



前提条件の設定

NetApp Solutions

NetApp
April 10, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/netapp-solutions/databases/hybrid_dbops_snapcenter_prereq_onprem.html on April 10, 2024. Always check docs.netapp.com for the latest.

目次

前提条件の設定	1
オンプレミス	1
パブリッククラウド	1
オンプレミスの前提条件	1
パブリッククラウドの前提条件	5

前提条件の設定

ハイブリッドクラウドデータベースワークロードを実行する前に、オンプレミスとクラウドの両方で特定の前提条件を設定する必要があります。ここでは、このプロセスの概要を示し、必要なシステム構成の詳細については次のリンクを参照してください。

オンプレミス

- SnapCenter のインストールと設定
- オンプレミスのデータベースサーバのストレージ構成
- ライセンス要件
- ネットワークとセキュリティ
- 自動化

パブリッククラウド

- NetApp Cloud Central へのログイン
- Web ブラウザから複数のエンドポイントへのネットワークアクセス
- コネクタのネットワーク上の場所
- クラウドプロバイダの権限
- 個々のサービスのネットワーク

重要な考慮事項：

1. Cloud Manager Connector の導入場所
2. Cloud Volumes ONTAP のサイジングとアーキテクチャ
3. シングルノードとハイアベイラビリティのどちらか？

詳細については、次のリンクを参照してください。

["オンプレミス"](#)

["パブリッククラウド"](#)

オンプレミスの前提条件

SnapCenter ハイブリッドクラウドデータベースワークロード環境を準備するには、オンプレミスで次のタスクを完了する必要があります。

SnapCenter のインストールと設定

NetApp SnapCenter ツールは Windows ベースのアプリケーションで、通常は Windows ドメイン環境で実行

されますが、ワークグループ導入も可能です。これは、集中管理サーバー（ SnapCenter サーバー）とデータベースワークロード用のデータベースサーバーホスト上の SnapCenter プラグインを含む多層アーキテクチャに基づいています。ここでは、ハイブリッドクラウドの導入に関する主な考慮事項をいくつか示します。

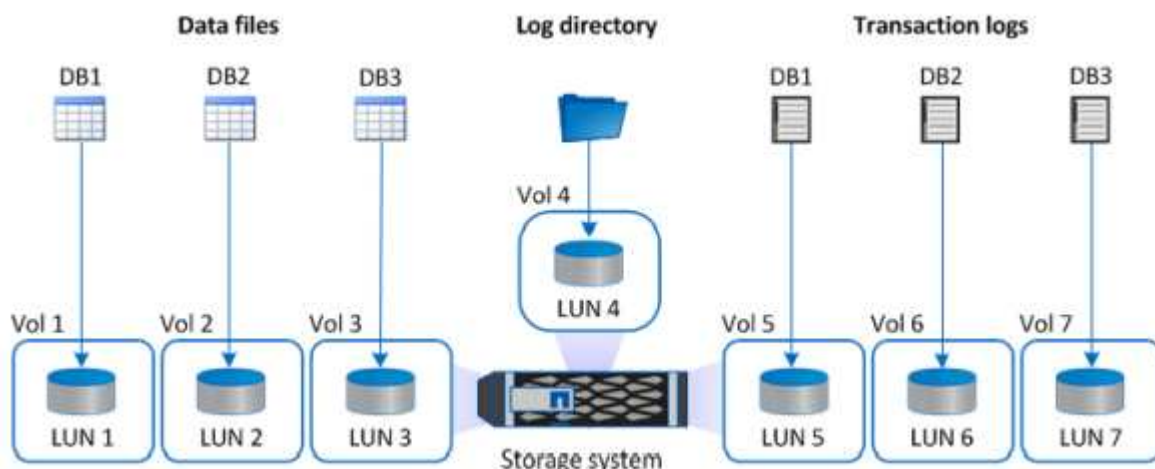
- * 単一インスタンスまたは HA 展開。 * HA 展開は、単一 SnapCenter インスタンスサーバーに障害が発生した場合に冗長性を提供します。
- * 名前解決。 * フォワードルックアップとリバースルックアップのためには、ストレージ SVM 上だけでなくすべてのデータベースホストを解決するために SnapCenter サーバ上で DNS を設定する必要があります。フォワードルックアップとリバースルックアップの両方で SnapCenter サーバとストレージ SVM を解決するためには、データベースサーバで DNS も設定する必要があります。
- * ロールベースアクセス制御（RBAC）の設定。 * 混在データベースワークロードの場合は、RBAC を使用して、Oracle データベースの管理者や SQL Server の管理者など、異なる DB プラットフォーム用の管理責任を分離できます。DB 管理者ユーザには、必要な権限が付与されている必要があります。
- * バックアップの一貫性と信頼性を確保するために、ポリシー・ベースのバックアップ戦略を有効にします。 *
- * ファイアウォール上の必要なネットワーク・ポートを開きます。 * オンプレミスの SnapCenter サーバが、クラウド DB ホストにインストールされたエージェントと通信できるようにします。
- * ポートは、オンプレミスとパブリッククラウド間の SnapMirror トラフィックを許可するためにオープンである必要があります。 * SnapCenter サーバは、ONTAP SnapMirror を使用して、オンサイトの Snapshot バックアップをクラウドの CVO ストレージ SVM にレプリケートします。

インストール前の計画と考慮事項を慎重に検討したら、これをクリックしてください ["SnapCenter の設置ワークフロー"](#) SnapCenter のインストールと設定の詳細については、を参照してください。

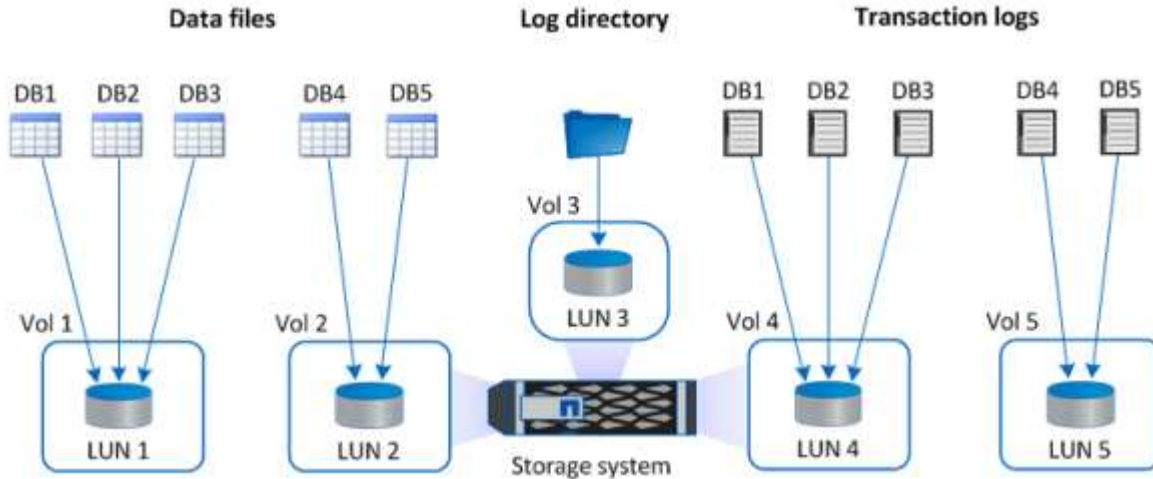
オンプレミスのデータベースサーバのストレージ構成

データベースとアプリケーションの全体的なパフォーマンスには、ストレージのパフォーマンスが重要な役割を果たします。適切に設計されたストレージレイアウトでは、DB のパフォーマンスを向上させるだけでなく、データベースのバックアップとリカバリの管理も簡単に行えます。ストレージレイアウトを定義する際には、データベースのサイズ、データベースの予想されるデータ変更率、バックアップの実行頻度など、いくつかの要素を考慮する必要があります。

一般に、仮想データベースワークロード用に NFS または iSCSI でストレージ LUN をゲスト VM に直接接続すると、VMDK 経由で割り当てられたストレージよりもパフォーマンスが向上します。次の図に示す LUN 上にある大規模な SQL Server データベースのストレージレイアウトを使用することを推奨します。



次の図は、LUN 上の小規模または中規模の SQL Server データベースに推奨されるストレージレイアウトを示しています。



ログディレクトリは SnapCenter 専用で、データベースリカバリ用のトランザクションログロールアップを実行します。1つのボリュームに複数の LUN を割り当てて、パフォーマンスを向上させることもできます。

Oracle データベースワークロードの場合、SnapCenter は、ONTAP ストレージを使用するデータベース環境をサポートします。この環境は、物理デバイスまたは仮想デバイスとしてホストにマウントされます。環境の重要度に基づいて、データベース全体を単一または複数のストレージデバイス上にホストすることができます。通常、専用ストレージにあるデータファイルは、制御ファイル、REDO ファイル、アーカイブログファイルなどの他のすべてのファイルから分離されます。これにより、管理者は Snapshot テクノロジーを使用して数秒から数分以内に（ONTAP の単一ファイル SnapRestore）を迅速にリストアしたり、大規模な重要データベース（ペタバイト規模）のクローンを作成したりできます。

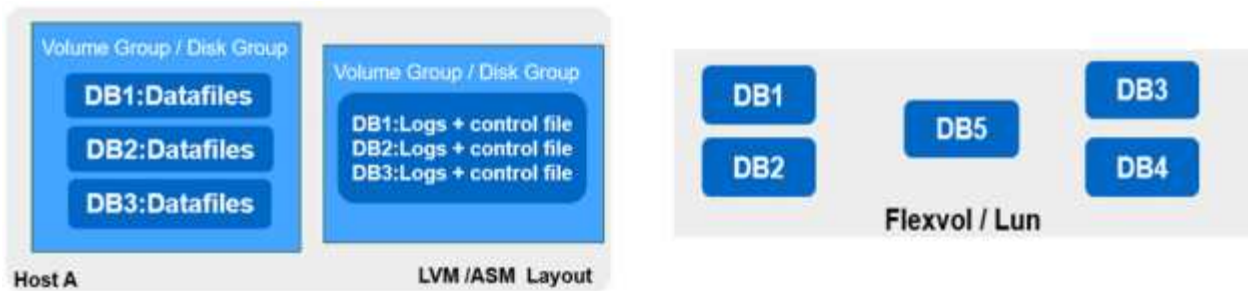


レイテンシの影響を受けやすいミッションクリティカルなワークロードに対しては、可能なかぎり最適なレイテンシを実現するために、異なる種類の Oracle ファイルに専用のストレージボリュームを導入する必要があります。大規模なデータベースの場合は、ボリュームごとに複数の LUN をデータファイルに割り当てる必要があります（最大 8 個まで推奨）。



小規模な Oracle データベースの場合、SnapCenter は共有ストレージレイアウトをサポートしています。共有ストレージレイアウトでは、同じストレージボリュームまたは LUN 上で複数のデータベースまたはデータ

ベースの一部をホストできます。このレイアウトの例として、+DATAASM ディスクグループまたはボリュームグループ上のすべてのデータベースのデータファイルをホストできます。それ以外のファイル（REDO ファイル、アーカイブログファイル、および制御ファイル）は、別の専用ディスクグループまたはボリュームグループ（LVM）でホストすることができます。このような導入シナリオを次に示します。



Oracle データベースの再配置を容易にするには、通常のバックアップポリシーに含まれている別の LUN に Oracle バイナリをインストールする必要があります。これにより、新しいサーバホストにデータベースを再配置する場合、Oracle バイナリの同期が取れていないため、潜在的な問題が発生することなく、Oracle スタックをリカバリ用に起動できます。

ライセンス要件

SnapCenter は、ネットアップが提供するライセンスソフトウェアです。これは通常、オンプレミスの ONTAP ライセンスに含まれています。ただし、ハイブリッドクラウドの導入の場合は、SnapCenter に CVO をターゲットデータレプリケーションのデスティネーションとして追加するために、SnapCenter のクラウドライセンスも必要です。詳細については、次のリンク先で SnapCenter の標準容量ベースのライセンスを確認してください。

["SnapCenter の容量単位の標準ライセンスです"](#)

ネットワークとセキュリティ

オンプレミスの本番データベースをオンプレミスで運用し、開発 / テストやディザスタリカバリのためにクラウドへの移行が非常に活発になるハイブリッドデータベースでは、環境をセットアップしてオンプレミスのデータセンターからパブリッククラウドに接続する際に、ネットワークとセキュリティを考慮することが重要です。

パブリッククラウドでは、一般に仮想プライベートクラウド（VPC）を使用して、パブリッククラウドプラットフォーム内の異なるユーザを分離します。個々の VPC 内では、VPC のロックダウンのユーザニーズに基づいて設定可能なセキュリティグループなどの手法を使用してセキュリティが制御されます。

オンプレミスのデータセンターから VPC への接続は、VPN トンネルを介して保護できます。VPN ゲートウェイでは、NAT およびファイアウォールルールを使用してセキュリティを強化できます。このルールでは、インターネット上のホストから企業データセンター内のホストへのネットワーク接続の確立をブロックします。

ネットワークとセキュリティに関する考慮事項については、任意のパブリッククラウドに対する、関連するインバウンドおよびアウトバウンドの CVO ルールを確認してください。

- ["CVO-AWS のセキュリティグループルール"](#)
- ["CVO-Azure のセキュリティグループルール"](#)
- ["CVO-GCP のファイアウォールルール"](#)

Ansible による自動化を使用して、オンプレミスとクラウドの間で **DB** インスタンスを同期することもできます。これはオプションです

ハイブリッドクラウドデータベース環境の管理を簡易化するために、ネットアップでは Ansible コントローラを導入して、コンピューティングインスタンスをオンプレミスやクラウドに同期させるなどの一部の管理タスクを自動化することを強く推奨していますが、必須ではありません。特に重要なのは、クラウド内の同期されていないコンピューティングインスタンスが原因で、カーネルパッケージやその他の問題が原因で、リカバリされたデータベースがクラウドエラーになる可能性があるためです。

Ansible コントローラの自動化機能を使用して、SnapMirror インスタンスの解除などの特定のタスクで SnapCenter を補強し、本番環境で DR データコピーをアクティブ化することもできます。

以下の手順に従って、RedHat または CentOS マシン用の Ansible コントロールノードをセットアップします。"[RedHat / CentOS Ansible コントローラのセットアップ](#)"。Ubuntu または Debian マシン用の Ansible の制御ノードをセットアップするには、次の手順に従います。"[Ubuntu / Debian Ansible のコントローラセットアップ](#)"。

パブリッククラウドの前提条件

Cloud Manager Connector と Cloud Volumes ONTAP をインストールして SnapMirror を設定する前に、クラウド環境向けの準備を行う必要があります。このページでは、Cloud Volumes ONTAP を導入する際に考慮すべき点と同様に、実行する必要がある作業について説明します。

Cloud Manager と Cloud Volumes ONTAP の導入の前提条件チェックリスト

- NetApp Cloud Central へのログイン
- Web ブラウザから複数のエンドポイントへのネットワークアクセス
- コネクタのネットワーク上の場所
- クラウドプロバイダの権限
- 個々のサービスのネットワーク

開始する必要がある項目の詳細については、を参照してください "[クラウドのドキュメント](#)"。

考慮事項

1. Cloud Manager Connector とは

ほとんどの場合、Cloud Central アカウント管理者はクラウドまたはオンプレミスネットワークにコネクタを導入する必要があります。Connector を使用すると、Cloud Manager でパブリッククラウド環境内のリソースとプロセスを管理できます。

コネクタの詳細については、を参照してください "[クラウドのドキュメント](#)"。

2. Cloud Volumes ONTAP のサイジングとアーキテクチャ

Cloud Volumes ONTAP を導入する際には、事前定義されたパッケージを選択するか、独自の設定を作成するかを選択できます。これらの値の多くはあとで無停止で変更することができますが、クラウドに導入するワー

クラウドに基づいていくつかの重要な決定を行う必要があります。

クラウドプロバイダごとに導入オプションが異なり、ほぼすべてのワークロードに独自のプロパティがあります。ネットアップには、があります ["CVO のサイジングツール"](#) これは、容量とパフォーマンスに基づいて導入の規模を正しく決定するのに役立ちますが、次の点を考慮していくつかの基本的な概念を中心に構築されています。

- 容量が必要です
- クラウド仮想マシンのネットワーク機能
- クラウドストレージのパフォーマンス特性

重要な点は、現在の容量とパフォーマンスの要件を満たすだけでなく、将来の拡張も考慮する構成を計画することです。これは、一般に容量ヘッドルームおよびパフォーマンスヘッドルームと呼ばれます。

詳細については、の計画に関するドキュメントを参照してください ["AWS"](#)、["Azure"](#) および ["GCP"](#)。

3. シングルノードとハイアベイラビリティのどちらか？

どのクラウドでも、CVO を導入できるノードは 1 つだけです。2 つのノードで構成されるクラスタハイアベイラビリティペアにもなります。ユースケースによっては、コストを削減するためにシングルノードを導入したり、可用性と冗長性を向上させるために HA ペアを導入したりすることができます。

DR のユースケースでは、開発とテストのために一時的なストレージをスピンアップする場合でも、突然のゾーンの停止やインフラの停止による影響が小さいため、シングルノードが一般的です。ただし、本番環境では、データが 1 箇所だけに格納されている場合や、データセットの冗長性と可用性を高める必要がある場合に、高可用性を推奨します。

各クラウドバージョンのハイアベイラビリティのアーキテクチャの詳細については、のドキュメントを参照してください ["AWS"](#)、["Azure"](#) および ["GCP"](#)。

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。