avec stockage « Guest ») en utilisant la fonctionnalité de réplication Veeam et en utilisant SnapMirror pour les copies de volumes d'application vers Cloud Volumes ONTAP.

Installer les composants Veeam

Selon le scénario de déploiement, le serveur de sauvegarde Veeam, le référentiel de sauvegarde et le proxy de sauvegarde à déployer. Pour ce cas d'utilisation, nul besoin de déployer un magasin d'objets pour Veeam et le référentiel scale-out non plus requis.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Se référer à la documentation Veeam pour la procédure d'installation"]

Configuration de la réplication de machine virtuelle avec Veeam

VCenter sur site et GCVE vCenter doit être enregistré auprès de Veeam. "Configuration de la tâche de réplication de VM vSphere" À l'étape traitement invité de l'assistant, sélectionnez Désactiver le traitement de l'application, car nous utilisons SnapCenter pour la sauvegarde et la restauration intégrant la cohérence applicative.

Configuration de la tâche de réplication de VM vSphere

Le basculement de la machine virtuelle Microsoft SQL Server

Le basculement de la machine virtuelle Microsoft SQL Server

Avantages de cette solution

- Utilise la réplication efficace et résiliente de SnapMirror.
- Restauration des points disponibles à temps avec la conservation des snapshots de ONTAP.
- Une automatisation complète est disponible pour toutes les étapes nécessaires à la restauration de centaines de milliers de machines virtuelles, depuis les étapes de validation du stockage, du calcul, du réseau et des applications.
- SnapCenter utilise des mécanismes de clonage qui ne modifient pas le volume répliqué.
  - Cela permet d'éviter le risque de corruption des données pour les volumes et les snapshots.
  - Evite les interruptions de réplication pendant les workflows de test de reprise après incident
  - Optimise les données de reprise après incident pour les flux de travail autres que la reprise après incident, comme le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau, et les tests de résolution des problèmes.
- Veeam Replication permet de modifier les adresses IP des VM sur le site de reprise après incident.