GCP / GCVEでのワークロードの保護

NetApp Solutions

NetApp
September 10, 2024

目次

GCP / GCVEでのワークロードの保護

NetApp SnapCenterとVeeamのレプリケーションにより、アプリケーションと整合性のあるディザスタリカバリを実現

クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェアなどのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Google Cloudで実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。

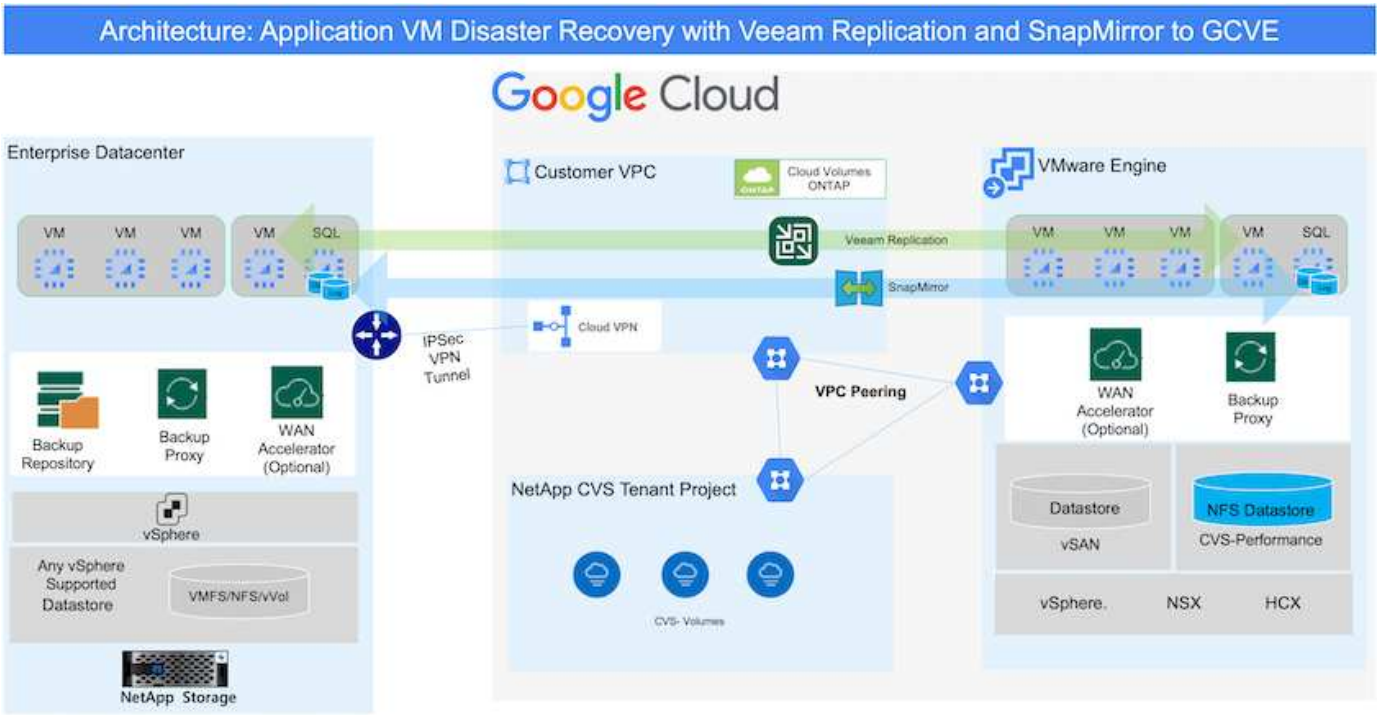
執筆者：ネットアップSuresh Thoppay

概要

多くのお客様は、VMware vSphereでホストされているアプリケーションVMに対して、効果的なディザスタリカバリ解決策を求めています。それらの多くは、既存のバックアップ解決策を使用して、ダイヤル中に回復を実行します。
多くの場合、解決策はRTOを高め、期待に応えられません。RPOとRTOを短縮するために、適切な権限を持つネットワーク接続と環境が利用可能であれば、オンプレミスからGCVEへのVeeam VMレプリケーションを利用できます。
注: Veeam VM Replicationでは、ゲストVM内のiSCSIマウントやNFSマウントなどのVMゲスト接続ストレージデバイスは保護されません。それらを別 々 に保護する必要があります。

SQL VMでアプリケーションと整合性のあるレプリケーションを実現し、RTOを短縮するために、SnapCenterを使用してSQLデータベースとログボリュームのSnapMirror処理をオーケストレーションしました。

このドキュメントでは、NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチについて説明します。



前提条件

本ドキュメントでは、アプリケーションデータ用のゲスト内ストレージ（ゲスト接続とも呼ばれます）を中心に説明します。オンプレミス環境では、アプリケーションと整合性のあるバックアップにSnapCenter を使用していると想定しています。

> 本ドキュメントは、環境 サードパーティ製バックアップまたはリカバリ用解決策 に関するものです。環境で使用されている解決策 に応じて、ベストプラクティスに従って、組織のSLAを満たすバックアップポリシーを作成してください。

オンプレミス環境とGoogle Cloudネットワーク間の接続には、専用のインターコネクトやCloud VPNなどの接続オプションを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必要があります。

> オンプレミスのデータセンターをGoogle Cloudに接続する方法は複数ありますが、この方法では、このドキュメントの特定のワークフローの概要を説明することはできません。オンプレミスからGoogleへの適切な接続方法については、Google Cloudのドキュメントを参照してください。

DR解決策 の導入

解決策 の導入の概要

1. SnapCenter を使用して、必要なRPO要件に従ってアプリケーションデータがバックアップされていることを確認してください。
2. 適切なサブスクリプションと仮想ネットワーク内でBlueXPを使用して、正しいインスタンスサイズでCloud Volumes ONTAPをプロビジョニングします。
   a. 該当するアプリケーションボリュームに対してSnapMirrorを設定します。
   b. スケジュールされたジョブの実行後にSnapMirror更新をトリガーするには、SnapCenter でバックアッ

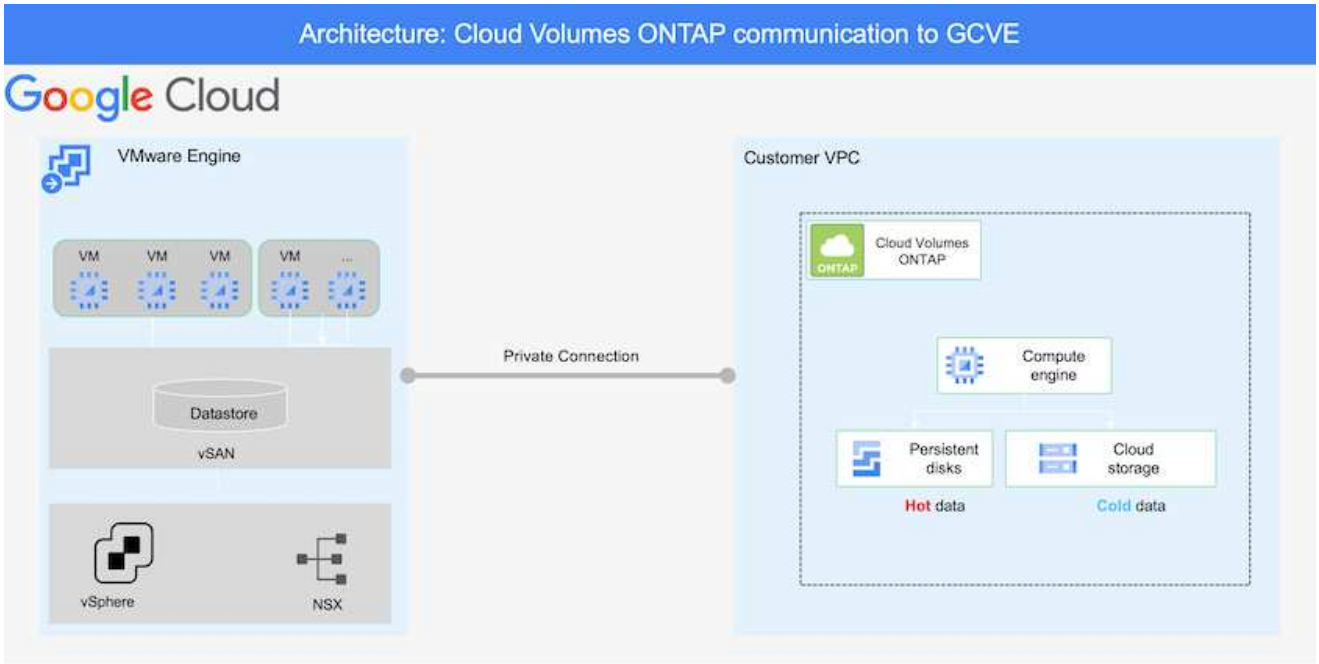
プポリシーを更新してください。

3. Veeamソフトウェアをインストールし、Google Cloud VMware Engineインスタンスへの仮想マシンのレプリケーションを開始します。
4. 災害発生時には、BlueXPを使用してSnapMirror関係を解除し、Veeamで仮想マシンのフェイルオーバーをトリガーします。
   a. アプリケーションVMのiSCSI LUNおよびNFSマウントを再接続します。
   b. アプリケーションをオンラインにします。
5. プライマリサイトのリカバリ後にSnapMirrorを逆再同期して、保護サイトへのフェイルバックを開始します。

展開の詳細

Google Cloudで**CVO**を構成し、ボリュームを**CVO**にレプリケート

最初のステップは、Google CloudでCloud Volumes ONTAPを設定することです（"CVOを確認して"）をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。



SnapCenter を設定してデータを複製する手順の例については、を参照してください "SnapCenter を使用してレプリケーションを設定する"

SnapCenterを使用したSQL VMの保護の確認

GCVEホストと**CVO**データアクセスを設定する

SDDCを導入する際に考慮すべき2つの重要な要素は、GCVE解決策 のSDDCクラスタのサイズと、SDDCの稼働時間です。ディザスタリカバリ解決策 に関する以下の2つの重要な考慮事項は、全体的な運用コストの削減に役立ちます。SDDCは、3台のホストの規模に対応し、フルスケールの導入ではマルチホストクラスタにまで対応できます。

NetApp Cloud Volume Service for NFS DatastoreおよびCloud Volumes ONTAP for SQLデータベースとログを任意のVPCに導入できます。GCVEは、NFSデータストアをマウントしてVMをiSCSI LUNに接続するために、そのVPCにプライベート接続を確立する必要があります。

GCVE SDDCを設定するには、を参照してください "Google Cloud Platform （ GCP ）への仮想化環境の導入と構成"。前提条件として、接続が確立された後で、GCVEホストに存在するゲストVMがCloud Volumes ONTAP からデータを使用できることを確認します。

Cloud Volumes ONTAP とGCVEを適切に設定したら、Veeamのレプリケーション機能を使用して、Cloud Volumes ONTAP へのアプリケーションボリュームコピーにSnapMirrorを利用することで、オンプレミスのワークロードのGCVE（アプリケーションVMDKおよびゲストストレージを搭載したVM）へのリカバリを自動化するようにVeeamを設定します。

Veeamコンポーネントをインストールします

導入シナリオに基づいて、Veeamバックアップサーバ、バックアップリポジトリ、およびバックアッププロキシを導入する必要があります。このユースケースでは、Veeam用のオブジェクトストアとスケールアウトリポジトリも必要ありません。
"インストール手順 については、Veeamの製品ドキュメントを参照してください"
追加情報については、を参照してください "Veeam Replicationによる移行"

VMレプリケーションを**Veeam**とセットアップする

オンプレミスのvCenterとGCVEのvCenterをVeeamに登録する必要があります。 "vSphere VMレプリケーションジョブをセットアップします" ウィザードの[ゲスト処理]ステップで、[アプリケーション対応のバックアップとリカバリにSnapCenter を使用するので、アプリケーション処理を無効にする]を選択します。

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

Microsoft SQL Server VMのフェイルオーバー

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

この解決策 の利点

- 効率性と耐障害性に優れたSnapMirrorレプリケーションを使用します。
- ONTAP スナップショットの保持により、利用可能な任意の時点までリカバリします。

- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百~数千のVMのリカバリに必要なすべての手順を完全に自動化できます。
- SnapCenter では、レプリケートされたボリュームを変更しないクローニングメカニズムが使用されます。
  - これにより、ボリュームとSnapshotのデータが破損するリスクを回避できます。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。
- Veeam Replicationでは、DRサイトのVMのIPアドレスを変更できます。

SnapCenter 、Cloud Volumes ONTAP 、Veeamレプリケーションを使用したアプリケーションディザスタリカバリ

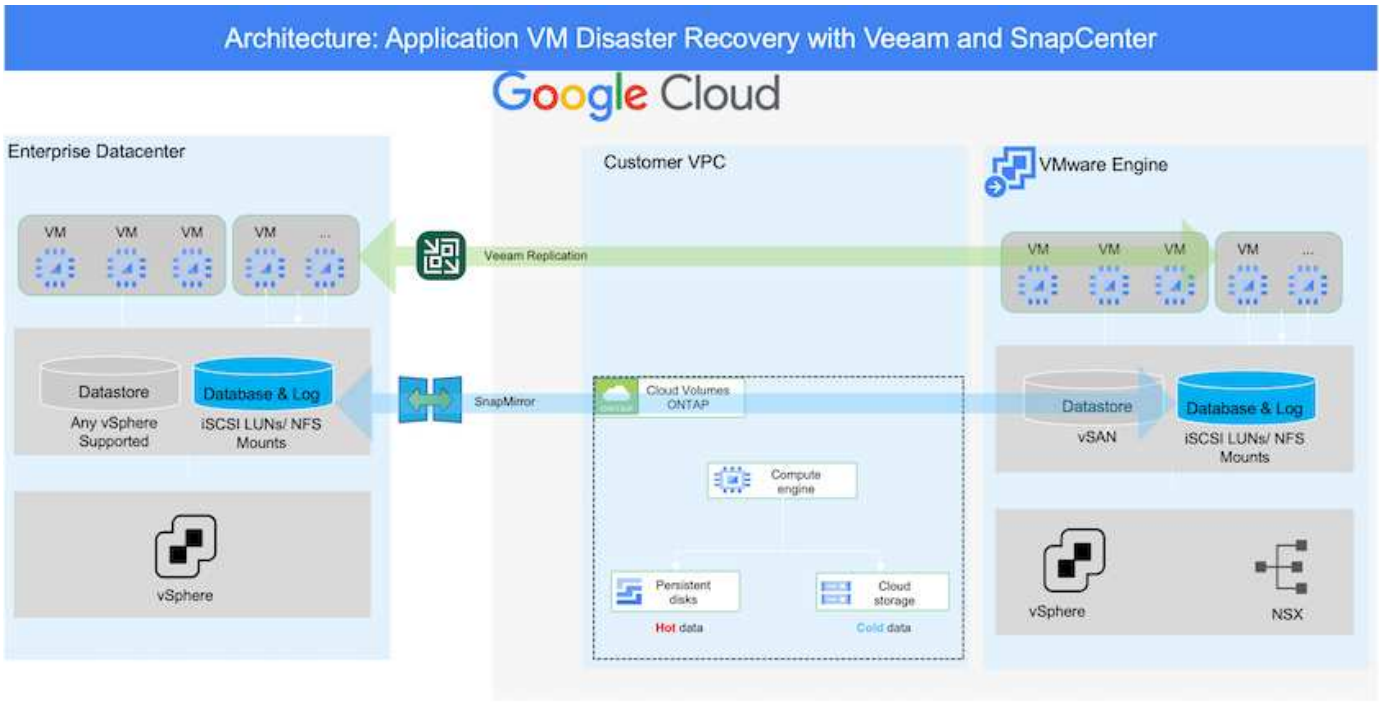
クラウドへのディザスタリカバリは、耐障害性と対費用効果に優れた方法で、サイトの停止やランサムウェアなどのデータ破損からワークロードを保護します。NetApp SnapMirrorを使用すると、ゲスト接続ストレージを使用するオンプレミスのVMwareワークロードを、Google Cloudで実行されているNetApp Cloud Volumes ONTAP にレプリケートできます。

執筆者：ネットアップSuresh Thoppay

概要

これはアプリケーションデータに適用されますが、実際のVM自体についてはどうでしょうか。ディザスタリカバリは、仮想マシン、VMDK、アプリケーションデータなど、依存するすべてのコンポーネントを対象にする必要があります。これを実現するために、SnapMirrorとVeeamを併用すれば、オンプレミスからCloud Volumes ONTAP にレプリケートしたワークロードをシームレスにリカバリしながら、VM VMDKにvSANストレージを使用することができます。

このドキュメントでは、NetApp SnapMirror、Veeam、Google Cloud VMware Engine（GCVE）を使用してディザスタリカバリを設定および実行するためのステップバイステップ形式のアプローチについて説明します。



前提条件

本ドキュメントでは、アプリケーションデータ用のゲスト内ストレージ（ゲスト接続とも呼ばれます）を中心に説明します。オンプレミス環境では、アプリケーションと整合性のあるバックアップにSnapCenter を使用していると想定しています。

> ⓘ 本ドキュメントは、環境 サードパーティ製バックアップまたはリカバリ用解決策 に関するものです。環境で使用されている解決策 に応じて、ベストプラクティスに従って、組織のSLAを満たすバックアップポリシーを作成してください。

オンプレミス環境とGoogle Cloudネットワーク間の接続には、専用のインターコネクトやCloud VPNなどの接続オプションを使用します。オンプレミスVLANの設計に基づいてセグメントを作成する必要があります。

> ⓘ オンプレミスのデータセンターをGoogle Cloudに接続する方法は複数ありますが、この方法では、このドキュメントの特定のワークフローの概要を説明することはできません。オンプレミスからGoogleへの適切な接続方法については、Google Cloudのドキュメントを参照してください。

DR解決策 の導入

解決策 の導入の概要

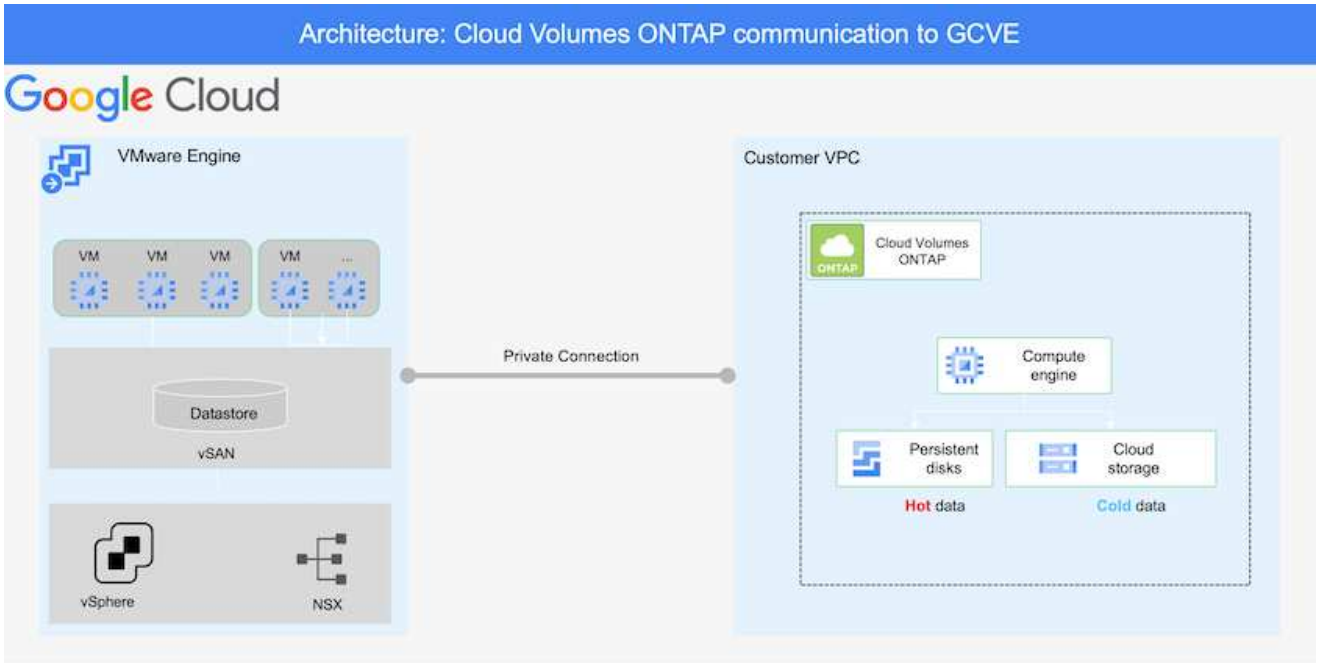
1. SnapCenter を使用して、必要なRPO要件に従ってアプリケーションデータがバックアップされていることを確認してください。
2. 適切なサブスクリプションと仮想ネットワーク内で、Cloud Managerを使用して、適切なインスタンスサイズでCloud Volumes ONTAP をプロビジョニングします。
   a. 該当するアプリケーションボリュームに対してSnapMirrorを設定します。
   b. スケジュールされたジョブの実行後にSnapMirror更新をトリガーするには、SnapCenter でバックアップポリシーを更新してください。

3. Veeamソフトウェアをインストールし、Google Cloud VMware Engineインスタンスへの仮想マシンのレプリケーションを開始します。
4. 災害発生時は、Cloud Managerを使用してSnapMirror関係を解除し、仮想マシンとVeeamのフェイルオーバーをトリガーします。
   a. アプリケーションVMのiSCSI LUNおよびNFSマウントを再接続します。
   b. アプリケーションをオンラインにします。
5. プライマリサイトのリカバリ後にSnapMirrorを逆再同期して、保護サイトへのフェイルバックを開始します。

展開の詳細

Google Cloudで**CVO**を構成し、ボリュームを**CVO**にレプリケート

最初のステップは、Google CloudでCloud Volumes ONTAPを設定することです（"CVOを確認して"）をクリックし、必要なボリュームを、必要な頻度とSnapshotの保持を使用してCloud Volumes ONTAP にレプリケートします。



SnapCenter を設定してデータを複製する手順の例については、を参照してください "SnapCenter を使用してレプリケーションを設定する"

SnapCenter を使用してレプリケーションを設定する

GCVEホストと**CVO**データアクセスを設定する

SDDCを導入する際に考慮すべき2つの重要な要素は、GCVE解決策 のSDDCクラスタのサイズと、SDDCの稼働時間です。ディザスタリカバリ解決策 に関する以下の2つの重要な考慮事項は、全体的な運用コストの削減に役立ちます。SDDCは、3台のホストの規模に対応し、フルスケールの導入ではマルチホストクラスタにまで対応できます。

Cloud Volumes ONTAP は任意のVPCに導入でき、GCVEはそのVPCへのプライベート接続でiSCSI LUNに接続する必要があります。

GCVE SDDCを設定するには、を参照してください "Google Cloud Platform （ GCP ）への仮想化環境の導入と構成"。前提条件として、接続が確立された後で、GCVEホストに存在するゲストVMがCloud Volumes ONTAP からデータを使用できることを確認します。

Cloud Volumes ONTAP とGCVEを適切に設定したら、Veeamのレプリケーション機能を使用して、Cloud Volumes ONTAP へのアプリケーションボリュームコピーにSnapMirrorを利用することで、オンプレミスのワークロードのGCVE（アプリケーションVMDKおよびゲストストレージを搭載したVM）へのリカバリを自動化するようにVeeamを設定します。

Veeamコンポーネントをインストールします

導入シナリオに基づいて、Veeamバックアップサーバ、バックアップリポジトリ、およびバックアッププロキシを導入する必要があります。このユースケースでは、Veeam用のオブジェクトストアとスケールアウトリポジトリも必要ありません。https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["インストール手順 については、Veeamの製品ドキュメントを参照してください"]

VMレプリケーションを**Veeam**とセットアップする

オンプレミスのvCenterとGCVEのvCenterをVeeamに登録する必要があります。 "vSphere VMレプリケーションジョブをセットアップします" ウィザードの[ゲスト処理]ステップで、[アプリケーション対応のバックアップとリカバリにSnapCenter を使用するので、アプリケーション処理を無効にする]を選択します。

vSphere VMレプリケーションジョブをセットアップします

Microsoft SQL Server VMのフェイルオーバー

Microsoft SQL Server VMのフェイルオーバー

この解決策 の利点

- 効率性と耐障害性に優れたSnapMirrorレプリケーションを使用します。
- ONTAP スナップショットの保持により、利用可能な任意の時点までリカバリします。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証から、数百~数千のVMのリカバリに必要なすべての手順を完全に自動化できます。

- SnapCenter では、レプリケートされたボリュームを変更しないクローニングメカニズムが使用されます。
  - これにより、ボリュームとSnapshotのデータが破損するリスクを回避できます。
  - DRテストのワークフロー中にレプリケーションが中断されるのを回避します
  - 開発とテスト、セキュリティテスト、パッチとアップグレードのテスト、修正テストなど、DR以外のワークフローにDRデータを活用します。
- Veeam Replicationでは、DRサイトのVMのIPアドレスを変更できます。