Schutz von Workloads in GCP/GCVE

NetApp Solutions

NetApp
April 26, 2024

Inhalt

Schutz von Workloads in GCP/GCVE

Applikationskonsistente Disaster Recovery mit NetApp SnapCenter und Veeam Replizierung

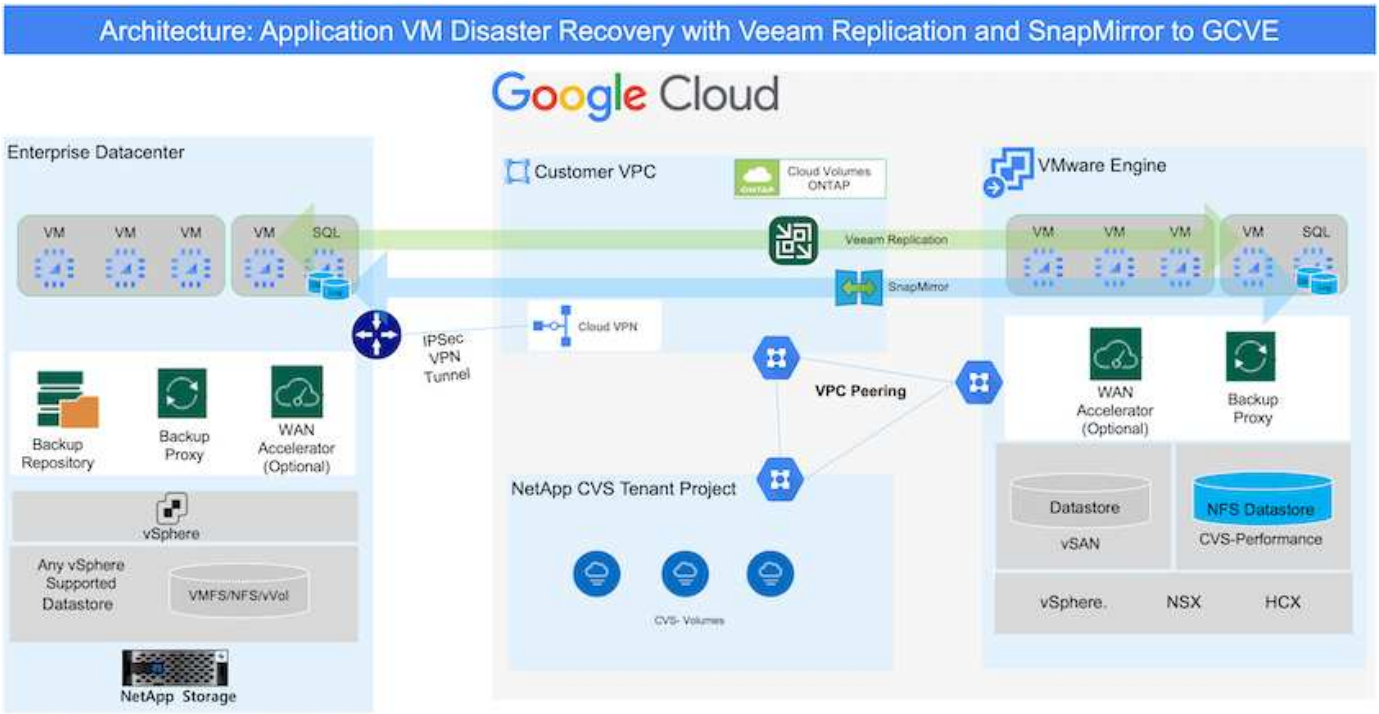
Autoren: Suresh ThopPay, NetApp

Überblick

Viele Kunden suchen nach einer effektiven Disaster Recovery-Lösung für ihre Applikations-VMs, die auf VMware vSphere gehostet werden. Viele von ihnen nutzen ihre bestehende Backup-Lösung, um im Diaster Recovery durchzuführen.
Oft erhöht diese Lösung die RTO und entspricht nicht ihren Erwartungen. Um RPO und RTO zu reduzieren, kann die Veeam VM-Replizierung sogar von On-Premises zu GCVE genutzt werden, sofern Netzwerkverbindungen und Umgebung mit entsprechenden Berechtigungen verfügbar sind.
HINWEIS: Veeam VM Replication schützt keine über VM-Gastsysteme verbundenen Storage-Geräte wie iSCSI- oder NFS-Mounts innerhalb der Gast-VM. Sie müssen sie separat schützen.

Für eine applikationskonsistente Replizierung für SQL VM und zur Reduzierung des RTO wurde SnapCenter zum Orchestrieren von snapmirror Vorgängen von SQL Datenbank- und Protokoll-Volumes eingesetzt.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

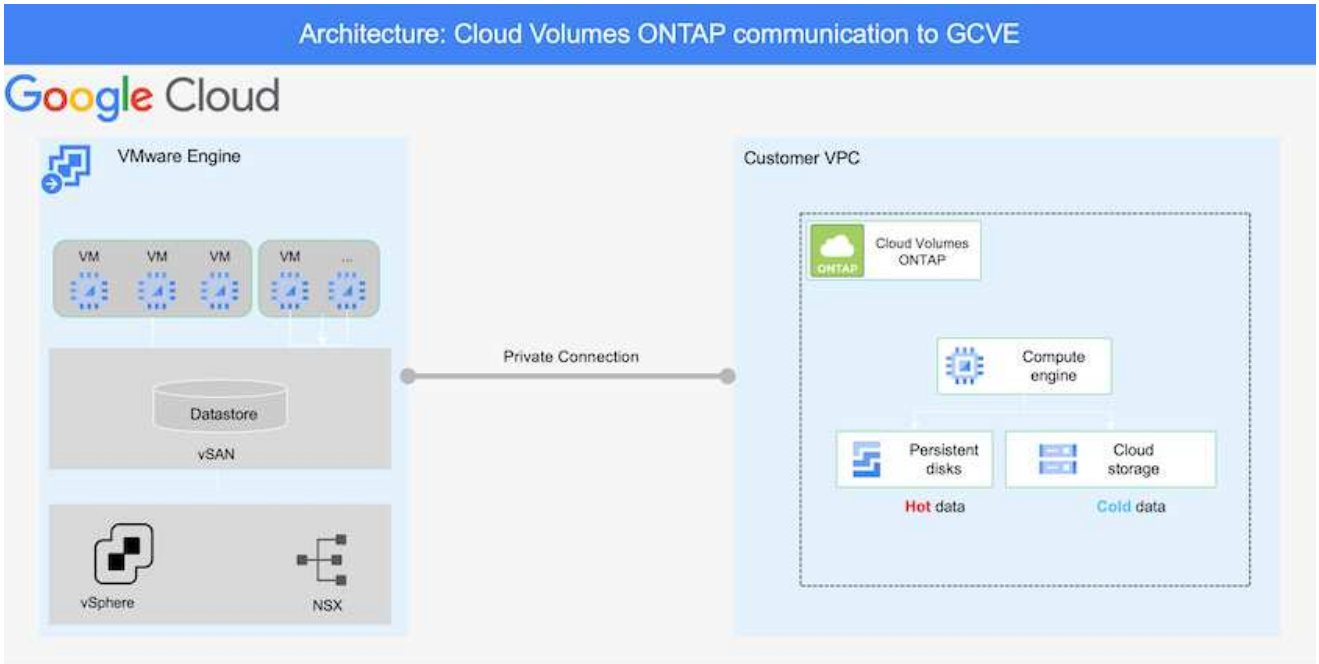
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mit BlueXP innerhalb des entsprechenden Abonnements und virtuellen Netzwerks Cloud Volumes ONTAP mit der korrekten Instanzgröße bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Ausfalls die SnapMirror Beziehung mit BlueXP auf und lösen Sie Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Google Cloud konfigurieren ("cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Überprüfen Sie den SQL VM-Schutz mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Der NetApp Cloud Volume Service für NFS-Datastore und die Cloud Volumes ONTAP für SQL-Datenbanken und das Protokoll können in jede VPC implementiert werden. GCVE sollte über eine private Verbindung zu dieser VPC verfügen, um den NFS-Datastore zu mounten und die VM mit den iSCSI-LUNs zu verbinden.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.
"Das Installationsverfahren finden Sie in der Veeam-Dokumentation"
Weitere Informationen finden Sie unter "Migration mit Veeam Replication"

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

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

Failover von Microsoft SQL Server VM

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

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung

- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.

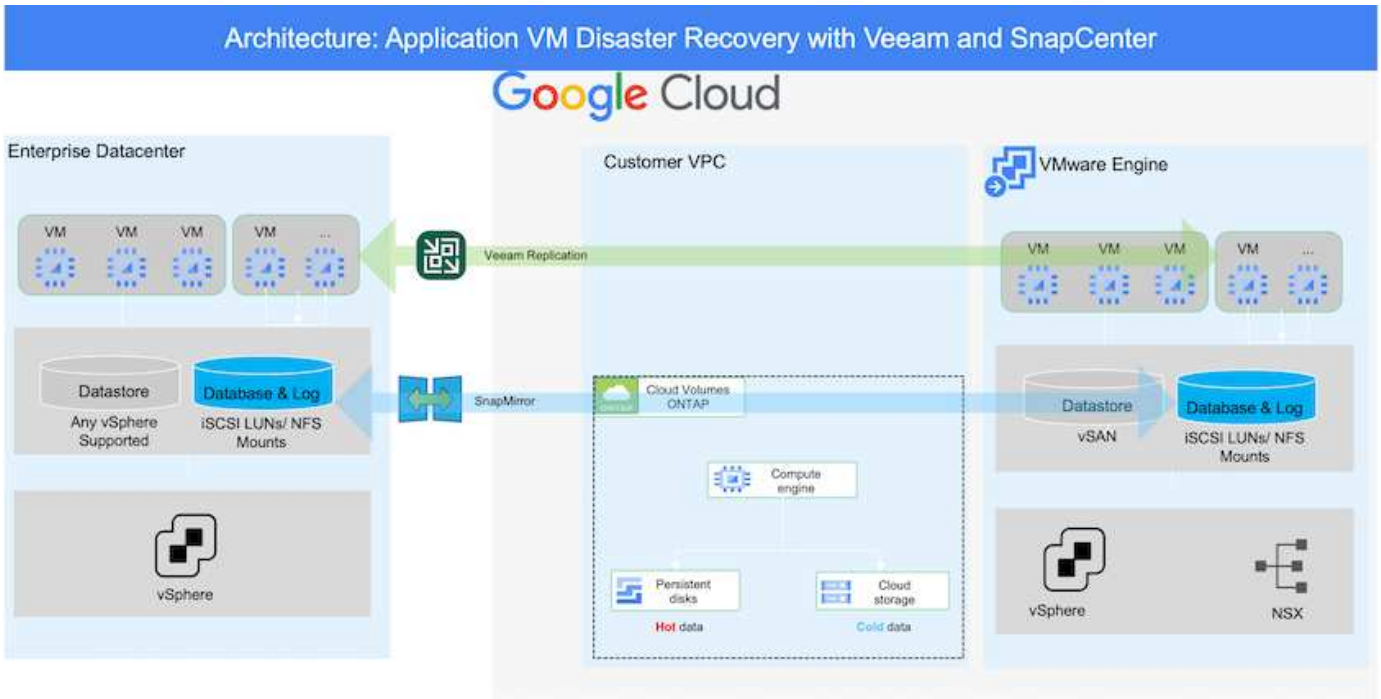
Disaster Recovery für Applikationen mit SnapCenter, Cloud Volumes ONTAP und Veeam Replication

Autoren: Suresh ThopPay, NetApp

Überblick

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die Storage mit Anbindung des Gastspeichers verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, die in Google Cloud ausgeführt werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Dazu kann SnapMirror zusammen mit Veeam verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig mit vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet eine Schritt-für-Schritt-Methode zum Einrichten und Durchführen von Disaster-Recovery mit NetApp SnapMirror, Veeam und der Google Cloud VMware Engine (GCVE).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.

> Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Verbindung zwischen der lokalen Umgebung und dem Google Cloud-Netzwerk können Sie die Konnektivitätsoptionen wie dediziertes Interconnect oder Cloud VPN verwenden. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen, um On-Premises-Datacenter mit Google Cloud zu verbinden, was uns daran hindert, einen bestimmten Workflow in diesem Dokument zu beschreiben. Die entsprechende On-Premises-zu-Google-Verbindungsmethode finden Sie in der Google Cloud-Dokumentation.

Implementieren der DR-Lösung

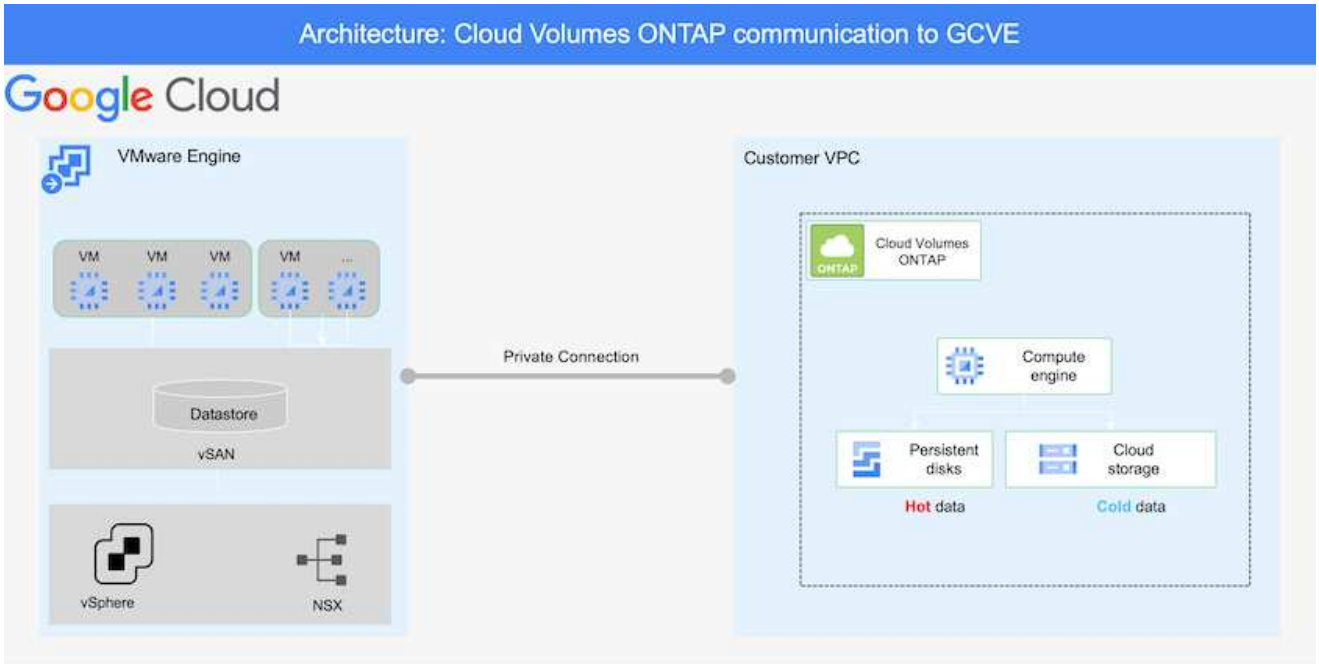
Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
   a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes
   b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die Veeam Software und beginnen Sie mit der Replizierung von Virtual Machines zu Google Cloud VMware Engine Instanz.
4. Brechen Sie während eines Notfallereignisses die SnapMirror Beziehung mithilfe von Cloud Manager auf und lösen Sie das Failover von Virtual Machines mit Veeam aus.
   a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
   b. Anwendungen online schalten.
5. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Google Cloud und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Google Cloud konfigurieren ("cvo") Und replizieren Sie die gewünschten Volumen zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.



Eine Schritt-für-Schritt-Anleitung zum Einrichten von SnapCenter und zum Replizieren der Daten finden Sie unter "Einrichtung der Replikation mit SnapCenter"

Einrichtung der Replikation mit SnapCenter

Konfigurieren Sie GCVE-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der GCVE-Lösung und die Dauer, bis das SDDC den Betrieb aufrecht erhalten hat. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Cloud Volumes ONTAP kann in jede VPC implementiert werden und GCVE sollte über eine private Verbindung zu dieser VPC verfügen, damit VM-Verbindung mit iSCSI-LUNs hergestellt werden kann.

Informationen zum Konfigurieren von GCVE SDDC finden Sie unter "Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)". Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den GCVE-Hosts Daten aus dem Cloud Volumes ONTAP nutzen können, nachdem eine Verbindung hergestellt wurde.

Nachdem Cloud Volumes ONTAP und GCVE ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Veeam, um die Wiederherstellung lokaler Workloads auf GCVE (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) zu automatisieren. Dazu nutzen Sie die Veeam Replication-Funktion und können SnapMirror für Applikations-Volumes-Kopien in Cloud Volumes ONTAP nutzen.

Veeam Komponenten Installieren

Der Veeam Backup-Server, Backup-Repository und Backup-Proxy, der bereitgestellt werden muss, basieren auf einem Implementierungsszenario. In diesem Anwendungsfall müssen kein Objektspeicher für Veeam implementiert und auch kein Scale-out-Repository erforderlich sein.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Das Installationsverfahren finden Sie in der Veeam-Dokumentation"]

VM Replication mit Veeam einrichten

VCenter vor Ort und GCVE vCenter müssen bei Veeam registriert werden. "VSphere VM Replication Job einrichten" Wählen Sie im Assistenten zur Gastverarbeitung die Option Anwendungsverarbeitung deaktivieren, da wir SnapCenter für applikationsgerechtes Backup und Recovery verwenden werden.

VSphere VM Replication Job einrichten

Failover von Microsoft SQL Server VM

Failover von Microsoft SQL Server VM

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
  - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.
  - Keine Replizierungsunterbrechungen während der DR-Test-Workflows
  - Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- Veeam Replication ermöglicht das Ändern der VM-IP-Adressen am DR-Standort.