Cloud Manager および Cloud Volumes ONTAP のドキュメント

Cloud Manager 3.7

NetApp
March 25, 2024

目次

Cloud Manager および Cloud Volumes ONTAP のドキュメント

Cloud Manager を使用すると、 NetApp Cloud Volumes ONTAP を導入して管理できます。 NetApp Cloud Volumes ONTAP は、クラウドベースのワークロードを保護、可視化、制御するデータ管理ソリューションです。

BlueXP

NetApp BlueXPは、Cloud Managerを通じて提供される機能を拡張、強化します。

"BlueXPのドキュメントにアクセス"

最新情報をご確認ください

- "Cloud Manager の新機能"
- "Cloud Volumes ONTAP の新機能"

はじめに

- "AWS を始めましょう"
- "Azure で始めましょう"
- "Google クラウドプラットフォームをご利用ください"
- "Cloud Volumes ONTAP でサポートされている構成を検索します"
- "Cloud Manager のネットワーク要件を確認します"
- "Cloud Volumes ONTAP for AWS のネットワーク要件を確認します"
- "Cloud Volumes ONTAP for Azure のネットワーク要件を確認します"
- "Cloud Volumes ONTAP for GCP のネットワーキング要件を確認します"
- "Cloud Volumes ONTAP の構成を計画します"

API による自動化

- "API 開発者ガイド"
- "自動化のサンプル"

同僚とつながり、サポートを受け、詳細情報を入手します

- "ネットアップコミュニティ：クラウドデータサービス"
- "NetApp Cloud Volumes ONTAP のサポート"
- "ヘルプを参照したり、詳細情報を参照したりするには"

リリースノート

クラウドマネージャ

Cloud Manager 3.7 の新機能

通常、 Cloud Manager では毎月新しいリリースが導入され、新機能、拡張機能、およびバグ修正が提供されます。

以前のリリースをお探しですか？"3.6 の新機能"
"3.5 の新機能"
"3.4 の新機能"

Cloud Manager 3.7.5 の更新（ 2019 年 12 月 16 日）

この更新プログラムには、次の拡張機能が含まれてい

- Cloud Volumes ONTAP 9.7
- Cloud Volumes ONTAP 向けクラウドコンプライアンス

Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 が、 AWS 、 Azure 、 Google Cloud Platform で利用できるようになりました。

"Cloud Volumes ONTAP 9.7 の新機能を参照してください"。

Cloud Volumes ONTAP 向けクラウドコンプライアンス

Cloud Compliance は、 AWS と Azure での Cloud Volumes ONTAP 向けのデータプライバシーとコンプライアンスのサービスです。人工知能（ AI ）ベースのテクノロジを使用したクラウドコンプライアンスは、データコンテキストを把握し、 Cloud Volumes ONTAP システム全体で機密データを特定するのに役立ちます。

Cloud Compliance は現在、限定リリースとして提供されています。

"Cloud Compliance の詳細はこちらをご覧ください"。

Cloud Manager 3.7.5 （ 2019 年 12 月 3 日）

Cloud Manager 3.7.5 では、次の機能が強化されています。

- GCP の Cloud Volumes ONTAP では高速の書き込み速度です
- オンプレミスの ONTAP クラスタを Kubernetes の永続的ストレージとして使用
- Kubernetes 向けの最新の Trident バージョン
- Azure 汎用 v2 ストレージアカウントをサポート
- API を使用して Azure ストレージアカウント名にプレフィックスが追加されます

GCP の Cloud Volumes ONTAP では高速の書き込み速度です

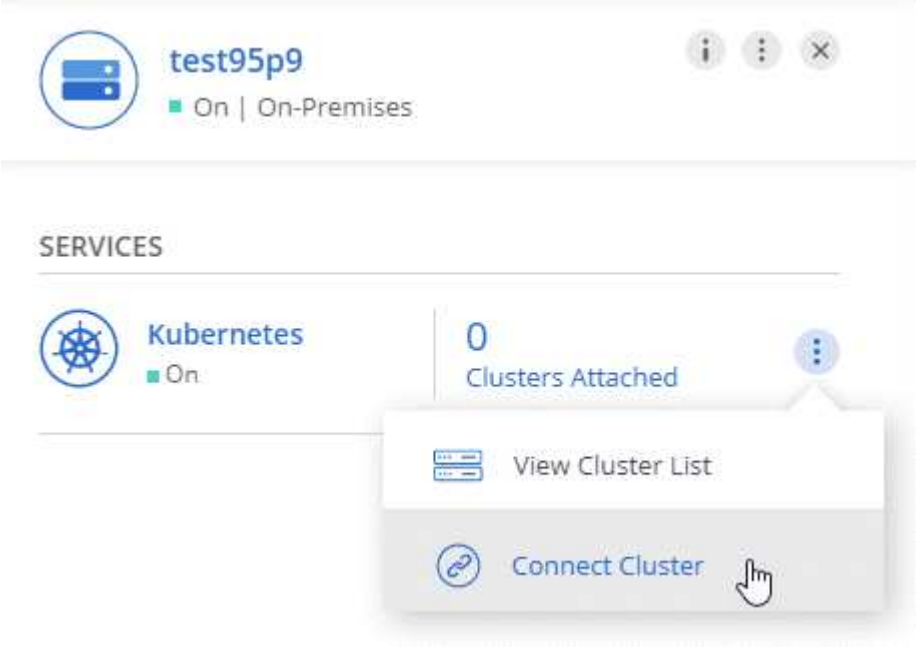
Google Cloud Platform の新規および既存の Cloud Volumes ONTAP システムで高速書き込みを有効にできるようになりました。ワークロードに高速な書き込みパフォーマンスが必要な場合は、高速の書き込み速度を使用することを推奨します。

- "書き込み速度を選択する方法について説明します"
- "既存のシステムの書き込み速度を変更する方法について説明します"

オンプレミスの ONTAP クラスタを Kubernetes の永続的ストレージとして使用

Cloud Manager では、オンプレミスの ONTAP クラスタをコンテナ用の永続的ストレージとして使用できるようになりました。Cloud Volumes ONTAP と同様に、 Cloud Manager は NetApp Trident の導入を自動化し、は ONTAP を Kubernetes クラスタに接続します。

Kubernetes クラスタを Cloud Manager に追加したら、作業環境のページから Kubernetes クラスタをオンプレミスの ONTAP クラスタに接続できます。



"開始方法をご確認ください"。

Kubernetes 向けの最新の Trident バージョン

作業環境を Kubernetes クラスタに接続すると、 Cloud Manager によって Trident の最新バージョン（バージョン 19.07.1 ）がインストールされるようになりました。

Azure 汎用 v2 ストレージアカウントをサポート

Azure に新しい Cloud Volumes ONTAP システムを導入すると、 Cloud Manager が診断やデータ階層化用に作成するストレージアカウントが汎用 v2 のストレージアカウントになります。

API を使用して Azure ストレージアカウント名にプレフィックスが追加されます

Cloud Manager で Cloud Volumes ONTAP 用に作成する Azure ストレージアカウントの名前にプレフィック

スを追加できるようになりました。Azure に新しい Cloud Volumes ONTAP システムを導入する場合は、*storageAccountPrefix* パラメータを使用してください。

"API の使用の詳細については、『API 開発者ガイド』を参照してください"。

Cloud Manager 3.7.4 （2019 年 10 月 6 日）

Cloud Manager 3.7.4 では、次の機能が強化されています。

- Azure NetApp Files のサポート
- Cloud Volumes ONTAP for GCP の機能強化
- S3 へのバックアップの機能拡張
- AWS のブートディスクとルートディスクの暗号化
- AWS バーレーンリージョンがサポートされます
- Azure UAE 北部をサポート

Azure NetApp Files のサポート

Azure NetApp Files の NFS ボリュームを Cloud Manager から直接表示および作成できるようになりました。この機能強化は、クラウドストレージを単一のインターフェイスから管理できるようにすることを目的としています。

"開始方法をご確認ください"。

この機能を使用するには、最新ので示されている新しい権限が必要です "Azure 向け Cloud Manager ポリシー"。

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

Cloud Volumes ONTAP for GCP の機能強化

Cloud Manager 3.7.4 では、 Cloud Volumes ONTAP for Google Cloud Platform の次の機能が拡張されました。

GCP Marketplace での従量課金制サブスクリプション

Google Cloud Platform Marketplace で Cloud Volumes ONTAP に登録すれば、 Cloud Volumes ONTAP の料金を支払うことができます。

"Google Cloud Platform Marketplace ： Cloud Manager for Cloud Volumes ONTAP"

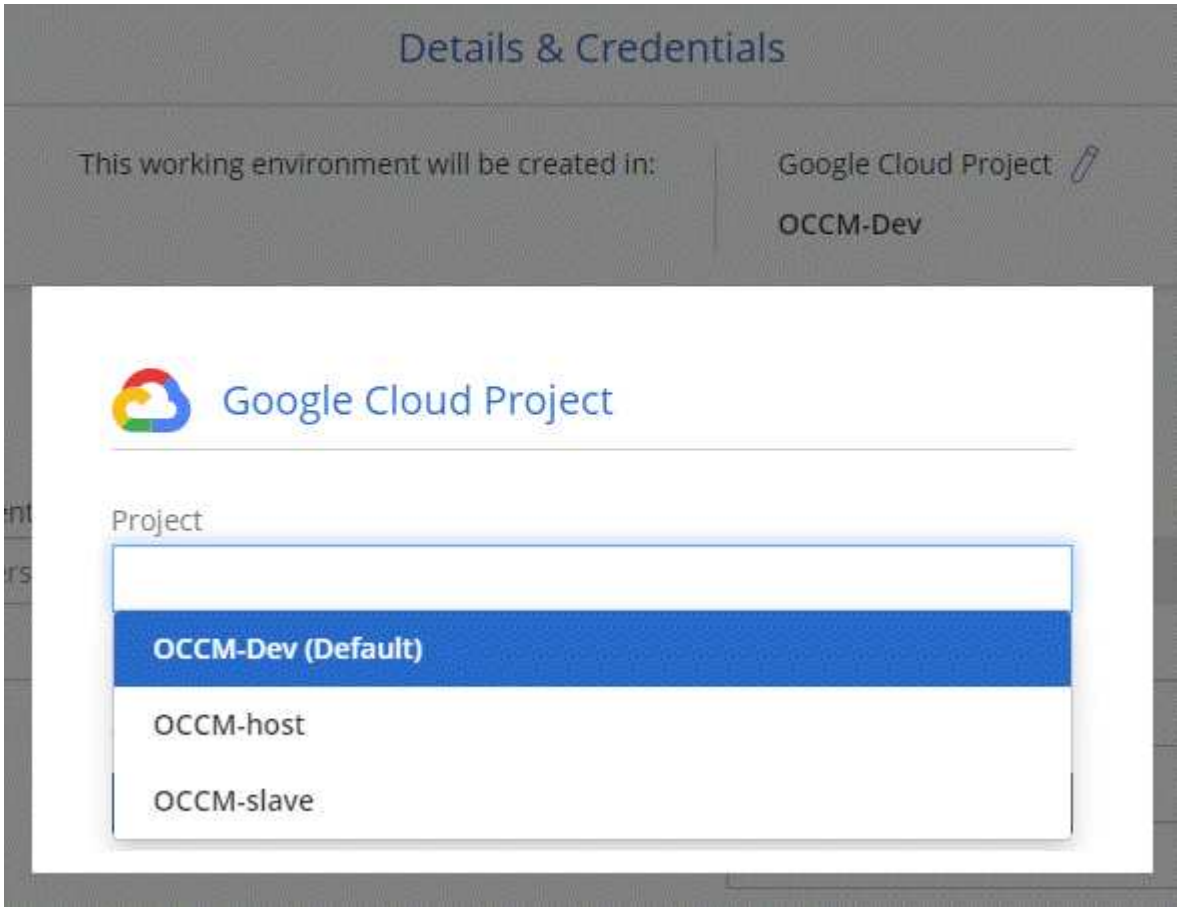
共有 **VPC**

Cloud Manager と Cloud Volumes ONTAP が Google Cloud Platform の共有 VPC でサポートされるようになりました。

共有 VPC を使用すると、複数のプロジェクトの仮想ネットワークを設定し、一元管理できます。共有 VPC ネットワークを *host project* でセットアップし、サービス project_ に Cloud Manager と Cloud Volumes ONTAP の仮想マシンインスタンスを導入できます。 "Google Cloud のドキュメント：「 Shared VPC Overview"。

複数の **Google Cloud** プロジェクト

Cloud Volumes ONTAP を Cloud Manager と同じプロジェクトに含める必要はなくなりました。Cloud Manager サービスアカウントとロールを追加のプロジェクトに追加し、 Cloud Volumes ONTAP を導入するプロジェクトから選択できます。



Cloud Manager サービスアカウントの設定の詳細については、 "このページの手順 4b を参照してください"。

Cloud Manager API を使用する場合、お客様が管理する暗号化キー

Google Cloud Storage では常にデータが暗号化されてからディスクに書き込まれますが、 Cloud Manager API を使用して、 _cuser-managed 暗号化キー _ を使用する新しい Cloud Volumes ONTAP システムを作成できます。これらは、 Cloud Key Management Service を使用して GCP で生成および管理するキーです。

を参照してください "API 開発者ガイド" "GcpEncryption" パラメータの使用方法の詳細については、を参照してください。

この機能を使用するには、最新ので示されている新しい権限が必要です "GCP 向け Cloud Manager ポリシー"：

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

S3 へのバックアップの機能拡張

これで、既存ボリュームのバックアップを削除できるようになります。以前は、削除できたのは削除されたボリュームのバックアップだけでした。

"S3 へのバックアップに関する詳細情報"。

AWS のブートディスクとルートディスクの暗号化

AWS Key Management Service （ KMS ；キー管理サービス）を使用したデータ暗号化を有効にすると、Cloud Volumes ONTAP のブートディスクとルートディスクも暗号化されるようになりました。これには、HA ペアのメディエーターインスタンスのブートディスクが含まれます。ディスクは、作業環境の作成時に選択した CMK を使用して暗号化されます。

> ブートディスクとルートディスクは、これらのクラウドプロバイダではデフォルトで暗号化が有効になるため、 Azure と Google Cloud Platform では常に暗号化されます。

AWS バーレーンリージョンがサポートされます

Cloud Manager と Cloud Volumes ONTAP は、 AWS Middle East （バーレーン）リージョンでサポートされるようになりました。

Azure UAE 北部をサポート

Cloud Manager と Cloud Volumes ONTAP は、 Azure UAE 北部でサポートされるようになりました。

"サポートされているすべてのリージョンを表示し"。

Cloud Manager 3.7.3 の更新（ 2019 年 9 月 15 日）

Cloud Manager で、 Cloud Volumes ONTAP から Amazon S3 にデータをバックアップできるようになりました。

S3 へのバックアップ

S3 へのバックアップは、クラウドデータを完全に管理して保護するバックアップとリストアの機能を提供する、 Cloud Volumes ONTAP 向けのアドオンサービスです。バックアップは、ほぼ長期のリカバリやクローニングに使用されるボリュームの Snapshot コピーとは無関係に S3 オブジェクトストレージに格納されます。

"開始方法をご確認ください"。

この機能を使用するには、を更新する必要があります "Cloud Manager ポリシー"。現在、次の VPC エンドポイント権限が必要です。

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Cloud Manager 3.7.3 （2019 年 9 月 11 日）

Cloud Manager 3.7.3 では、次の機能が強化されています。

- Cloud Volumes Service for AWS の検出および管理
- AWS Marketplace での新しいサブスクリプションが必要です
- AWS GovCloud （米国東部）のサポート

Cloud Volumes Service for AWS の検出および管理

Cloud Manager ので Cloud Volume を検出できるようになりました "Cloud Volumes Service for AWS" サブスクリプション。検出後、 Cloud Volume は Cloud Manager から直接追加できます。この機能拡張により、単一のコンソールからネットアップのクラウドストレージを管理できます。

"開始方法をご確認ください"。

AWS Marketplace での新しいサブスクリプションが必要です

"AWS Marketplace で新しいサブスクリプションが提供されています"。Cloud Volumes ONTAP 9.6 PAYGO を導入するには、この 1 回限りのサブスクリプションが必要です（ 30 日間の無償トライアルシステムを除く）。サブスクリプションでは、 Cloud Volumes ONTAP PAYGO および BYOL のアドオン機能も提供できます。作成した Cloud Volumes ONTAP PAYGO システムごと、および有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。

バージョン 9.6 以降では、この新しいサブスクリプション方式で、 Cloud Volumes ONTAP PAYGO の既存の 2 つの AWS Marketplace サブスクリプションが置き換えられました。からのサブスクリプションが必要です "Cloud Volumes ONTAP BYOL を導入する際の既存の AWS Marketplace のページ"。

"各 AWS Marketplace のページについては、こちらをご覧ください"。

AWS GovCloud （米国東部）のサポート

Cloud Manager と Cloud Volumes ONTAP が AWS GovCloud （ US-East ）リージョンでサポートされるようになりました。

GCP で Cloud Volumes ONTAP が一般提供されています （2019 年 9 月 3 日）

Cloud Volumes ONTAP は、お客様が独自のライセンスを使用（ BYOL ）したときに、一般的に Google Cloud Platform （ GCP ）で利用できるようになりました。従量課金制のプロモーションもご利用いただけます。このキャンペーンでは、無制限のシステム数のライセンスが無料で提供されており、 2019 年 9 月末に有効期限が切れます。

- "GCP の使用を開始する方法をご確認ください"
- "サポートされている構成を表示する"

Cloud Manager 3.7.2 （2019 年 8 月 5 日）

- FlexCache ライセンス
- iSCSI 用の Kubernetes ストレージクラス
- inode の管理
- AWS での香港リージョンのサポート
- Azure のオーストラリア中部リージョンのサポート

FlexCache ライセンス

Cloud Manager で、すべての新しい Cloud Volumes ONTAP システム用の FlexCache ライセンスが生成されるようになりました。ライセンスの使用量は 500GB に制限されています。

ライセンスを生成するには、 Cloud Manager から https://ipa-signer.cloudmanager.netapp.com にアクセスする必要があります。この URL にファイアウォールからアクセスできることを確認してください。

iSCSI 用の Kubernetes ストレージクラス

Cloud Volumes ONTAP を Kubernetes クラスタに接続すると、 Cloud Manager は、 iSCSI 永続ボリュームで使用できる Kubernetes ストレージクラスを 2 つ追加で作成するようになりました。

- * NetApp-file-san* ： iSCSI パーシステントボリュームをシングルノードの Cloud Volumes ONTAP システムにバインドする場合
- * NetApp-file-redundant-san * ： iSCSI 永続的ボリュームを Cloud Volumes ONTAP HA ペアにバインドする場合

inode の管理

Cloud Manager でボリュームの inode の使用量が監視されるようになりました。inode の 85% を使用すると、 Cloud Manager はボリュームのサイズを増やして、使用可能な inode の数を増やします。ボリュームに含めることができるファイル数は、ボリューム内の inode の数によって決まります。

> Cloud Manager は、容量管理モードが自動（デフォルト設定）に設定されている場合にのみ inode 使用量を監視します。

AWS での香港リージョンのサポート

Cloud Manager と Cloud Volumes ONTAP が AWS のアジア太平洋（香港）リージョンでサポートされるようになりました。

Azure のオーストラリア中部リージョンのサポート

Cloud Manager と Cloud Volumes ONTAP が次の Azure リージョンでサポートされるようになりました。

- オーストラリア中部
- オーストラリアセントラル 2.

"サポートされているリージョンの一覧を参照してください"。

バックアップとリストアに関する最新情報（ **2019** 年 **7** 月 **15** 日）

3.7.1 リリース以降、 Cloud Manager では、バックアップのダウンロードとリストアに使用する Cloud Manager の設定はサポートされなくなりました。 "Cloud Manager をリストアするには、次の手順を実行する必要があります"。

Cloud Manager 3.7.1 （ **2019** 年 **7** 月 **1** 日）

- このリリースには主にバグ修正が含まれています。
- 拡張機能が 1 つ含まれています。 Cloud Manager は、ネットアップサポートに登録されている各 Cloud Volumes ONTAP システム（新規および既存の両方のシステム）に NetApp Volume Encryption （ NVE ）ライセンスをインストールするようになりました。
  - "Cloud Manager へのネットアップサポートサイトのアカウントの追加"
  - "従量課金制システムの登録"
  - "NetApp Volume Encryption のセットアップ"

> Cloud Manager は、中国地域のシステムに NVE ライセンスをインストールしません。

Cloud Manager 3.7 の更新（ **2019** 年 **6** 月 **16** 日）

Cloud Volumes ONTAP 9.6 は、 AWS 、 Azure 、 Google Cloud Platform でプライベートプレビューとして利用できるようになりました。プライベートプレビューに参加するには、 ng-Cloud-Volume-ONTAP-preview@netapp.com にリクエストを送信します。

"Cloud Volumes ONTAP 9.6 の新機能をご覧ください"

Cloud Manager 3.7 （ **2019** 年 **6** 月 **5** 日）

- 今後の Cloud Volumes ONTAP 9.6 リリースでサポートされる予定です
- NetApp Cloud Central アカウント
- Cloud Backup Service を使用したバックアップとリストア

今後の **Cloud Volumes ONTAP 9.6** リリースでサポートされる予定です

Cloud Manager 3.7 では、次回の Cloud Volumes ONTAP 9.6 リリースがサポートされます。9.6 リリースには、 Cloud Volumes ONTAP のプライベートプレビューが Google Cloud Platform に含まれています。9.6 が利用可能になったらリリースノートを更新します。

NetApp Cloud Central アカウント

クラウドリソースの管理方法が強化されました。各 Cloud Manager システムには、 _NetApp Cloud Central アカウント _ が関連付けられます。このアカウントはマルチテナンシーに対応しており、将来的には他のネットアップクラウドデータサービスにも対応する予定です。

Cloud Manager では、 Cloud Central アカウントは、 Cloud Volumes ONTAP を導入する Cloud Manager システムおよび _ ワークスペース _ のコンテナです。

"Cloud Central アカウントでマルチテナンシーを実現する方法をご確認ください"。

> Cloud Central アカウントサービスに接続するためには、 Cloud Manager から https://cloudmanager.cloud.netapp.com_ にアクセスする必要があります。ファイアウォールでこの URL を開いて、 Cloud Manager がサービスに接続できることを確認します。

システムと **Cloud Central** アカウントの統合

クラウドマネージャ 3.7 にアップグレードした後、クラウドセントラルアカウントと統合するために、特定のクラウドマネージャシステムを選択する予定です。アカウントを作成し、各ユーザに新しいロールを割り当ててワークスペースを作成し、既存の作業環境をワークスペースに配置します。Cloud Volumes ONTAP システムが停止することはありません。

"質問がある場合は、この FAQ を参照してください。"。

Cloud Backup Service を使用したバックアップとリストア

NetApp Cloud Backup Service for Cloud Volumes ONTAP は、クラウドデータの保護と長期保管のためのフルマネージドのバックアップ / リストア機能を提供します。Cloud Backup Service と Cloud Volumes ONTAP for AWS を統合できます。サービスによって作成されたバックアップは、 AWS S3 オブジェクトストレージに格納されます。

"Cloud Backup Service の詳細については、こちらをご覧ください"。

バックアップエージェントをインストールして設定し、バックアップとリストアの処理を開始します。サポートが必要な場合は、 Cloud Manager のチャットアイコンを使用してお問い合わせください。

> この手動プロセスはサポートされなくなりました。S3 へのバックアップ機能は、 3.7.3 リリースで Cloud Manager に統合されました。

既知の問題

既知の問題は、このリリースの製品を正常に使用できない可能性のある問題を特定します。

このリリースの Cloud Manager には既知の問題はありません。

Cloud Volumes ONTAP の既知の問題については、を参照してください 。 "Cloud Volumes ONTAP リリースノート" および ONTAP ソフトウェアについては、を参照してください "ONTAP リリースノート"。

既知の制限

既知の制限事項は、このリリースの製品でサポートされていないプラットフォーム、デバイス、機能、または製品と正しく相互運用できない機能を特定します。これらの制限事項を慎重に確認してください

Cloud Manager は常時実行されている必要があります

Cloud Manager は、 Cloud Volumes ONTAP の健全性と課金において重要な要素です。Cloud Manager の電源がオフになっている場合、 Cloud Manager との通信が失われてから 4 日以上が経過すると Cloud Volumes ONTAP システムがシャットダウンします。

共有 **Linux** ホストはサポートされません

他のアプリケーションと共有しているホストでは、 Cloud Manager はサポートされません。専用のホストである必要があります。

Cloud Manager では **FlexGroup** ボリュームはサポートされません

Cloud Volumes ONTAP では FlexGroup ボリュームがサポートされますが、 Cloud Manager ではサポートされません。System Manager または CLI から FlexGroup ボリュームを作成する場合は、 Cloud Manager の容量管理モードを手動に設定する必要があります。FlexGroup ボリュームで自動モードが適切に機能しない可能性があります。

Cloud Manager の新規インストールでは、 **Active Directory** はデフォルトでサポートされていません

バージョン 3.4 以降では、 Cloud Manager を新規にインストールした場合、組織の Active Directory 認証を使用したユーザ管理はサポートされません。必要に応じて、 Cloud Manager を使用した Active Directory のセットアップをネットアップがサポートします。Cloud Manager の右下にあるチャットアイコンをクリックすると、サポートを受けることができます。

AWS GovCloud （米国）地域の制限

- AWS GovCloud （ US ）リージョンで Cloud Volumes ONTAP インスタンスを起動する場合は、 Cloud Manager を AWS GovCloud （ US ）リージョンに導入する必要があります。
- AWS GovCloud （ US ）リージョンに導入されている場合、 Cloud Manager は、 Microsoft Azure 構成用の NetApp プライベートストレージまたは SoftLayer 構成用の NetApp プライベートストレージ内の ONTAP クラスタを検出できません。

Cloud Manager は **iSCSI** ボリュームをセットアップしません

Storage System View を使用して Cloud Manager でボリュームを作成する場合は、 NFS または CIFS プロトコルを選択できます。iSCSI 用のボリュームを作成するには、 OnCommand System Manager を使用する必要があります。

Storage Virtual Machine （ **SVM** ）の制限

Cloud Volumes ONTAP は、 1 つのデータサービス SVM と、災害復旧に使用される 1 つ以上の SVM をサポートします。1 つのデータ提供用 SVM は、 Cloud Volumes ONTAP システム全体（ HA ペアまたはシングルノード）にまたがります。

Cloud Manager では、 SVM ディザスタリカバリのセットアップやオーケストレーションはサポートされません。また、追加の SVM ではストレージ関連のタスクをサポートしません。SVM ディザスタリカバリには、 System Manager または CLI を使用する必要があります。

概念

Cloud Manager と Cloud Volumes ONTAP の概要

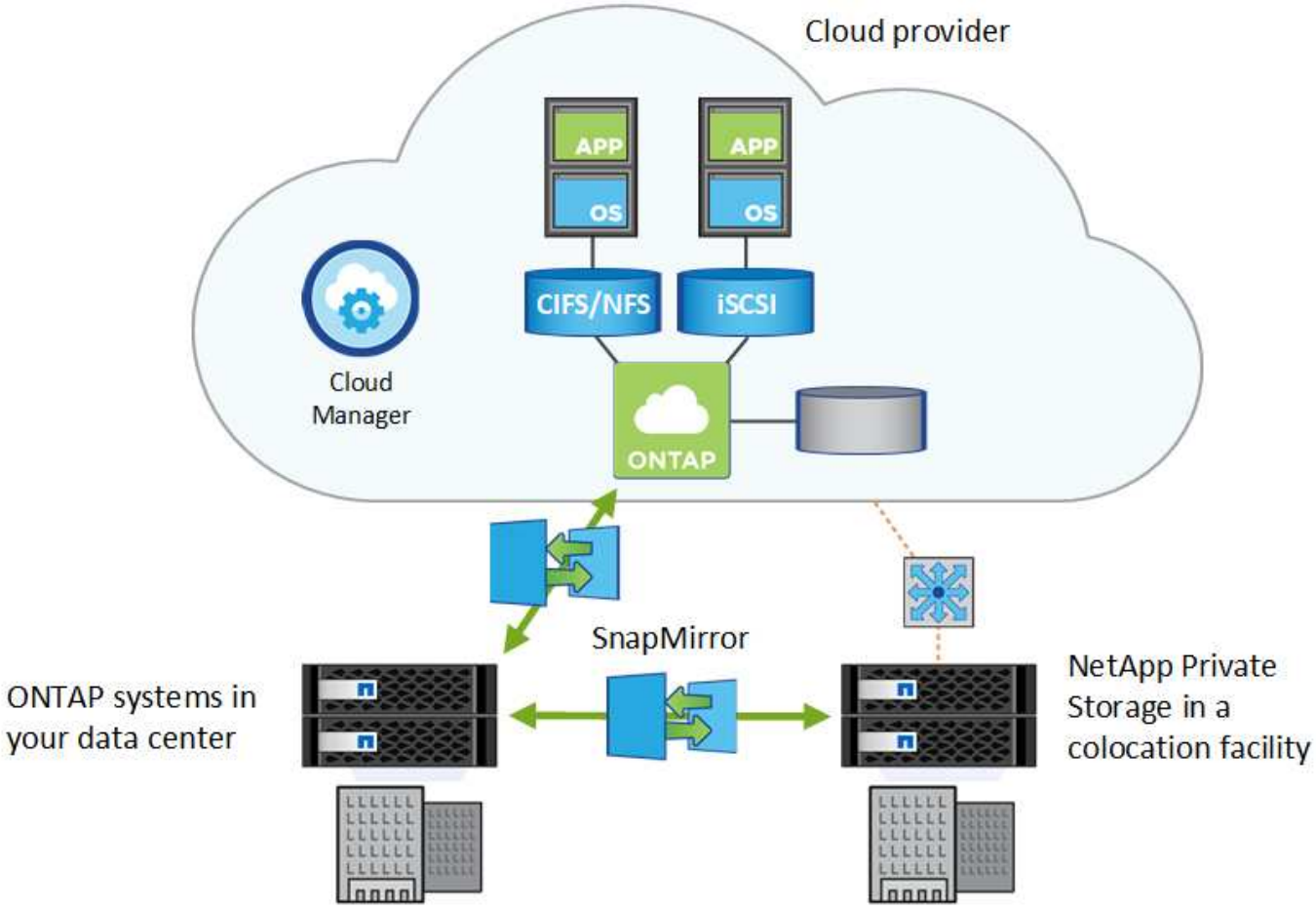
Cloud Manager を使用すると、 Cloud Volumes ONTAP を導入できます。これにより、クラウドストレージでエンタープライズクラスの機能を利用できます。また、ネットアップを基盤に構築されたハイブリッドクラウド全体でデータを簡単にレプリケートできます。

クラウドマネージャ

Cloud Manager は、シンプルさを念頭に置いて構築されています。Cloud Volumes ONTAP のセットアップ手順を順を追って説明します。ストレージプロビジョニングの簡易化と容量管理の自動化を実現し、ハイブリッドクラウド全体でのドラッグアンドドロップによるデータレプリケーションを可能にすることで、データ管理を簡易化します。

Cloud Manager は、 Cloud Volumes ONTAP の導入と管理に必要ですが、オンプレミスの ONTAP クラスタのストレージの検出とプロビジョニングも可能です。これにより、クラウドとオンプレミスのストレージインフラを一元管理できます。

Cloud Manager は、クラウドまたはネットワークで実行できます。 Cloud Volumes ONTAP を導入するネットワークに接続するだけで済みます。次の図は、クラウドプロバイダで実行されている Cloud Manager と Cloud Volumes ONTAP を示しています。また、ハイブリッドクラウド全体のデータレプリケーションも示しています。



"Cloud Manager の詳細については、こちらをご覧ください"

Cloud Volumes ONTAP

Cloud Volumes ONTAP は、 ONTAP データ管理ソフトウェアをクラウドで実行するソフトウェア専用のストレージアプライアンスです。Cloud Volumes ONTAP は、本番ワークロード、ディザスタリカバリ、 DevOps 、ファイル共有、データベース管理に使用できます。

Cloud Volumes ONTAP では、次の主要な機能を使用して、エンタープライズストレージをクラウドに拡張します。

- ストレージの効率化：組み込みのデータ重複排除機能、データ圧縮機能、シンプロビジョニング機能、クローニング機能を活用して、ストレージコストを最小限に抑えます。
- 高可用性は、クラウド環境で障害が発生した場合にエンタープライズクラスの信頼性と継続的な運用を実現します。
- Data Replication Cloud Volumes ONTAP は、ネットアップの業界をリードするレプリケーションテクノロジである SnapMirror を活用してオンプレミスデータをクラウドにレプリケートするため、複数のユースケースでセカンダリコピーを簡単に使用できます。
- アプリケーションをオフラインにすることなく、オンデマンドでハイパフォーマンスストレージプールと低パフォーマンスストレージプールの間のデータ階層化スイッチを切り替えます。
- アプリケーションの整合性 NetApp SnapCenter を使用して、 NetApp Snapshot コピーの整合性を確保します。

ONTAP 機能のライセンスは、 Cloud Volumes ONTAP に含まれています。

"サポートされている Cloud Volumes ONTAP 構成を表示します"

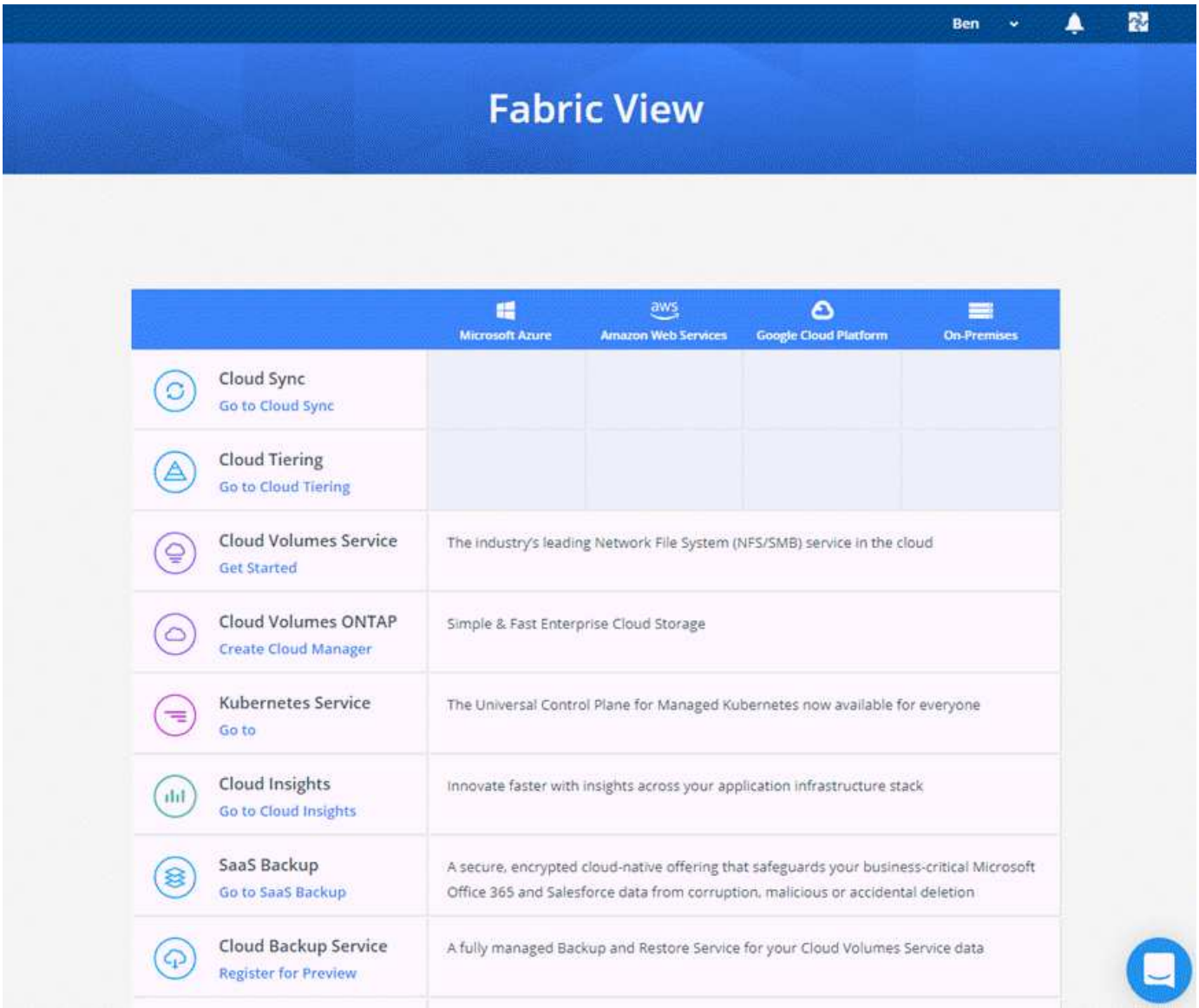
"Cloud Volumes ONTAP の詳細については、こちらを参照してください"

NetApp Cloud Central

"NetApp Cloud Central" ネットアップのクラウドデータサービスにアクセスして管理するための一元的な場所を提供します。これらのサービスを利用すると、重要なアプリケーションをクラウドで実行したり、自動化された DR サイトを作成したり、 SaaS データをバックアップしたり、複数のクラウド間でデータを効果的に移行および制御したりすることができます。

Cloud Manager と NetApp Cloud Central を統合すると、導入環境の簡易化、複数の Cloud Manager システムの表示と管理を行う単一の場所、ユーザ認証の一元化など、いくつかのメリットが得られます。

一元的なユーザ認証では、 Cloud Manager システム全体、および Cloud Manager と他のデータサービス（ Cloud Sync など）の間で同じクレデンシャルセットを使用できます。パスワードを忘れた場合は、簡単にリセットできます。



Cloud Central アカウント

各 Cloud Manager システムには、 _NetApp Cloud Central アカウント _ が関連付けられています。Cloud Central アカウントはマルチテナンシーを提供し、分離されたワークスペースでユーザやリソースを整理することができます。

Cloud Central アカウントでは、マルチテナンシーが可能です。

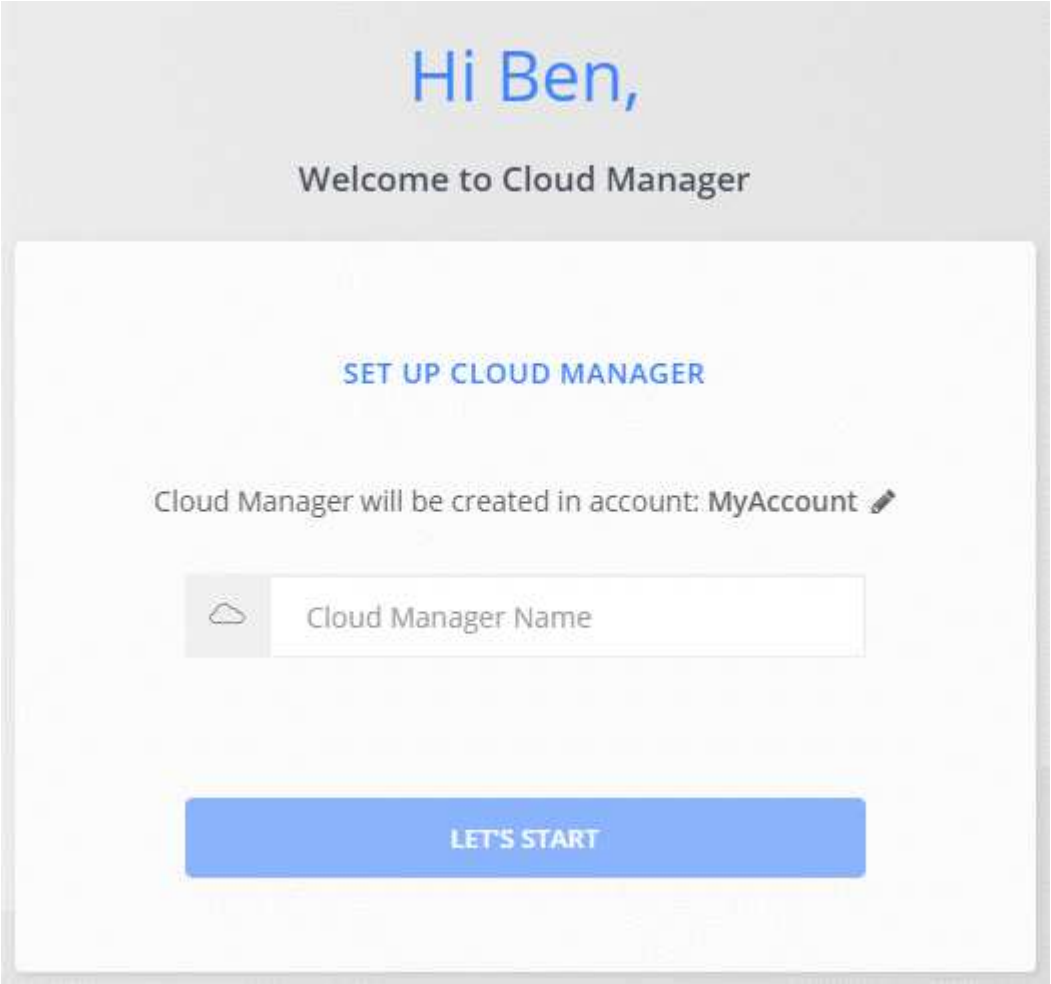
- 単一のクラウドセントラルアカウントには、さまざまなビジネスニーズに対応する複数のクラウドマネージャシステムを含めることができます。

  ユーザは Cloud Central アカウントに関連付けられるため、 Cloud Manager システムごとにユーザを設定する必要はありません。

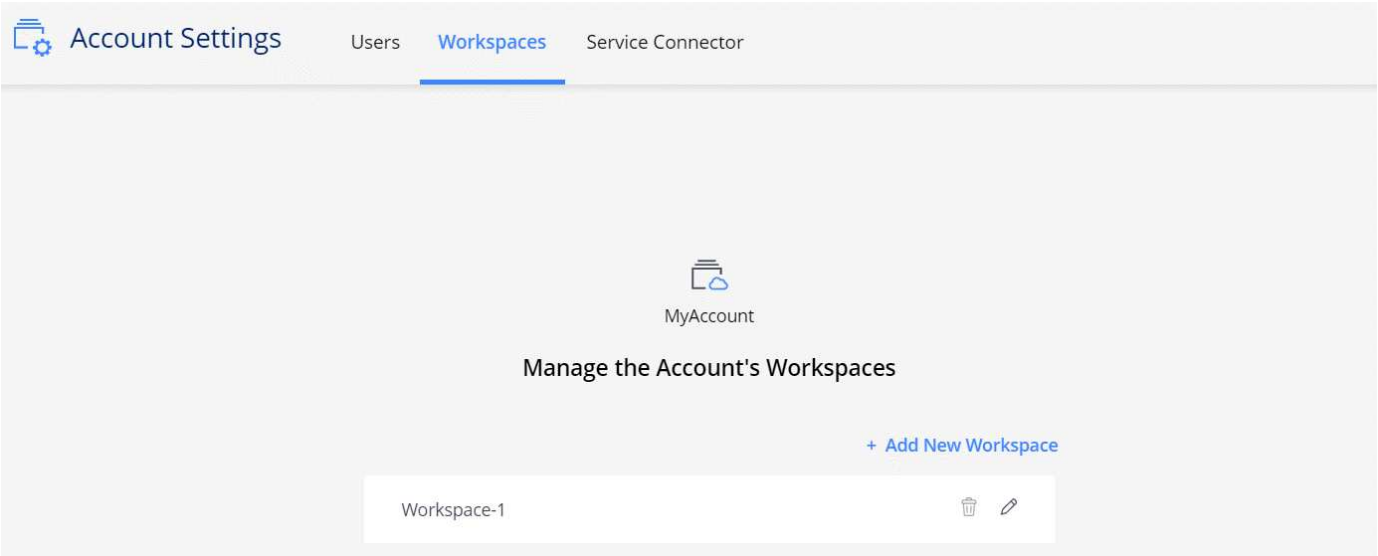
- 各 Cloud Manager システム内では、複数のユーザが、ワークスペースと呼ばれる分離された環境に Cloud Volumes ONTAP システムを導入して管理できます。

  これらのワークスペースは、共有されていない限り、他のユーザーには表示されません。

Cloud Manager を導入する場合は、システムに関連付ける Cloud Central アカウントを選択します。



アカウント管理者は、ユーザー、ワークスペース、サービスコネクタを管理することで、このアカウントの設定を変更できます。



手順については、を参照してください "Cloud Central アカウントをセットアップします"。

Cloud Central アカウントサービスに接続するためには、 Cloud Manager から https://cloudmanager.cloud.netapp.com_ にアクセスする必要があります。ファイアウォールでこの URL を開いて、 Cloud Manager がサービスに接続できることを確認します。

ユーザ、ワークスペース、およびサービスコネクタ

Cloud Manager の ［アカウント設定］ ウィジェットを使用すると、アカウント管理者は Cloud Central アカウントを管理できます。アカウントを作成したばかりの場合は、最初から作成します。アカウントをすでに設定している場合は、アカウントに関連付けられているユーザ、ワークスペース、サービスコネクタが *ALL* と表示されます。

ユーザ

これらは、 Cloud Central アカウントに関連付けられている NetApp Cloud Central ユーザです。ユーザーをアカウントに関連付け、そのアカウント内の 1 つ以上のワークスペースを使用すると、ユーザーは Cloud Manager で作業環境を作成して管理できます。

ユーザを関連付けると、ユーザにロールが割り当てられます。

- *Account Admin* ： Cloud Manager で任意の操作を実行できます。
- _ ワークスペース管理者 _ ：割り当てられたワークスペースでリソースを作成および管理できます。

ワークスペース

Cloud Manager では、ワークスペースによって、いくつかの _ 作業環境 _ が他の作業環境から分離されます。アカウント管理者がそのワークスペースに管理者を関連付けないと、ワークスペース管理者はワークスペース内の作業環境にアクセスできません。

稼働環境はストレージシステムを表します。

- シングルノードクラウドボリューム ONTAP システムまたは HA ペア
- ネットワーク内のオンプレミス ONTAP クラスタ
- NetApp プライベートストレージ構成の ONTAP クラスタ

サービスコネクタ

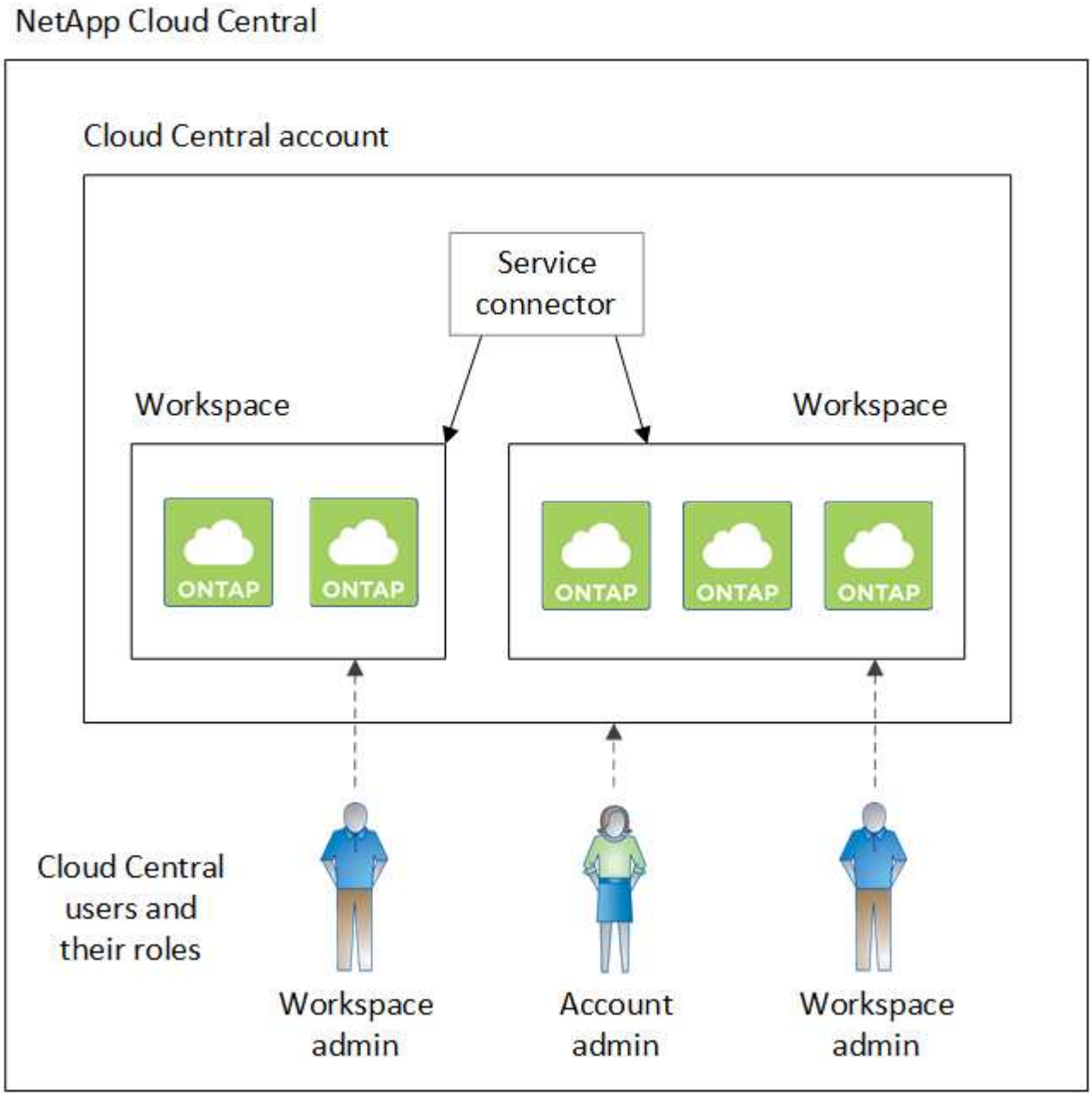
Service Connector は Cloud Manager の一部です。クラウドマネージャソフトウェアの多く（ユーザインターフェイスなど）が実行されますが、接続先のクラウドセントラルサービス（ Auth0 アカウントと Cloud Central アカウント）がいくつかあります。Service Connector は、クラウドプロバイダに導入された仮想マシンインスタンス、または設定したオンプレミスホストで実行されます。

Service Connector は、複数の NetApp クラウドデータサービスで使用できます。たとえば、 Cloud Manager 用の Service Connector がすでにある場合は、 Cloud Tiering Service のセットアップ時にそのコネクタを選択できます。

例

次の例は、 2 つのワークスペースを使用して、 Cloud Volumes ONTAP システムの分離環境を作成するアカウントを示しています。たとえば、 1 つのワークスペースがステージング環境用で、もう 1 つのワークスペースが本番環境用であるとします。

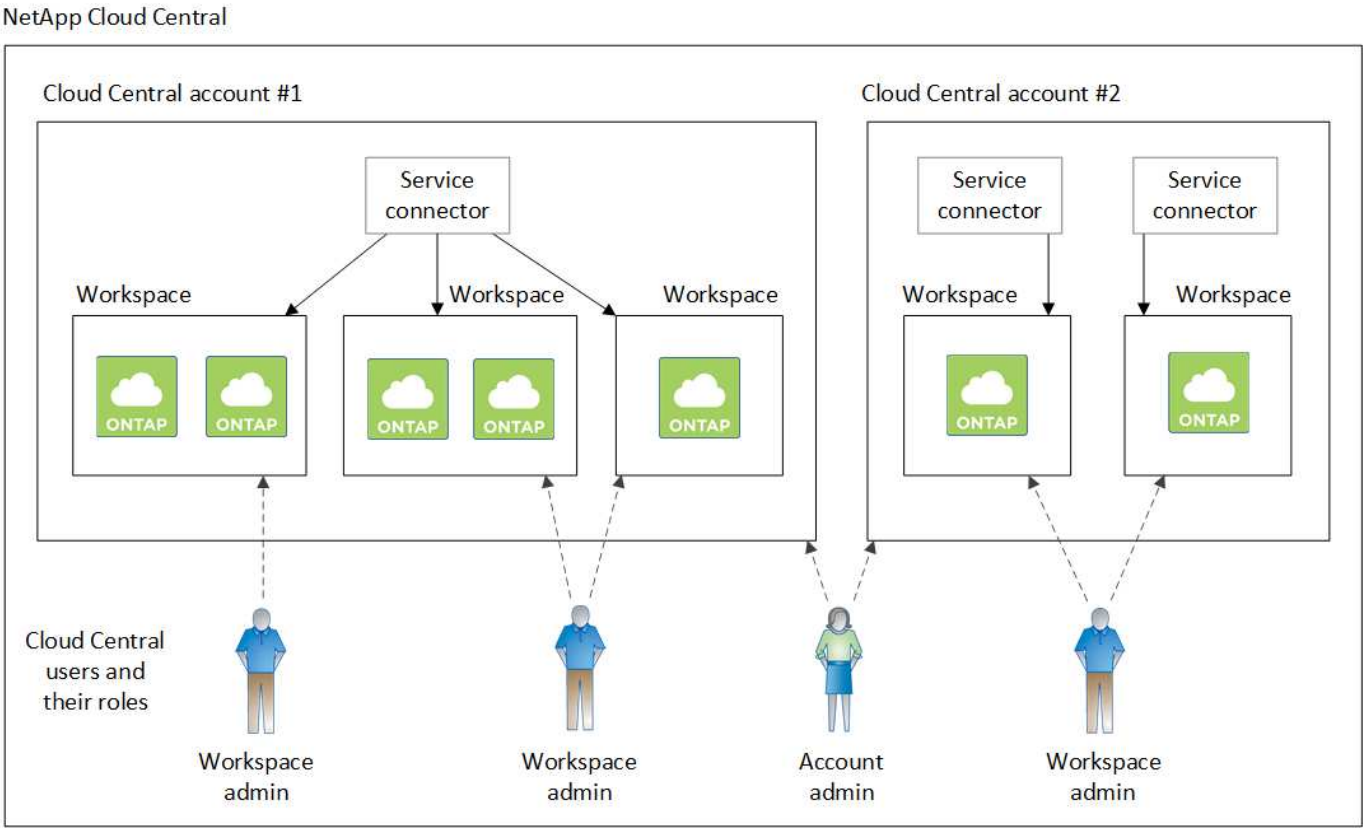
Cloud Manager と Cloud Volumes ONTAP システムは、実際には NetApp Cloud Central アカウントには存在しません。クラウドプロバイダで実行されています。これは、各コンポーネント間の関係の概念図です。



次に、 2 つの異なる Cloud Central アカウントを使用した、最高レベルのマルチテナンシーの例を示します。たとえば、あるサービスプロバイダーがクラウドセントラルアカウントの Cloud Manager を使用して顧客にサービスを提供し、別のアカウントを使用していずれかのビジネスユニットに災害復旧を提供する場合などです。

Account 2 には、 2 つの個別のサービスコネクタが含まれています。これは、システムが別々の地域にある場合や、別々のクラウドプロバイダにある場合に発生することがあります。

繰り返しになりますが、 Cloud Manager と Cloud Volumes ONTAP システムは、実際には NetApp Cloud Central アカウントではなく、クラウドプロバイダで実行されています。これは、各コンポーネント間の関係の概念図です。



Cloud Central アカウントとの統合に関する FAQ

クラウドマネージャ 3.7 にアップグレードした後、クラウドセントラルアカウントと統合するために、特定のクラウドマネージャシステムを選択する予定です。この FAQ では、このプロセスに関する質問にお答えします。

プロセスにはどのくらいの時間がかかりますか？

わずか数分。

Cloud Manager は使用できませんか。

いいえ。 Cloud Manager システムには引き続きアクセスできます。

Cloud Volumes ONTAP について教えてください。

Cloud Volumes ONTAP システムが停止することはありません。

このプロセスでは何が起こりますか？

ネットアップは、統合プロセスで次のことを行います。

1. 新しい Cloud Central アカウントを作成し、 Cloud Manager システムに関連付けます。

2. 既存の各ユーザに新しいロールを割り当てます。
    - Cloud Manager 管理者はアカウント管理者になります
    - テナント管理者と作業環境管理者は、ワークスペース管理者になります
3. 既存のテナントを置き換えるワークスペースを作成します。
4. 作業環境をこれらのワークスペースに配置します。
5. Service Connector をすべてのワークスペースに関連付けます。

Cloud Manager システムのインストール先はどこにいても問題ありませんか。

いいえネットアップは、 AWS 、 Azure 、オンプレミスのいずれの環境にあっても、 Cloud Central アカウントとシステムを統合します。

クラウドプロバイダアカウント

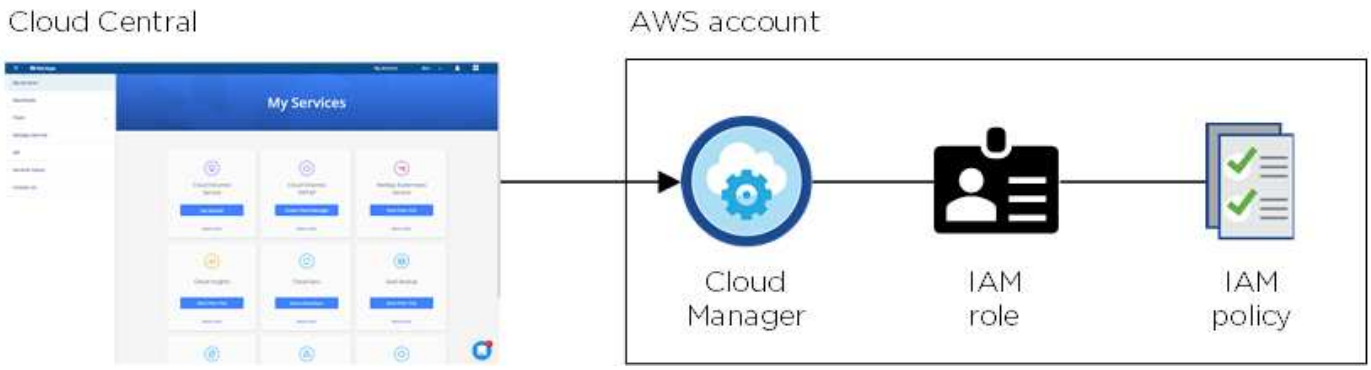
AWS アカウントと権限

Cloud Manager では、 Cloud Volumes ONTAP システムを導入する AWS アカウントを選択できます。すべての Cloud Volumes ONTAP システムを初期の AWS アカウントに導入することも、追加のアカウントを設定することもできます。

初期の AWS アカウント

NetApp Cloud Central から Cloud Manager を導入する場合は、 Cloud Manager インスタンスを起動する権限を持つ AWS アカウントを使用する必要があります。必要な権限は、に表示されます "AWS 向けの NetApp Cloud Central ポリシー"。

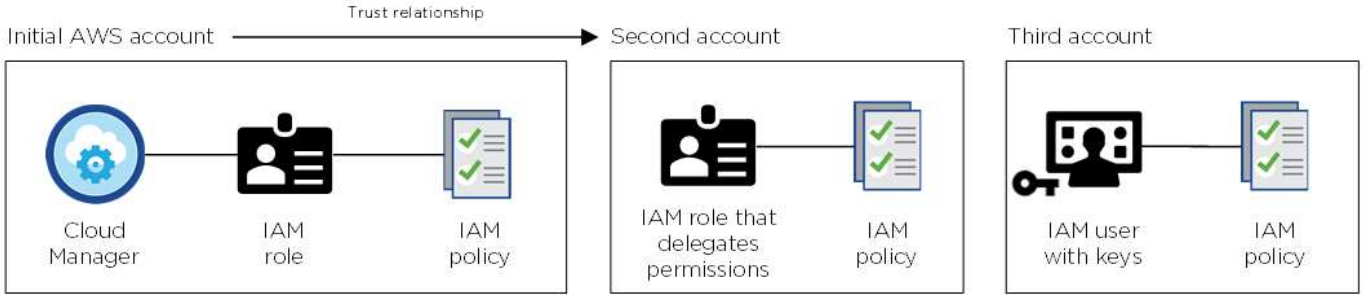
Cloud Central は、 AWS で Cloud Manager インスタンスを起動すると、 IAM ロールとインスタンスのインスタンスプロファイルを作成します。また、 Cloud Manager に、その AWS アカウントで Cloud Volumes ONTAP を導入および管理する権限を与えるポリシーも付加します。 "Cloud Manager での権限の使用方法を確認します。"。



Cloud Manager は、新しい作業環境を作成するときに、デフォルトでこのクラウドプロバイダアカウントを選択します。

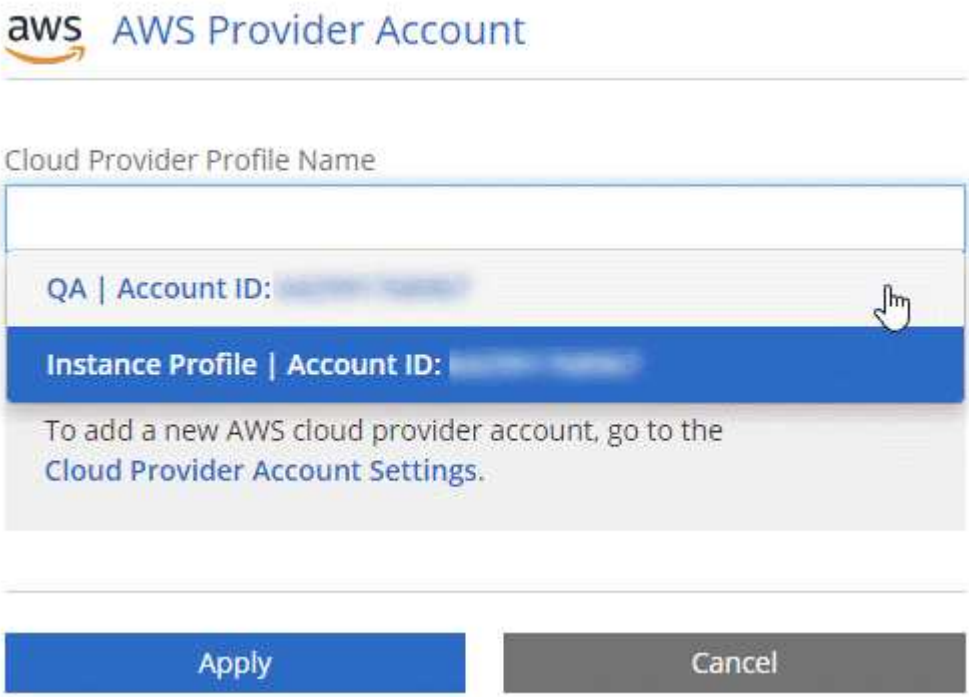
追加の **AWS** アカウント

別々の AWS アカウントで Cloud Volumes ONTAP を起動する場合は、どちらかを実行します "IAM ユーザまたは ARN に AWS キーを指定します 信頼できるアカウントのロール"。次の図は、 2 つの追加アカウントを示しています。 1 つは、信頼されたアカウントの IAM ロールを介してアクセス許可を提供し、もう 1 つは IAM ユーザの AWS キーを使用してアクセス許可を提供します。



そのあとで "Cloud Manager にクラウドプロバイダアカウントを追加します" IAM ロールの Amazon リソース名（ARN ）、または IAM ユーザの AWS キーを指定します。

別のアカウントを追加したら、新しい作業環境を作成するときにそのアカウントに切り替えることができます。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

市場への導入とオンプレミスの導入についてはどうでしょうか。

上記のセクションでは、 NetApp Cloud Central で推奨される導入方法について説明します。から AWS に Cloud Manager を導入することもできます "AWS Marketplace" また、次のことも可能です "Cloud Manager をオンプレミスにインストール"。

Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。IAM ロールを手動で作成して設定し、追加のアカウントに権限を付与するだけで済みます。

オンプレミス環境では、 Cloud Manager システム用の IAM ロールを設定することはできませんが、追加の AWS アカウントの場合と同様に権限を付与することはできます。

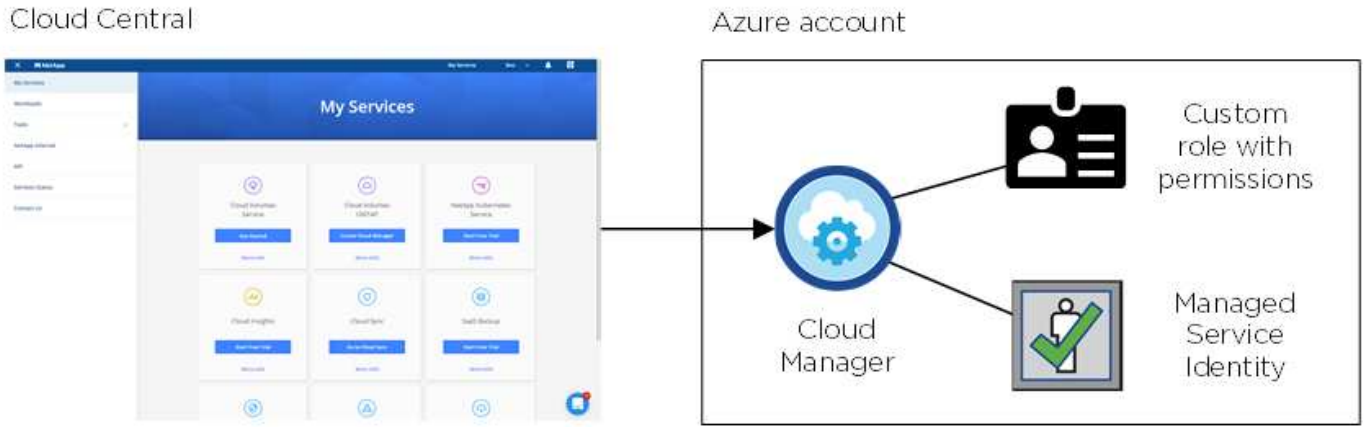
Azure アカウントと権限

Cloud Manager では、 Cloud Volumes ONTAP システムを導入する Azure アカウントを選択できます。すべての Cloud Volumes ONTAP システムを最初の Azure アカウントに導入することも、追加のアカウントを設定することもできます。

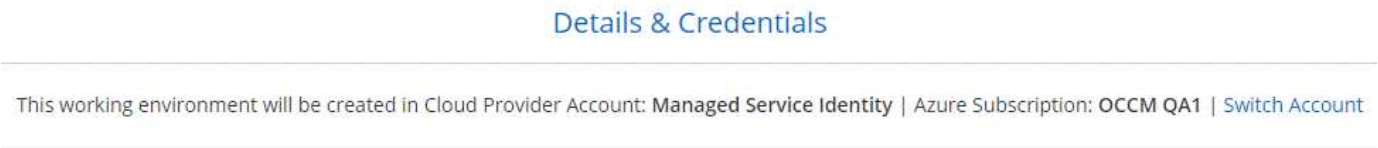
最初の Azure アカウント

NetApp Cloud Central から Cloud Manager を導入する場合は、 Cloud Manager 仮想マシンを導入する権限を持つ Azure アカウントを使用する必要があります。必要な権限は、に表示されます "Azure 向けの NetApp Cloud Central ポリシー"。

Cloud Central が Azure に Cloud Manager 仮想マシンを導入すると、が有効になります "システムによって割り当てられた管理 ID" Cloud Manager 仮想マシンで、カスタムロールを作成して仮想マシンに割り当てます。この役割は、 Cloud Manager に、その Azure サブスクリプションで Cloud Volumes ONTAP を導入および管理する権限を付与します。 "Cloud Manager での権限の使用方法を確認します。"。



Cloud Manager は、新しい作業環境を作成するときに、デフォルトでこのクラウドプロバイダアカウントを選択します。

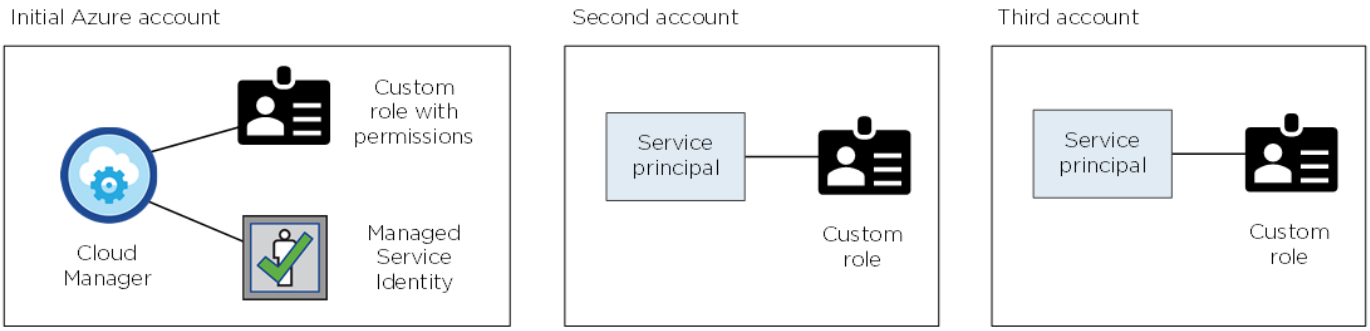


初期アカウント用の追加の **Azure** サブスクリプション

管理対象 ID は、 Cloud Manager を起動したサブスクリプションに関連付けられます。別の Azure サブスクリプションを選択する場合は、が必要です "管理対象 ID をこれらのサブスクリプションに関連付けます"。

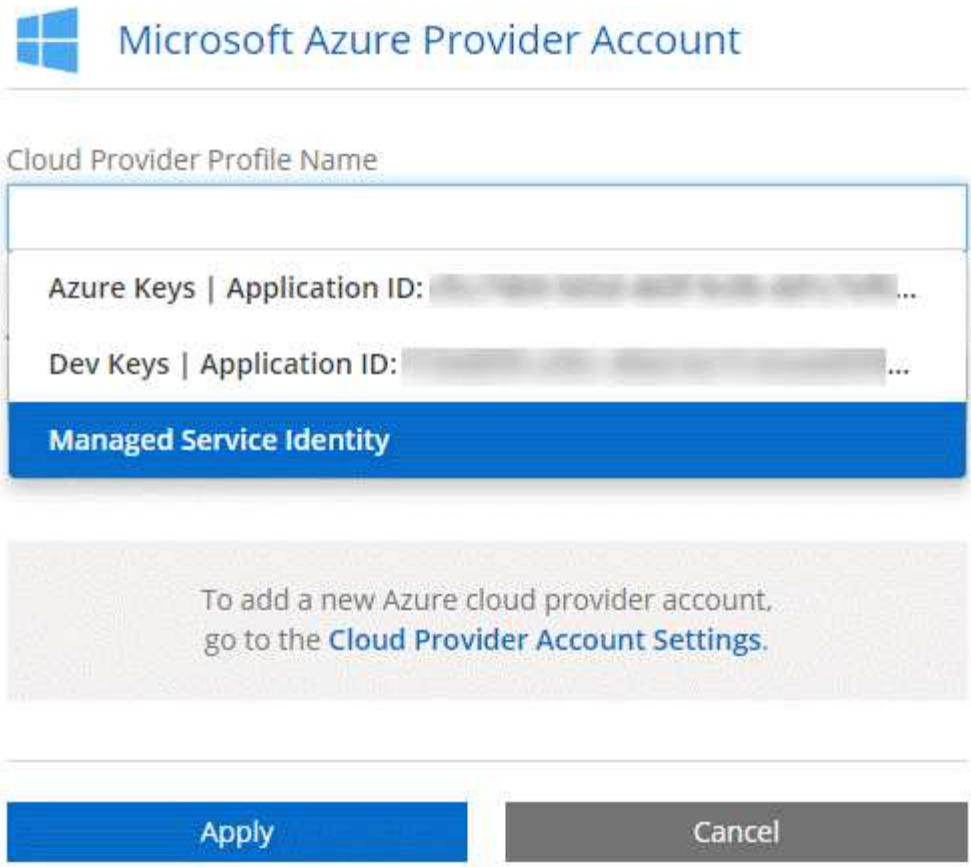
追加の **Azure** アカウント

Cloud Volumes ONTAP を別々の Azure アカウントに導入する場合は、で必要な権限を付与する必要があります "Azure Active でサービスプリンシパルを作成およびセットアップする ディレクトリ" を Azure アカウントごとに用意します。次の図は、 2 つの追加アカウントを示しています。各アカウントには、権限を提供するサービスプリンシパルとカスタムロールが設定されています。



そのあとで "Cloud Manager にクラウドプロバイダアカウントを追加します" AD サービスプリンシパルの詳細を指定します。

別のアカウントを追加したら、新しい作業環境を作成するときにそのアカウントに切り替えることができます。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

> 市場への導入とオンプレミスの導入についてはどうでしょうか。
>
> 上記のセクションでは、 NetApp Cloud Central で推奨される導入方法について説明します。から Azure に Cloud Manager を導入することもできます "Azure Marketplace で入手できます"を使用できます "Cloud Manager をオンプレミスにインストール"。
>
> Marketplace を使用する場合も、アクセス許可は同じ方法で提供されます。Cloud Manager の管理対象 ID を手動で作成して設定し、追加のアカウントに権限を付与するだけで済みます。
>
> オンプレミス環境では、 Cloud Manager システムの管理対象 ID を設定することはできませんが、追加のアカウントの場合と同様に権限を付与することはできます。

Google Cloud のプロジェクト、権限、アカウント

サービスアカウントを使用すると、 Cloud Manager と同じプロジェクトまたは異なるプロジェクトに Cloud Volumes ONTAP システムを導入して管理する権限が Cloud Manager に付与されます。Cloud Manager に追加した Google Cloud アカウントは、データの階層化に使用されます。

Cloud Manager のプロジェクトと権限

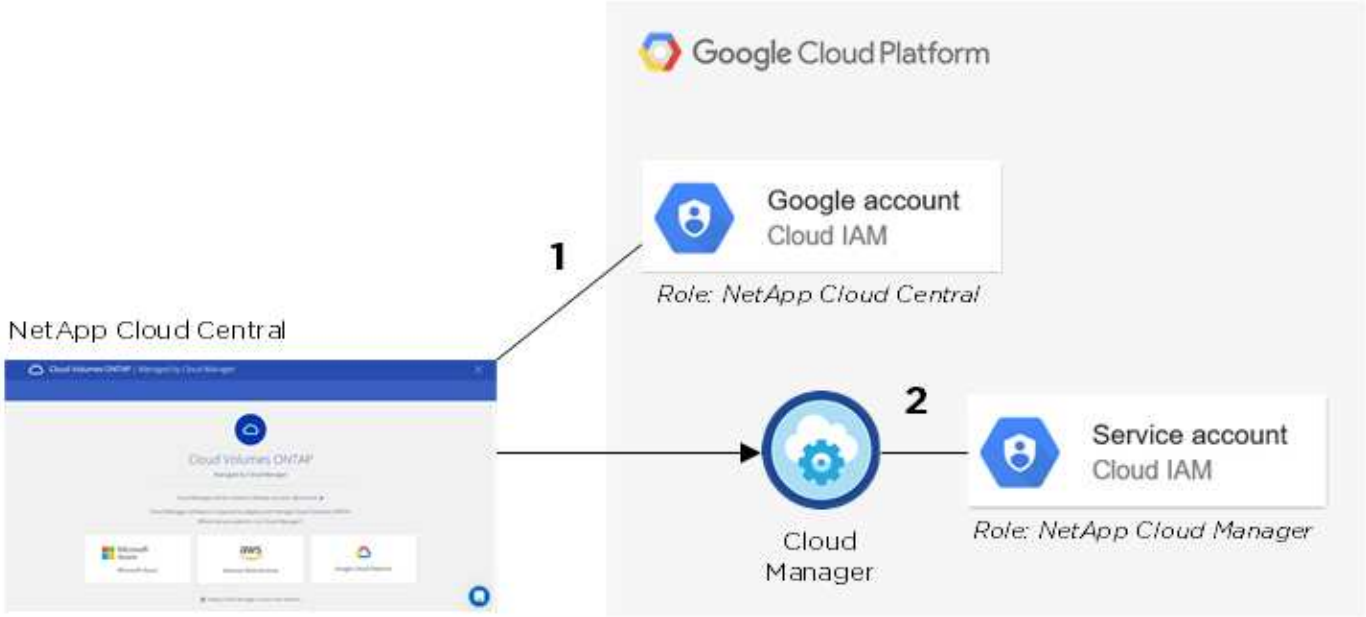
Cloud Volumes ONTAP を Google Cloud に導入する前に、まず Google Cloud プロジェクトに Cloud Manager を導入する必要があります。Cloud Manager をオンプレミスで実行したり、別のクラウドプロバイダで実行したりすることはできません。

Cloud Manager を導入する前に、 2 組の権限が設定されている必要があります "NetApp Cloud Central"：

1. Cloud Central から Cloud Manager VM インスタンスを起動する権限を持つ Google アカウントを使用して、 Cloud Manager を導入する必要があります。
2. Cloud Manager を導入する際に、を選択するように求められます "サービスアカウント" VM インスタンスの場合です。Cloud Manager は、サービスアカウントから権限を取得して、 Cloud Volumes ONTAP システムを代わりに作成および管理します。権限は、サービスアカウントにカスタムロールを割り当てることによって提供されます。

ユーザとサービスアカウントに必要な権限を含む YAML ファイルを 2 つ設定しました。 "YAML ファイルを使用して設定する方法を学習します 権限"。

次の図は、上記の番号 1 と 2 で説明した権限の要件を示しています。



Project for Cloud Volumes ONTAP の略

Cloud Volumes ONTAP は、 Cloud Manager と同じプロジェクトにも別のプロジェクトにも配置できます。Cloud Volumes ONTAP を別のプロジェクトに導入するには、まず Cloud Manager サービスアカウントとロールをそのプロジェクトに追加する必要があります。

- "Cloud Manager サービスアカウントの設定方法を確認する（ステップ 4 を参照）"。
- "GCP とで Cloud Volumes ONTAP を導入する方法について説明します プロジェクトを選択します"。

データの階層化を考慮してください

Cloud Volumes ONTAP システムでデータ階層化を有効にするには、 Cloud Manager に Google Cloud アカウントを追加する必要があります。データ階層化により、コールドデータを低コストのオブジェクトストレージ

に自動的に階層化し、プライマリストレージのスペースを再利用してセカンダリストレージを縮小できます。

アカウントを追加するときは、 Storage Admin の権限を持つサービスアカウントのストレージアクセスキーを Cloud Manager に提供する必要があります。Cloud Manager は、アクセスキーを使用して Cloud Storage バケットをセットアップおよび管理し、データを階層化します。

Google Cloud アカウントを追加したら、作成、変更、または複製するときに、個々のボリュームでデータ階層化を有効にできます。

- "GCP アカウントの設定方法と追加方法について説明します Cloud Manager の略"。
- "アクセス頻度の低いデータを低コストのオブジェクトストレージに階層化する方法について説明します"。

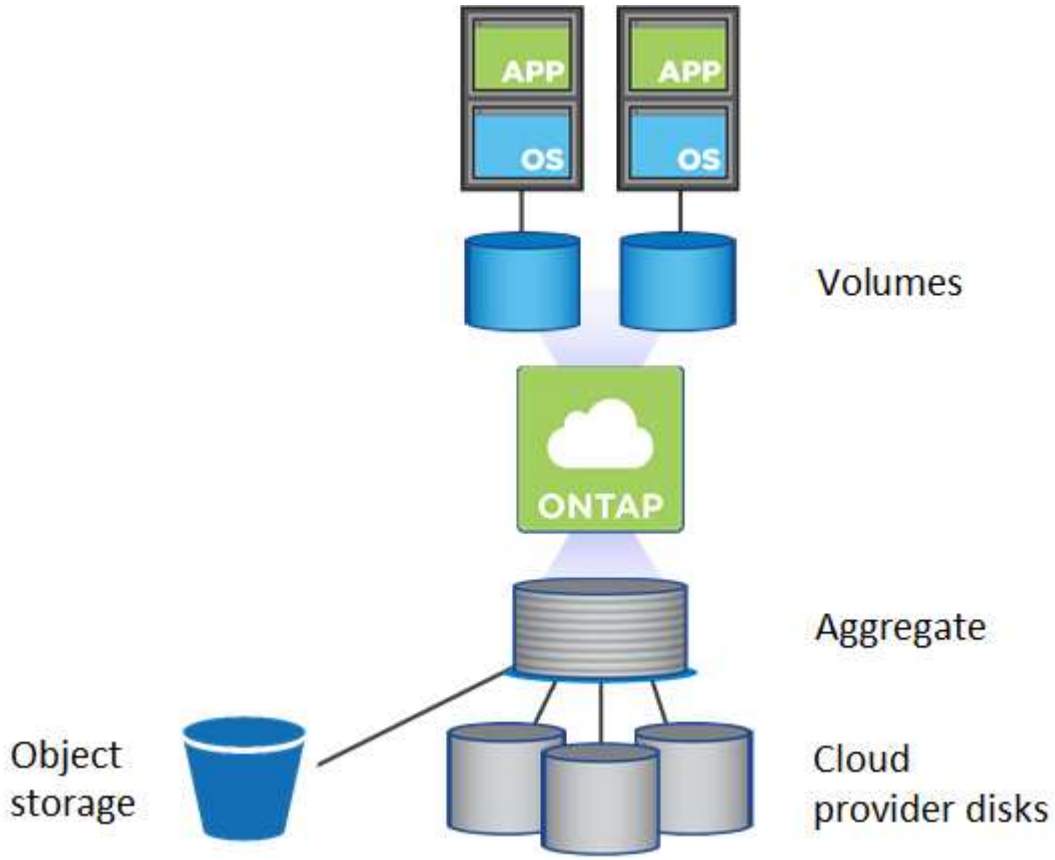
ストレージ

ディスクとアグリゲート

Cloud Volumes ONTAP でのクラウドストレージの使用方法を理解することで、ストレージコストを把握することができます。

概要

Cloud Volumes ONTAP では、クラウドプロバイダのストレージをディスクとして使用し、それらを 1 つ以上のアグリゲートにグループ化します。アグリゲートは、 1 つ以上のボリュームにストレージを提供します。



クラウドディスクにはいくつかのタイプがサポートされています。ディスクタイプはボリュームの作成時に選

択し、デフォルトのディスクサイズは Cloud Volumes ONTAP の導入時に選択します。

> クラウドプロバイダから購入したストレージの総容量は、 _raw 容量です。約 12~14% は Cloud Volumes ONTAP 用に予約されたオーバーヘッドであるため、使用可能な容量はこれより少なくなります。たとえば、 Cloud Manager が 500 GB のアグリゲートを作成した場合、使用可能な容量は 442.94 GB になります。

AWS ストレージ

AWS で Cloud Volumes ONTAP は、一部の EC2 インスタンスタイプで、ユーザデータ用の EBS ストレージとローカルの NVMe ストレージが Flash Cache として使用されます。

EBS ストレージ

AWS では、アグリゲートに同じサイズのディスクを最大 6 本含めることができます。最大ディスクサイズは 16TB です。

基盤となる EBS ディスクタイプは、汎用 SSD 、プロビジョニングされた IOPS SSD 、スループットに最適化された HDD 、コールド HDD のいずれかです。EBS ディスクと Amazon S3 をにペアリングできます "使用頻度の低いデータを低コストのオブジェクトストレージに階層化します"。

EBS ディスクタイプの違いは次のとおりです。

- _ 汎用 SSD_disks は、幅広いワークロードに対してコストとパフォーマンスのバランスを取ります。パフォーマンスは IOPS の観点から定義されます。
- _Provisioned IOPS ssd は、コストが高くても最高のパフォーマンスが必要な重要なアプリケーション用です。
- _Throughput Optimized HDD_disks は、高速で安定したスループットを低価格で実現する必要のある、アクセス頻度の高いワークロード用です。
- _Cold HDD_disks は、パフォーマンスが非常に低いため、バックアップまたはアクセス頻度の低いデータ用です。スループットに最適化された HDD ディスクと同様に、パフォーマンスはスループットの観点から定義されます。

> コールド HDD ディスクは、 HA 構成とデータ階層化ではサポートされていません。

ローカル **NVMe** ストレージ

一部の EC2 インスタンスタイプには、 Cloud Volumes ONTAP がとして使用するローカル NVMe ストレージが含まれています "Flash Cache"。

- 関連リンク *
- "AWS のドキュメント： EBS ボリュームのタイプ"
- "でディスクタイプとディスクサイズを選択する方法について説明します AWS のシステムを管理できます"
- "AWS での Cloud Volumes ONTAP のストレージの制限を確認します"
- "AWS で Cloud Volumes ONTAP がサポートされている構成を確認します"

Azure ストレージ

Azure では、アグリゲートに同じサイズのディスクを 12 本まで含めることができます。ディスクタイプと最大ディスクサイズは、シングルノードシステムと HA ペアのどちらを使用するかによって異なります。

シングルノードシステム

シングルノードシステムでは、次の 3 種類の Azure Managed Disks を使用できます。

- _Premium SSD Managed Disks （プレミアム SSD 管理ディスク） - I/O 負荷の高いワークロードに高パフォーマンスを提供し、コストを高めます。
- _ 標準 SSD 管理ディスク _ 低 IOPS を必要とするワークロードに一貫したパフォーマンスを提供します。
- _Standard HDD Managed Disks_are a good choice if you need high iops and want to Reduce your costs （高 IOPS が必要なく、コストを削減したい場合に最適です。）

  管理対象の各ディスクタイプの最大ディスクサイズは 32TB です。

  管理対象ディスクと Azure BLOB ストレージをペアリングすることができます からに "使用頻度の低いデータを低コストのオブジェクトストレージに階層化します"。

HA ペア

HA ペアでは、最大ディスクサイズが 8TB の Premium ページ Blob を使用します。

- 関連リンク *
- "Microsoft Azure のドキュメント：「 Introduction to Microsoft Azure Storage"
- "でディスクタイプとディスクサイズを選択する方法について説明します Azure の既存のシステムを"
- "Azure での Cloud Volumes ONTAP のストレージの制限を確認します"

GCP ストレージ

GCP では、アグリゲートに同じサイズのディスクを 6 本まで含めることができます。最大ディスクサイズは 16TB です。

ディスクタイプには、 _Zonal SSD persistent disks _ または _Zonal standard persistent disks _ を指定できます。永続ディスクを Google Storage バケットとペアリングできます からに "使用頻度の低いデータを低コストのオブジェクトストレージに階層化します"。

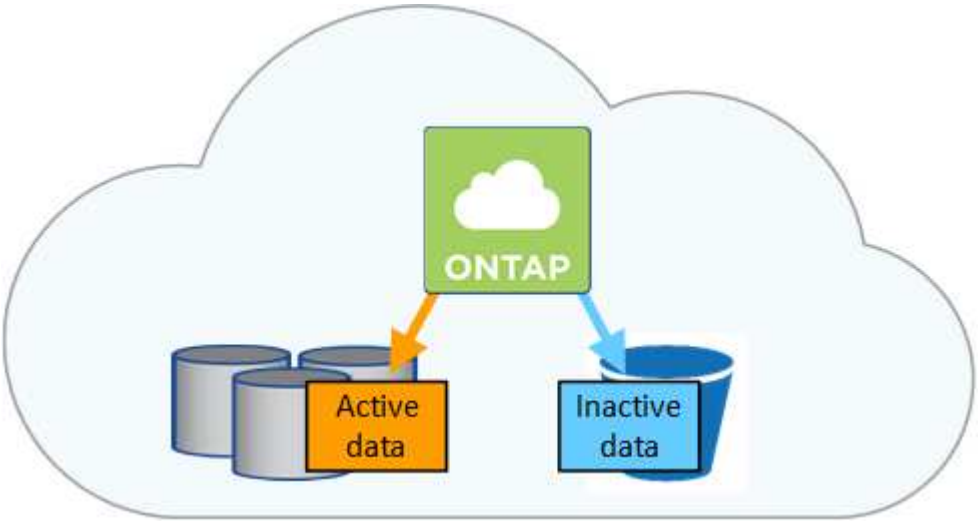
- 関連リンク *
- "Google Cloud Platform のドキュメント：「ストレージオプション"
- "GCP で Cloud Volumes ONTAP のストレージの制限を確認する"

RAID タイプ

各 Cloud Volumes ONTAP アグリゲートの RAID タイプは RAID 0 （ストライピング）です。その他の RAID タイプはサポートされません。Cloud Volumes ONTAP は、ディスクの可用性とデータ保持性についてクラウドプロバイダに依存しています。

データ階層化の概要

使用頻度の低いデータを低コストのオブジェクトストレージに自動的に階層化できるため、ストレージコストを削減できます。アクティブなデータはハイパフォーマンスの SSD または HDD に残り、非アクティブなデータは低コストのオブジェクトストレージに階層化されます。これにより、プライマリストレージのスペースを再利用し、セカンダリストレージを縮小できます。



Cloud Volumes ONTAP は、 AWS 、 Azure 、 Google Cloud Platform のデータ階層化をサポートしています。データ階層化は、 FabricPool テクノロジによって実現されます。

> データの階層化（ FabricPool ）を有効にするために機能ライセンスをインストールする必要はありません。

AWS でのデータ階層化

AWS でデータ階層化を有効にすると、 Cloud Volumes ONTAP はホットデータのパフォーマンス階層として EBS 、アクセス頻度の低いデータの大容量階層として AWS S3 を使用します。システムの階層化レベルを変更すると、別の S3 ストレージクラスを選択できます。

高パフォーマンス階層

パフォーマンス階層には、汎用 SSD 、プロビジョニングされた IOPS SSD 、スループットに最適化された HDD があります。

大容量階層

Cloud Volumes ONTAP システムは、 _Standard_storage クラスを使用して、アクセス頻度の低いデータを 1 つの S3 バケットに階層化します。Standard は、複数の可用性ゾーンにまたがって保存された頻繁にアクセスされるデータに最適です。

> Cloud Manager は、作業環境ごとに 1 つの S3 バケットを作成して、 fabric-pool-*cluster unique identifier* という名前を付けます。ボリュームごとに異なる S3 バケットが作成されることはありません。

階層化レベル

アクセス頻度の低いデータがない場合は、システムの階層化レベルを「インテリジェントな階層化」、「1 ゾーンの頻度の低いアクセス」、または「標準 - 低頻度アクセス」に変更することで、ストレージコストを削減できます。階層化レベルを変更すると、アクセス頻度の低いデータは Standard ストレージクラスから始まり、 30 日経ってもアクセスされない場合は選択したストレージクラスに移動します。

データにアクセスするとアクセスコストが高くなるため、階層化レベルを変更する前にこの点を考慮する必要があります。 "Amazon S3 ストレージクラスに関する詳細情報"。

階層化レベルの変更はシステムの作成後に実行できます。詳細については、を参照してください "使用頻度の低いデータを低コストのオブジェクトストレージに階層化"。

階層化レベルはシステム全体に適用され、ボリューム単位には適用されません。

Azure のデータ階層化

Azure でデータ階層化を有効にすると、 Cloud Volumes ONTAP は、ホットデータ用のパフォーマンス階層として Azure で管理されているディスクを、アクセス頻度の低いデータ用の大容量階層として Azure Blob Storage を使用します。システムの階層化レベルを変更すると、別の Azure ストレージ階層を選択できます。

高パフォーマンス階層

高パフォーマンス階層には SSD と HDD があります。

大容量階層

Cloud Volumes ONTAP システムは、 azure_hot_storage 階層を使用して、アクセス頻度の低いデータを単一の BLOB コンテナに階層化します。ホット階層は、アクセス頻度の高いデータに最適です。

> Cloud Manager は、 Cloud Volumes ONTAP 作業環境ごとに 1 つのコンテナを持つ新しいストレージアカウントを作成します。ストレージアカウントの名前はランダムです。ボリュームごとに異なるコンテナは作成されません。

階層化レベル

アクセス頻度の低いデータにアクセスしない場合は、システムの階層化レベルを azure_cool のストレージ階層に変更することで、ストレージコストを削減できます。階層化レベルを変更すると、アクセス頻度の低いデータは最初はホットストレージ階層に配置され、アクセス日数が 30 日を超えない場合はアクセス頻度の低いストレージ階層に移動されます。

データにアクセスするとアクセスコストが高くなるため、階層化レベルを変更する前にこの点を考慮する必要があります。 "Azure BLOB ストレージのアクセス階層の詳細については、こちらを参照してください"。

階層化レベルの変更はシステムの作成後に実行できます。詳細については、を参照してください "使用頻度の低いデータを低コストのオブジェクトストレージに階層化"。

階層化レベルはシステム全体に適用され、ボリューム単位には適用されません。

GCP でのデータ階層化

GCP でデータ階層化を有効にすると、 Cloud Volumes ONTAP はホットデータのパフォーマンス階層として永続的ディスクを使用し、アクセス頻度の低いデータの大容量階層として Google Cloud Storage バケットを使用します。

高パフォーマンス階層

高パフォーマンス階層には、 SSD または HDD （標準ディスク）を使用できます。

大容量階層

Cloud Volumes ONTAP システムは、 _Regional _storage クラスを使用して、アクセス頻度の低いデータを 1 つの Google Cloud Storage バケットに階層化します。

> Cloud Manager は、作業環境ごとに 1 つのバケットを作成し、 fabric-pool-*cluster unique identifier* という名前を付けます。ボリュームごとに異なるバケットが作成されることはありません。

階層化レベル

現時点では、他の GCP ストレージクラスはサポートされていません。

データ階層化と容量の制限

データの階層化を有効にしても、システムの容量制限は変わりません。この制限は、パフォーマンス階層と容量階層に分散されます。

ボリューム階層化ポリシー

データ階層化を有効にするには、ボリュームの作成、変更、またはレプリケート時にボリューム階層化ポリシーを選択する必要があります。ボリュームごとに異なるポリシーを選択できます。

一部の階層化ポリシーには、最小冷却期間が関連付けられています。この期間は、データを「コールド」と見なして容量階層に移動するために、ボリューム内のユーザーデータを非アクティブのままにする必要がある時間を設定します。

Cloud Manager では、ボリュームを作成または変更するときに、次のボリューム階層化ポリシーのいずれかを選択できます。

Snapshot のみ

アグリゲートの容量が 50% に達すると、 Cloud Volumes ONTAP は、アクティブなファイルシステムに関連付けられていない Snapshot コピーのコールドユーザデータを容量階層に階層化します。冷却期間は約 2 日間です。

読み取りの場合、容量階層のコールドデータブロックはホットになり、パフォーマンス階層に移動されます。

自動

アグリゲートの容量が 50% に達すると、 Cloud Volumes ONTAP はボリューム内のコールドデータブロックを容量階層に階層化します。コールドデータには、 Snapshot コピーだけでなく、アクティブなファイルシステムのコールドユーザデータも含まれます。冷却期間は約 31 日です。

このポリシーは、 Cloud Volumes ONTAP 9.4 以降でサポートされます。

ランダム読み取りで読み取りを行うと、容量階層のコールドデータブロックがホットになり、パフォーマンス階層に移動します。インデックススキャンやアンチウイルススキャンに関連するようなシーケンシャルリードで読み取られた場合、コールドデータブロックはコールド状態を維持し、パフォーマンス階層には移動しません。

なし

ボリュームのデータをパフォーマンス階層に保持し、容量階層に移動できないようにします。

ボリュームをレプリケートする場合、データをオブジェクトストレージに階層化するかどうかを選択できます。このように設定すると、 Cloud Manager は * Backup * ポリシーをデータ保護ボリュームに適用します。Cloud Volumes ONTAP 9.6 以降では、「 * all * 」階層化ポリシーがバックアップポリシーに置き換えられます。

Cloud Volumes ONTAP をオフにすると、冷却期間に影響します

データブロックはクーリングスキャンによって冷却されます。このプロセスでは、使用されていないブロックのブロック温度が次の低い値に移動（冷却）されます。デフォルトのクーリング時間は、ボリューム階層化ポリシーによって異なります。

- 自動： 31 日
- Snapshot のみ： 2 日

冷却スキャンが機能するためには、 Cloud Volumes ONTAP が実行されている必要があります。Cloud Volumes ONTAP をオフにすると、冷却も停止します。その結果、冷却にかかる時間が長くなる可能性があります。

データ階層化の設定

手順およびサポートされている構成の一覧については、を参照してください "使用頻度の低いデータを低コストのオブジェクトストレージに階層化"。

ストレージ管理

Cloud Manager は、 Cloud Volumes ONTAP ストレージの簡易化された高度な管理機能を提供します。

> すべてのディスクとアグリゲートは、 Cloud Manager から直接作成および削除する必要があります。これらのアクションは、別の管理ツールから実行しないでください。これにより、システムの安定性が低下し、将来ディスクを追加できなくなる可能性があります。また、クラウドプロバイダの冗長料金が発生する可能性もあります。

ストレージのプロビジョニング

Cloud Manager では、ディスクを購入してアグリゲートを管理することで、 Cloud Volumes ONTAP のストレージプロビジョニングが容易になります。ボリュームを作成するだけで済みます。必要に応じて、 Advanced Allocation オプションを使用してアグリゲートをプロビジョニングできます。

プロビジョニングの簡素化

アグリゲートは、ボリュームにクラウドストレージを提供します。Cloud Manager では、インスタンスを起動したとき、および追加ボリュームをプロビジョニングしたときに、アグリゲートが作成されます。

ボリュームを作成すると、 Cloud Manager は次の 3 つのいずれかを実行します。

- 十分な空きスペースがある既存のアグリゲートにボリュームを配置します。

- ボリュームを既存のアグリゲートに配置するには、そのアグリゲート用に追加のディスクを購入します。
- 新しいアグリゲートのディスクを購入し、そのアグリゲートにボリュームを配置します。

Cloud Manager は、アグリゲートの最大サイズ、シンプロビジョニングが有効になっているかどうか、アグリゲートの空きスペースのしきい値など、いくつかの要因を確認して新しいボリュームをどこに配置するかを決定します。

アカウント管理者は、 [設定 *] ページから空き容量のしきい値を変更できます。

AWS でのアグリゲートのディスクサイズの選択

Cloud Manager は、 AWS で Cloud Volumes ONTAP 用の新しいアグリゲートを作成すると、システム内のアグリゲートの数が増えるにつれて、アグリゲート内のディスクサイズを徐々に増加させます。Cloud Manager は、 AWS で許可される最大データディスク数に達する前に、システムの最大容量を利用できるようにします。

たとえば、 Cloud Manager では、 Cloud Volumes ONTAP Premium または BYOL システムのアグリゲートに次のディスクサイズを選択できます。

アグリゲート番号	ディスクサイズ	最大アグリゲート容量
1.	500 MB	3 TB
4.	1 TB	6TB
6.	2TB	12TB

ディスクサイズは、 Advanced Allocation オプションを使用して選択できます。

高度な割り当て

Cloud Manager でアグリゲートを管理するのではなく、自分で管理できます。 "Advanced allocation * ページからアクセスします"では、特定の数のディスクを含む新しいアグリゲートの作成、既存のアグリゲートへのディスクの追加、および特定のアグリゲートでのボリュームの作成を行うことができます。

容量管理

アカウント管理者は、ストレージ容量の決定について Cloud Manager から通知するかどうか、または Cloud Manager が容量の要件を自動的に管理するかどうかを選択できます。これらのモードの仕組みを理解するのに役立つ場合があります。

自動容量管理

容量管理モードは、デフォルトで自動に設定されています。このモードでは、 Cloud Volumes ONTAP インスタンスで追加の容量が必要になると、 Cloud Manager によって新しいディスクが自動的に購入されます。また、未使用のディスクセット（アグリゲート）の削除、必要に応じてアグリゲート間でのボリュームの移動、ディスクの障害状態の解除を試行します。

次の例は、このモードの動作を示しています。

- EBS ディスクが 5 台以下のアグリゲートが容量のしきい値に達すると、 Cloud Manager はそのアグリゲートの新しいディスクを自動的に購入し、ボリュームを継続して拡張できるようにします。

- 12 個の Azure ディスクを持つアグリゲートが容量のしきい値に達すると、 Cloud Manager は、ボリュームをそのアグリゲートから使用可能な容量を持つアグリゲートまたは新しいアグリゲートに自動的に移動します。

  ボリュームに新しいアグリゲートを作成すると、 Cloud Manager はそのボリュームのサイズに対応するディスクサイズを選択します。

  元のアグリゲートに空きスペースがあることに注意してください。既存のボリュームまたは新しいボリュームでは、そのスペースを使用できます。このシナリオでは、スペースを AWS または Azure に戻すことはできません。

- アグリゲートに 12 時間を超えるボリュームが含まれていない場合は、 Cloud Manager によって削除されます。

容量の自動管理による **inode** の管理

Cloud Manager は、ボリューム上の inode の使用量を監視します。inode の 85% を使用すると、 Cloud Manager はボリュームのサイズを増やして、使用可能な inode の数を増やします。ボリュームに含めることができるファイル数は、ボリューム内の inode の数によって決まります。

手動による容量管理

アカウント管理者が容量管理モードを手動に設定した場合、容量の決定が必要な状況になると、 Cloud Manager に「 Action Required 」メッセージが表示され、自動モードで説明されている例と同じ例が手動モードにも適用されますが、アクションを受け入れる必要があります。

WORM ストレージ

Cloud Volumes ONTAP システム上で Write Once Read Many （ WORM ）ストレージをアクティブにして、指定した保存期間内にファイルを変更せずに保持できます。WORM ストレージには、エンタープライズモードの SnapLock テクノロジが採用されています。つまり、 WORM ファイルはファイルレベルで保護されます。

WORM ストレージにコミットされたファイルは、保存期間が終了した後でも変更できません。改ざん防止クロックは、 WORM ファイルの保持期間が経過したタイミングを決定します。

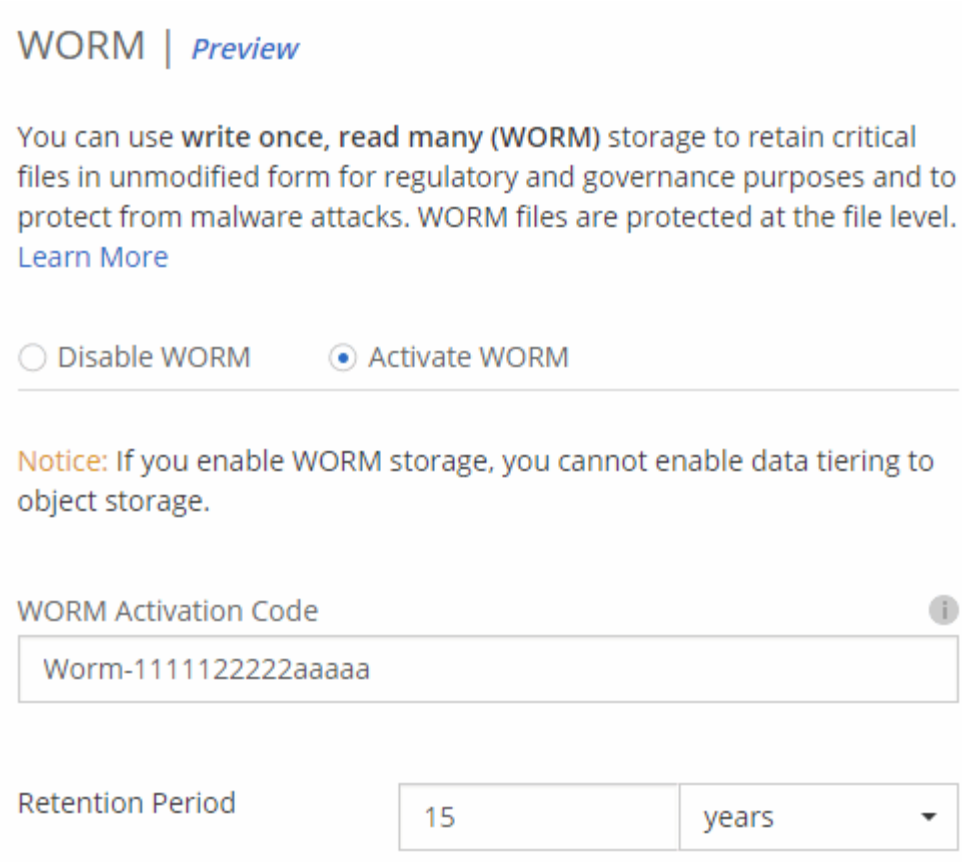
保存期間が経過すると、不要になったファイルを削除する必要があります。

WORM ストレージのアクティブ化

新しい作業環境を作成するときに、 Cloud Volumes ONTAP システムで WORM ストレージをアクティブにできます。これには、アクティベーションコードの指定とファイルのデフォルトの保存期間の設定が含まれます。アクティベーションコードを取得するには、 Cloud Manager インターフェイスの右下にあるチャットアイコンを使用します。

> 個々のボリュームで WORM ストレージをアクティブ化することはできません — WORM はシステムレベルでアクティブ化する必要があります

次の図は、作業環境の作成時に WORM ストレージをアクティブにする方法を示しています。



ファイルを **WORM** にコミットしています

アプリケーションを使用して、 NFS または CIFS を介してファイルを WORM にコミットしたり、 ONTAP CLI を使用してファイルを WORM に自動コミットしたりできます。また、追記可能 WORM ファイルを使用して、ログ情報のように増分的に書き込まれるデータを保持することもできます。

Cloud Volumes ONTAP システムで WORM ストレージをアクティブにした後は、 WORM ストレージのすべての管理に ONTAP CLI を使用する必要があります。手順については、を参照してください "ONTAP のドキュメント"。

> WORM ストレージに対する Cloud Volumes ONTAP のサポートは、 SnapLock Enterprise モードと同等です。

制限

- AWS または Azure からディスクを直接削除または移動すると、ボリュームは有効期限前に削除されます。
- WORM ストレージをアクティブにすると、オブジェクトストレージへのデータ階層化を有効にできません。

ハイアベイラビリティペア

AWS におけるハイアベイラビリティペア

Cloud Volumes ONTAP High Availability （ HA ）構成は、無停止の運用と耐障害性を提

供します。AWS では、 2 つのノード間でデータが同期ミラーリングされます。

概要

AWS では、 Cloud Volumes ONTAP HA 構成に次のコンポーネントが含まれます。

- データが同期的にミラーリングされる 2 つの Cloud Volumes ONTAP ノード。
- ストレージのテイクオーバーとギブバックプロセスを支援するためにノード間の通信チャネルを提供するメディエータインスタンス。

> メディエータインスタンスは、 t2.Micro インスタンス上で Linux オペレーティングシステムを実行し、約 8 GB の EBS 磁気ディスクを 1 つ使用します。

ストレージのテイクオーバーとギブバック

ノードがダウンした場合、もう一方のノードはパートナーにデータを提供して、継続的なデータサービスを提供できます。データはパートナーに同期的にミラーリングされているため、クライアントはパートナーノードから同じデータにアクセスできます。

ノードのリブート後、パートナーはデータを再同期してからストレージを返却する必要があります。データの再同期にかかる時間は、ノードがダウンしている間に変更されたデータの量によって異なります。

RPO と **RTO**

HA 構成では、次のようにデータの高可用性が維持されます。

- RPO （ Recovery Point Objective ：目標復旧時点）は 0 秒です。データはトランザクション的に整合性が保たれ、データ損失は発生しません。
- RTO （目標復旧時間）は 60 秒です。システム停止が発生した場合は、 60 秒以内にデータを利用できるようにする必要があります。

HA の導入モデル

複数の可用性ゾーン（ AZS ）または単一の AZ に HA 構成を導入することで、データの高可用性を確保できます。各構成の詳細を確認して、ニーズに最適な構成を選択してください。

複数の可用性ゾーンでの **Cloud Volumes ONTAP HA**

複数の可用性ゾーン（ AZS ）に HA 構成を導入すると、 AZ または Cloud Volumes ONTAP ノードを実行するインスタンスで障害が発生した場合でも、データの高可用性が確保されます。NAS IP アドレスがデータアクセスとストレージフェイルオーバーに与える影響を理解しておく必要があります。

NFS と **CIFS** のデータアクセス

HA 構成が複数のアベイラビリティゾーンに分散されている場合は、 _floating IP addresss_enable NAS client access 。障害が発生した場合に、ドメイン内のすべての VPC の CIDR ブロックの外側にあるフローティング IP アドレスをノード間で移行できます。VPC の外部にあるクライアントには、自分以外からネイティブにアクセスすることはできません "AWS 転送ゲートウェイを設定します"。

転送ゲートウェイを設定できない場合は、 VPC の外部にある NAS クライアントにプライベート IP アドレスを使用できます。ただし、これらの IP アドレスは静的であり、ノード間でフェイルオーバーすることはでき

ません。

HA 設定を複数の可用性ゾーンに展開する前に、フローティング IP アドレスとルートテーブルの要件を確認する必要があります。設定を展開するときは、フローティング IP アドレスを指定する必要があります。プライベート IP アドレスは Cloud Manager によって自動的に作成されます。

詳細については、を参照してください "複数の AZS での Cloud Volumes ONTAP HA の AWS ネットワーク要件"。

iSCSI データアクセス

iSCSI では浮動 IP アドレスが使用されないため、クロス VPC データ通信は問題になりません。

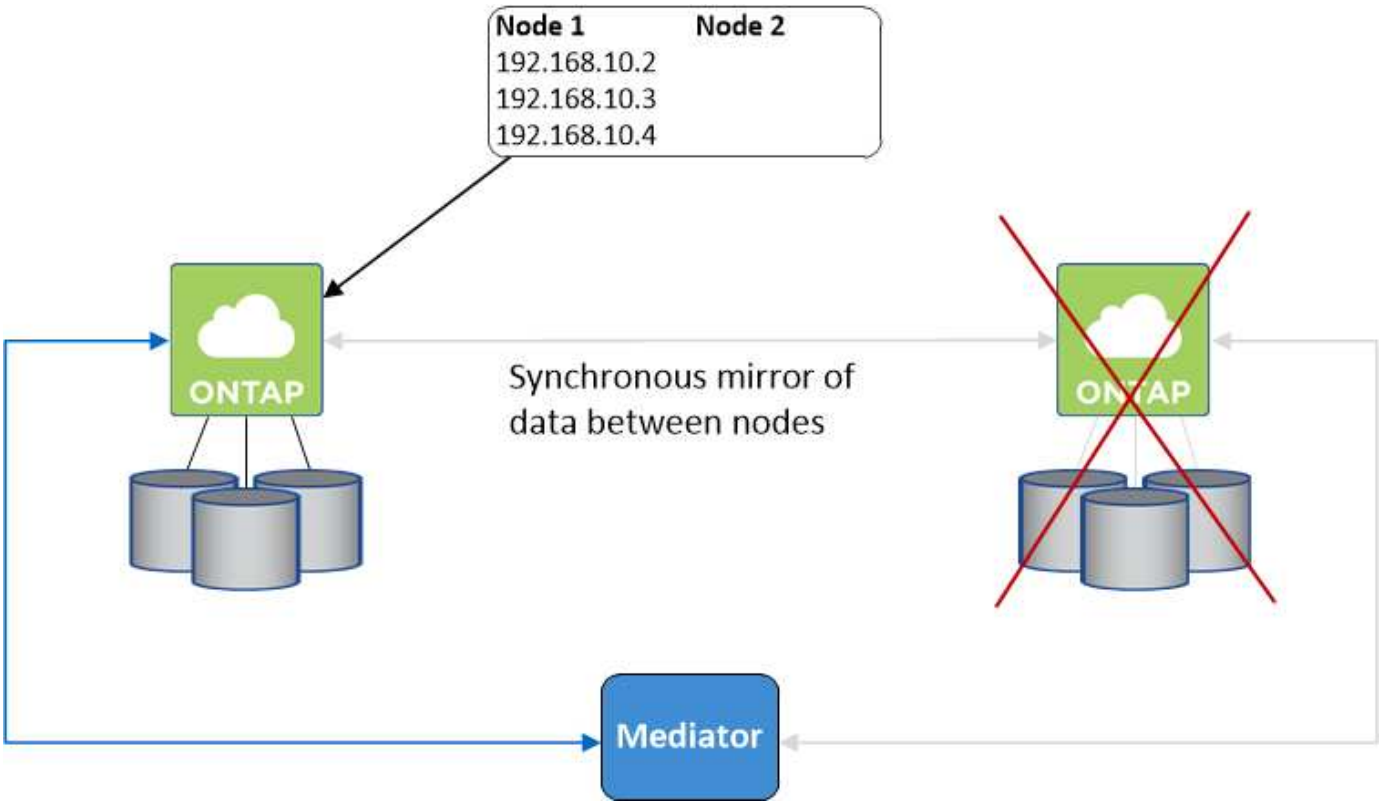
iSCSI のストレージテイクオーバーとギブバック

iSCSI の場合、 ONTAP はマルチパス I/O （ MPIO ）と非対称論理ユニットアクセス（ ALUA ）を使用して、アクティブ最適化パスと非最適化パス間のパスフェイルオーバーを管理します。

> ALUA をサポートする具体的なホスト構成については、を参照してください "NetApp Interoperability Matrix Tool で確認できます" およびお使いのホストオペレーティングシステムに対応した Host Utilities の『 Installation and Setup Guide 』を参照してください。

NAS のストレージテイクオーバーとギブバック

フローティング IP を使用する NAS 構成でテイクオーバーが発生すると、クライアントがデータへのアクセスに使用するノードのフローティング IP アドレスが他のノードに移動します。次の図は、フローティング IP を使用した NAS 構成でのストレージテイクオーバーを示しています。node2 がダウンすると、 node2 のフローティング IP アドレスが node1 に移動します。



障害が発生した場合、外部 VPC アクセスに使用される NAS データ IP はノード間で移行できません。ノードがオフラインになった場合は、もう一方のノードの IP アドレスを使用して、 VPC 外のクライアントにボリュームを手動で再マウントする必要があります。

障害の発生したノードがオンラインに戻ったら、元の IP アドレスを使用してクライアントをボリュームに再マウントします。この手順は、 2 つの HA ノード間で不要なデータが転送されないようにするために必要です。これは、パフォーマンスと安定性に大きな影響を与える可能性があります。

Cloud Manager から正しい IP アドレスを簡単に特定するには、ボリュームを選択して * Mount command * をクリックします。

単一の可用性ゾーンでの **Cloud Volumes ONTAP HA**

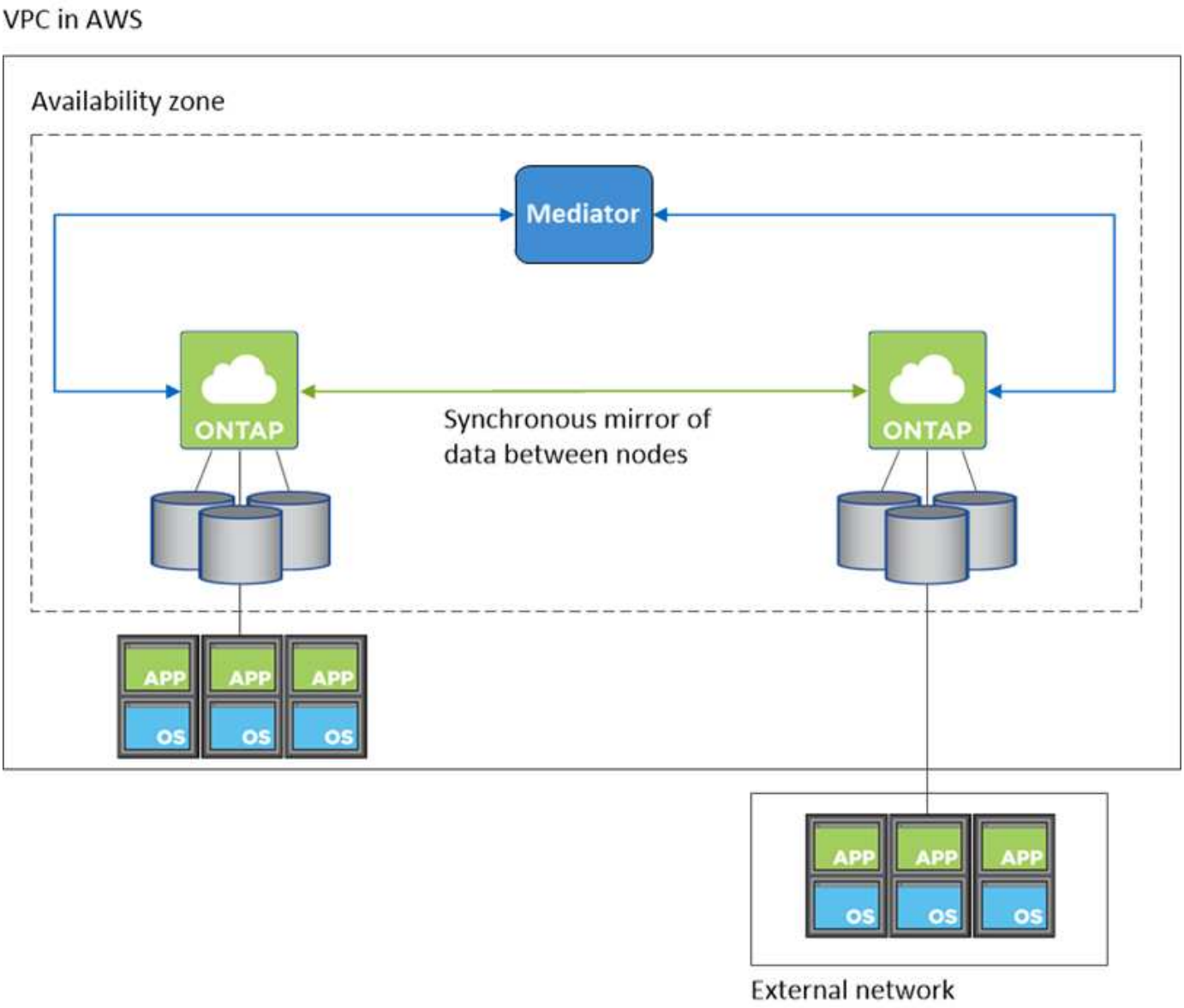
単一の可用性ゾーン（ AZ ）に HA 構成を導入すると、 Cloud Volumes ONTAP ノードを実行するインスタンスで障害が発生した場合でも、データの高可用性を確保できます。すべてのデータは、 vPC の外部からネイティブにアクセスできます。

> Cloud Manager によってが作成されます "AWS 分散配置グループ" をクリックすると、その配置グループ内の 2 つの HA ノードが起動します。配置グループは、インスタンスを別々の基盤ハードウェアに分散することで、同時障害のリスクを軽減します。この機能により、ディスク障害ではなく、コンピューティングの観点から冗長性が向上します。

データアクセス

この構成は単一の AZ 内にあるため、フローティング IP アドレスは必要ありません。同じ IP アドレスを使用して、 vPC 内からのデータアクセスと、 vPC 外部からのデータアクセスを行うことができます。

次の図は、単一の AZ での HA 構成を示しています。データには、 vPC 内および vPC 外部からアクセスできます。



ストレージのテイクオーバーとギブバック

iSCSI の場合、 ONTAP はマルチパス I/O （ MPIO ）と非対称論理ユニットアクセス（ ALUA ）を使用して、アクティブ最適化パスと非最適化パス間のパスフェイルオーバーを管理します。

> ALUA をサポートする具体的なホスト構成については、を参照してください "NetApp Interoperability Matrix Tool で確認できます" およびお使いのホストオペレーティングシステムに対応した Host Utilities の『 Installation and Setup Guide 』を参照してください。

NAS 構成では、障害が発生した場合に、データ IP アドレスを HA ノード間で移行できます。これにより、クライアントからストレージへのアクセスが保証されます。

HA ペアでのストレージの動作

ONTAP クラスタとは異なり、クラウドボリュームのストレージ ONTAP HA ペアはノード間で共有されません。代わりに、障害発生時にデータを利用できるように、データはノード間で同期的にミラーリングされます。

ストレージの割り当て

新しいボリュームを作成し、ディスクを追加する必要がある場合、 Cloud Manager は同じ数のディスクを両方のノードに割り当て、ミラーリングされたアグリゲートを作成してから、新しいボリュームを作成します。たとえば、ボリュームに 2 つのディスクが必要な場合、 Cloud Manager はノードごとに 2 つのディスクを割り当て、合計で 4 つのディスクを割り当てます。

ストレージ構成

HA ペアは、アクティブ / アクティブ構成として使用できます。アクティブ / アクティブ構成では、両方のノードがクライアントにデータを提供します。アクティブ / パッシブ構成では、パッシブノードは、アクティブノードのストレージをテイクオーバーした場合にのみデータ要求に応答します。

> アクティブ / アクティブ構成をセットアップできるのは、 Storage System View で Cloud Manager を使用している場合のみです。

HA 構成に期待されるパフォーマンス

Cloud Volumes ONTAP HA 構成では、ノード間でデータを同期的にレプリケートするため、ネットワーク帯域幅が消費されます。その結果、シングルノードの Cloud Volumes ONTAP 構成と比較して、次のパフォーマンスが期待できます。

- 1 つのノードからのみデータを提供する HA 構成では、読み取りパフォーマンスはシングルノード構成の読み取りパフォーマンスと同等ですが、書き込みパフォーマンスは低くなります。
- 両方のノードからデータを提供する HA 構成の場合、読み取りパフォーマンスはシングルノード構成の読み取りパフォーマンスよりも高く、書き込みパフォーマンスは同じかそれ以上です。

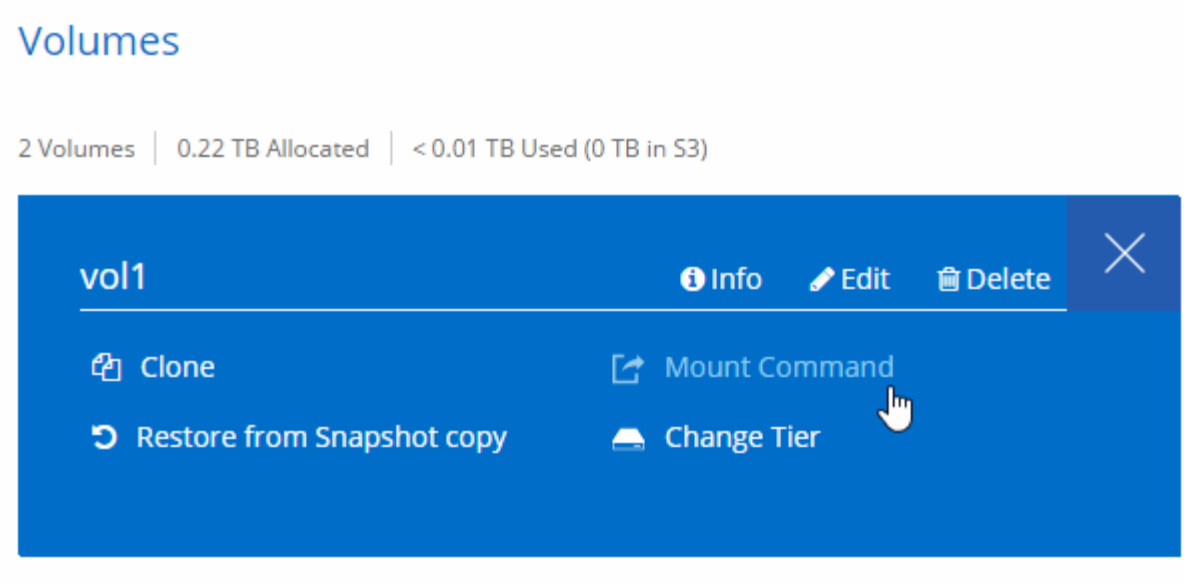
Cloud Volumes ONTAP のパフォーマンスの詳細については、を参照してください "パフォーマンス"。

ストレージへのクライアントアクセス

クライアントは、ボリュームが存在するノードのデータ IP アドレスを使用して、 NFS ボリュームと CIFS ボリュームにアクセスする必要があります。NAS クライアントがパートナーノードの IP アドレスを使用してボリュームにアクセスする場合、トラフィックは両方のノード間を通過するため、パフォーマンスが低下します。

> HA ペアのノード間でボリュームを移動する場合は、もう一方のノードの IP アドレスを使用してボリュームを再マウントする必要があります。そうしないと、パフォーマンスが低下する可能性があります。クライアントが CIFS の NFSv4 リファールまたはフォルダリダイレクションをサポートしている場合は、ボリュームの再マウントを回避するために、 Cloud Volumes ONTAP システムでこれらの機能を有効にできます。詳細については、 ONTAP のマニュアルを参照してください。

Cloud Manager から正しい IP アドレスを簡単に識別できます。

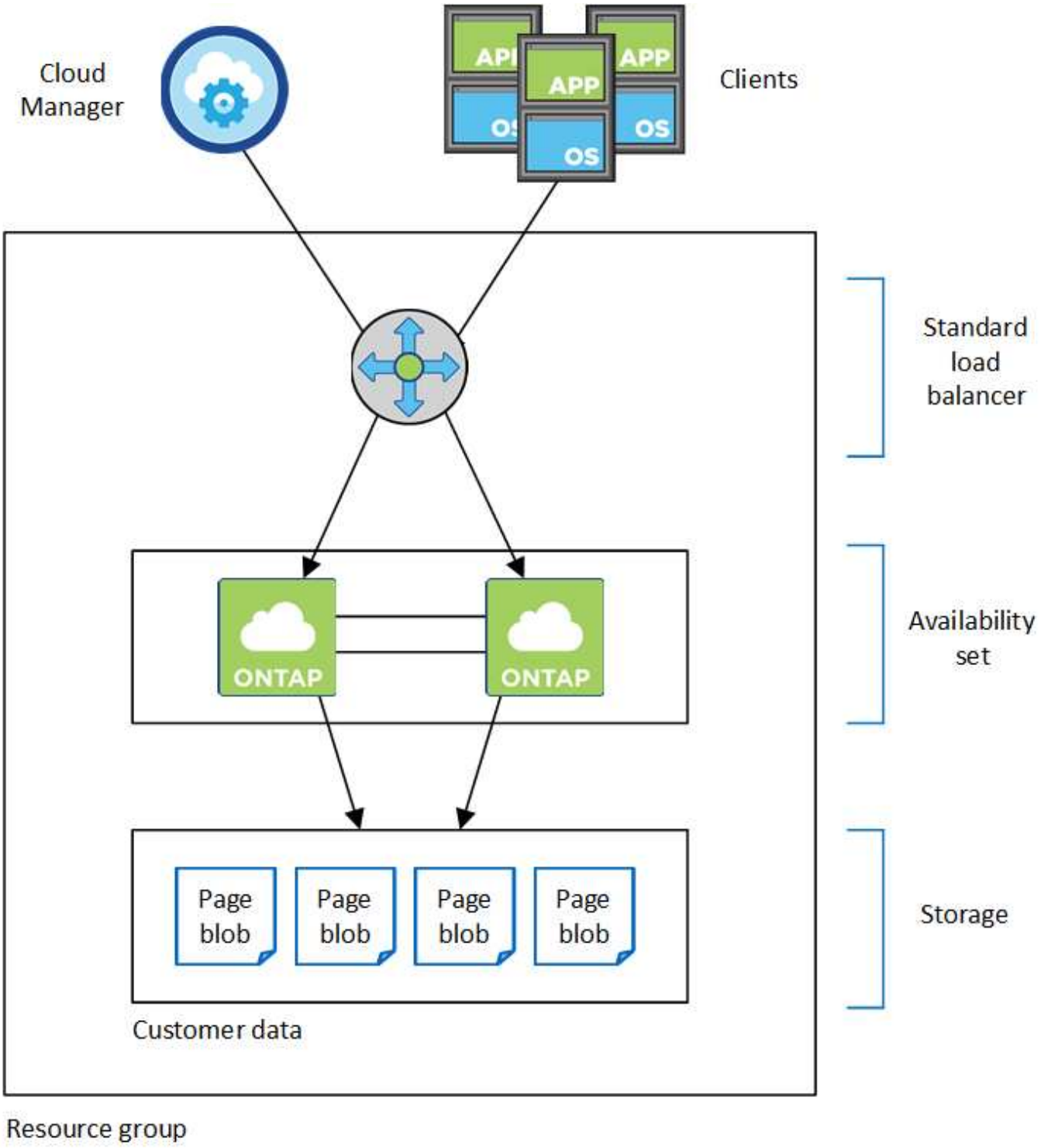


Azure のハイアベイラビリティペア

Cloud Volumes ONTAP ハイアベイラビリティ（HA）ペアは、クラウド環境で障害が発生した場合にエンタープライズクラスの信頼性と継続的な運用を実現します。Azure では、 2 つのノード間でストレージが共有されます。

HA コンポーネント

Azure の Cloud Volumes ONTAP HA 構成には、次のコンポーネントが含まれています。



Cloud Manager で導入される Azure コンポーネントは次のとおりです。

Azure Standard Load Balancer の略

ロードバランサは、 Cloud Volumes ONTAP HA ペアへの着信トラフィックを管理します。

可用性セット

可用性セットは、ノードが異なる障害になっていることを確認し、ドメインを更新します。

ディスク

お客様のデータは Premium Storage ページの BLOB にあります。各ノードがもう一方のノードのストレージにアクセスできます。ブートデータ、ルートデータ、コアデータには、追加のストレージも必要です。

- ブートボリューム用に 90GB の Premium SSD ディスクを 2 本（各ノードに 1 本）
- ルート用の 140 GB Premium Storage ページブロブ 2 つ ボリューム（ノードごとに 1 つ）
- コアを節約するために 128 GB の標準 HDD ディスク 2 台 （ノードごとに 1 つ）

ストレージアカウント

- 管理対象ディスクにはストレージアカウントが 1 つ必要です。
- ストレージ・アカウントあたりのディスク容量の上限に達しているため ' プレミアム・ストレージ・ページ・ブロブには 1 つ以上のストレージ・アカウントが必要です

  "Azure のドキュメント：「 Azure Storage スケーラビリティー and performance targets for storage accounts"。

- Azure BLOB ストレージへのデータ階層化には 1 つのストレージアカウントが必要です。

RPO と **RTO**

HA 構成では、次のようにデータの高可用性が維持されます。

- RPO （ Recovery Point Objective ：目標復旧時点）は 0 秒です。データはトランザクション的に整合性が保たれ、データ損失は発生しません。
- RTO （目標復旧時間）は 60 秒です。システム停止が発生した場合は、 60 秒以内にデータを利用できるようにする必要があります。

ストレージのテイクオーバーとギブバック

物理 ONTAP クラスタと同様に、 Azure HA ペアのストレージはノード間で共有されます。パートナーのストレージに接続することで、 _TAKEOVER_中 に各ノードがもう一方のストレージにアクセスできるようになります。ネットワークパスのフェイルオーバーメカニズムにより、クライアントとホストは稼働しているノードと引き続き通信できます。ノードがオンラインに戻ったときに、 partner_ギ ブバック _storage を提供します。

NAS 構成の場合は、障害の発生時にデータ IP アドレスが HA ノード間で自動的に移行されます。

iSCSI の場合、 ONTAP はマルチパス I/O （ MPIO ）と非対称論理ユニットアクセス（ ALUA ）を使用して、アクティブ最適化パスと非最適化パス間のパスフェイルオーバーを管理します。

> ALUA をサポートする具体的なホスト構成については、を参照してください "NetApp Interoperability Matrix Tool で確認できます" およびお使いのホストオペレーティングシステムに対応した Host Utilities の『 Installation and Setup Guide 』を参照してください。

ストレージ構成

HA ペアは、アクティブ / アクティブ構成として使用できます。アクティブ / アクティブ構成では、両方のノードがクライアントにデータを提供します。アクティブ / パッシブ構成では、パッシブノードは、アクティブノードのストレージをテイクオーバーした場合にのみデータ要求に応答します。

HA の制限事項

Azure の Cloud Volumes ONTAP HA ペアに影響を及ぼす制限事項を次に示します。

- HA ペアは、 Cloud Volumes ONTAP の Standard 、 Premium 、および BYOL でサポートされています。Explore はサポートされていません。
- NFSv4 はサポートされていません。NFSv3 がサポートされています。
- 一部のリージョンでは HA ペアがサポートされません。

  "サポートされる Azure リージョンの一覧を参照してください"。

"Azure に HA システムを導入する方法をご確認ください"。

評価中

Cloud Volumes ONTAP は、ソフトウェアの代金を支払う前に評価できます。

シングルノード Cloud Volumes ONTAP システムの 30 日間無償トライアルをから入手できます "NetApp Cloud Central"。時間単位のソフトウェア料金は発生しませんが、インフラ料金は引き続き適用されます。無料トライアルは、有効期限が切れると、自動的に 1 時間単位の有料サブスクリプションに変換されます。

コンセプトの実証のサポートが必要な場合は、にお問い合わせください "営業チーム" または、から利用できるチャットオプションを使用して、連絡してください "NetApp Cloud Central" さらに、 Cloud Manager からも実行できます。

ライセンス

各クラウドボリューム ONTAP BYOL システムには、アクティブなサブスクリプションを持つライセンスがインストールされている必要があります。アクティブライセンスがインストールされていない場合、 Cloud Volumes ONTAP システムは 30 日後にシャットダウンします。Cloud Manager では、ライセンスを管理し、有効期限が切れる前に通知することで、プロセスを簡素化します。

新しいシステムのライセンス管理

BYOL システムを作成する際、 Cloud Manager は NetApp Support Site のアカウントを入力するように求めます。Cloud Manager は、アカウントを使用してネットアップからライセンスファイルをダウンロードし、Cloud Volumes ONTAP システムにインストールします。

"ネットアップサポートサイトのアカウントをクラウドに追加する方法をご確認ください マネージャー"。

Cloud Manager がセキュアなインターネット接続経由でライセンスファイルにアクセスできない場合は、ファイルを自分で取得してから、手動で Cloud Manager にアップロードできます。手順については、を参照してください "Cloud Volumes ONTAP BYOL システムへのライセンスファイルのインストール"。

ライセンスの有効期限

ライセンスの有効期限が切れる 30 日前と、ライセンスの有効期限が切れる 30 日前に、 Cloud Manager から

警告が表示されます。次の図は、 30 日間の有効期限の警告を示しています。

メッセージを確認する作業環境を選択できます。

ライセンスを期限内に更新しないと、 Cloud Volumes ONTAP システムは自動的にシャットダウンします。再起動すると、自動的にシャットダウンされます。

> Cloud Volumes ONTAP では、 EMS （ Event Management System ）イベント通知を使用して、電子メール、 SNMP トラップホスト、または syslog サーバから通知することもできます。手順については、を参照してください "ONTAP 9 EMS 構成エクスプレスガイド"。

ライセンスの更新

ネットアップの担当者に連絡して BYOL サブスクリプションを更新すると、 Cloud Manager は自動的にネットアップから新しいライセンスを取得し、 Cloud Volumes ONTAP システムにインストールします。

Cloud Manager がセキュアなインターネット接続経由でライセンスファイルにアクセスできない場合は、ファイルを自分で取得してから、手動で Cloud Manager にアップロードできます。手順については、を参照してください "Cloud Volumes ONTAP BYOL システムへのライセンスファイルのインストール"。

セキュリティ

Cloud Volumes ONTAP は、データ暗号化をサポートし、ウィルスやランサムウェアからの保護を提供します。

保存データの暗号化

Cloud Volumes ONTAP は、次の暗号化テクノロジをサポートしています。

- NetApp Volume Encryption （ Cloud Volumes ONTAP 9.5 以降）
- AWS Key Management Service の略
- Azure Storage Service Encryption の略
- Google Cloud Platform のデフォルトの暗号化

NetApp Volume Encryption は、 AWS 、 Azure 、 GCP のネイティブ暗号化機能と組み合わせて使用できます。 GCP 暗号化はハイパーバイザーレベルでデータを暗号化します。

NetApp Volume Encryption の略

NetApp Volume Encryption （ NVE ）は、一度に 1 ボリュームずつ保管データを暗号化するためのソフトウェアベースのテクノロジです。データ、 Snapshot コピー、およびメタデータが暗号化されます。データへのア

クセスには、ボリュームごとに 1 つずつ、一意の XTS-AES-256 キーを使用します。

Cloud Volumes ONTAP は、外部キー管理サーバを使用した NetApp Volume Encryption をサポートしています。オンボードキーマネージャはサポートされていません。サポートされているキー管理ツールは、で確認できます "NetApp Interoperability Matrix Tool で確認できます" 主要マネージャー * ソリューションの下。

CLI または System Manager を使用して、新規または既存のボリュームで NetApp Volume Encryption を有効にできます。Cloud Manager では、 NetApp Volume Encryption がサポートされていません。手順については、を参照してください "NetApp ボリューム暗号化によるボリュームの暗号化"。

AWS Key Management Service の略

AWS で Cloud Volumes ONTAP システムを起動する場合、を使用してデータ暗号化を有効にできます "AWS Key Management Service （ KMS ；キー管理サービス）"。Cloud Manager は、 Customer Master Key （ CMK ）を使用してデータキーを要求します。

> Cloud Volumes ONTAP システムの作成後に AWS のデータ暗号化方式を変更することはできません。

この暗号化オプションを使用する場合は、 AWS KMS が適切に設定されていることを確認する必要があります。詳細については、を参照してください "AWS KMS のセットアップ"。

Azure Storage Service Encryption の略

"Azure Storage Service Encryption の略" Azure の Cloud Volumes ONTAP データでは、保存データに対してデフォルトで有効になります。セットアップは必要ありません。

> お客様が管理するキーは、 Cloud Volumes ONTAP ではサポートされません。

Google Cloud Platform のデフォルトの暗号化

"Google Cloud Platform の保存データ暗号化機能" Cloud Volumes ONTAP ではデフォルトで有効になっています。セットアップは必要ありません。

Google Cloud Storage では常にデータが暗号化されてからディスクに書き込まれますが、 Cloud Manager API を使用して、 _cuser-managed 暗号化キー _ を使用する Cloud Volumes ONTAP システムを作成できます。これらは、 Cloud Key Management Service を使用して GCP で生成および管理するキーです。

を参照してください "API 開発者ガイド" "GcpEncryption" パラメータの使用方法の詳細については、を参照してください。

ONTAP のウィルススキャン

ONTAP システムの統合アンチウイルス機能を使用すると、データがウイルスやその他の悪意のあるコードによって危険にさらされるのを防ぐことができます。

ONTAP ウィルススキャン（ _vscan ）は、クラス最高のサードパーティ製ウィルス対策ソフトウェアと ONTAP 機能を組み合わせたもので、どのファイルをスキャンするか、いつスキャンするかを柔軟に制御できます。

Vscan でサポートされるベンダー、ソフトウェア、およびバージョンについては、を参照してください

"NetApp Interoperability Matrix を参照してください"。

ONTAP システムでウィルス対策機能を設定および管理する方法については、を参照してください "ONTAP 9 ウィルス対策構成ガイド"。

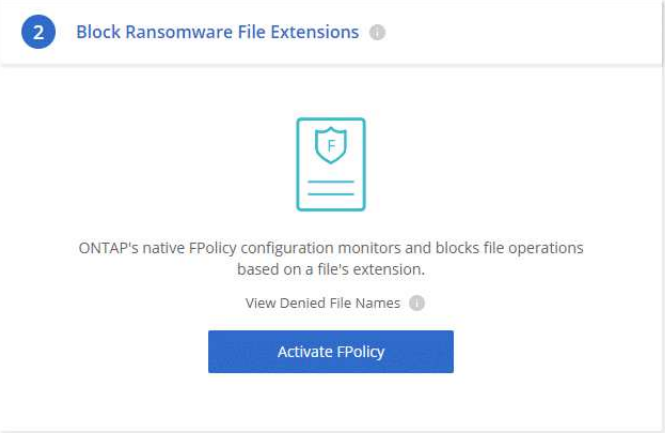
ランサムウェアからの保護

ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。Cloud Manager では、ランサムウェアに対応したネットアップソリューションを実装できます。これにより、可視化、検出、修復のための効果的なツールが提供されます。

- Cloud Manager は、 Snapshot ポリシーで保護されていないボリュームを特定し、それらのボリュームのデフォルトの Snapshot ポリシーをアクティブ化できます。

  Snapshot コピーは読み取り専用であり、ランサムウェアによる破損を防止します。単一のファイルコピーまたは完全なディザスタリカバリソリューションのイメージを作成する際の単位を提供することもできます。

- Cloud Manager では、 ONTAP の FPolicy ソリューションを有効にすることで、一般的なランサムウェアのファイル拡張子をブロックすることもできます。



"ネットアップのランサムウェア向けソリューションの実装方法をご確認ください"。

パフォーマンス

パフォーマンスの結果を確認して、 Cloud Volumes ONTAP に適したワークロードを決定できます。

Cloud Volumes ONTAP for AWS については、を参照してください "NetApp テクニカルレポート 4383 ：アプリケーションワークロードを使用した Amazon Web Services における Cloud Volumes ONTAP のパフォーマンス特性"。

Cloud Volumes ONTAP for Microsoft Azure については、を参照してください "NetApp テクニカルレポート 4671 ：アプリケーションワークロードを使用した Azure における Cloud Volumes ONTAP のパフォーマンス特性評価"。

はじめに

導入の概要

開始する前に、 Cloud Manager および Cloud Volumes ONTAP を導入するためのオプションについて理解を深めておくことを推奨します。

Cloud Manager のインストール

Cloud Volumes ONTAP の導入と管理には、 Cloud Manager ソフトウェアが必要です。Cloud Manager は、次のいずれかの場所に導入できます。

- Amazon Web Services （ AWS ）
- Microsoft Azure
- Google Cloud Platform の 1 つです

  GCP に Cloud Volumes ONTAP を導入する場合は、 Cloud Manager が Google Cloud Platform に含まれている必要があります。

- IBM クラウド
- 自分のネットワーク内

Cloud Manager の導入方法は、選択する場所によって異なります。

Cloud Manager の場所	Cloud Manager の導入方法
AWS	1. "NetApp Cloud Central から Cloud Manager を導入する" （推奨） 2. "AWS Marketplace から導入" 3. "Linux ホストにソフトウェアをダウンロードしてインストールします"
AWS C2S	"AWS Intelligence Community Marketplace から Cloud Manager を導入"
Azure の一般提供地域	1. "NetApp Cloud Central から Cloud Manager を導入する" （推奨） 2. "Azure Marketplace から導入" 3. "Linux ホストにソフトウェアをダウンロードしてインストールします"
Azure Government	"Azure US Government Marketplace から Cloud Manager を導入"
Azure ドイツ	"Linux ホストにソフトウェアをダウンロードしてインストールします"

Cloud Manager の場所	Cloud Manager の導入方法
Google Cloud Platform の 1 つです	1. "NetApp Cloud Central から Cloud Manager を導入する" （推奨） 2. "Linux ホストにソフトウェアをダウンロードしてインストールします" GCP Marketplace から Google Cloud で Cloud Manager を導入することはできません
IBM クラウド	"Linux ホストにソフトウェアをダウンロードしてインストールします"
オンプレミスネットワーク	"Linux ホストにソフトウェアをダウンロードしてインストールします"

Cloud Manager のセットアップ

Cloud Manager のインストール後に、クラウドプロバイダアカウントの追加、 HTTPS 証明書のインストールなどの追加のセットアップを実行できます。

- "Cloud Central アカウントをセットアップします"
- "Cloud Manager に AWS アカウントを追加する"
- "Cloud Manager への Azure アカウントの追加"
- "HTTPS 証明書のインストール"
- "AWS KMS のセットアップ"

Cloud Volumes ONTAP の導入

Cloud Manager を起動して実行したら、クラウドプロバイダで Cloud Volumes ONTAP の導入を開始できます。

"AWS の概要"、 "Azure の導入を開始します"および "GCP の概要" Cloud Volumes ONTAP を短時間で起動して実行するための手順を説明します。その他のヘルプについては、次を参照してください。

- "AWS の Cloud Volumes ONTAP 9.7 でサポートされている構成"
- "Cloud Volumes ONTAP 9.7 で Azure でサポートされる構成"
- "GCP の Cloud Volumes ONTAP 9.7 でサポートされている構成"
- "構成の計画"
- "AWS での Cloud Volumes ONTAP の起動"
- "Azure で Cloud Volumes ONTAP を起動します"
- "GCP での Cloud Volumes ONTAP の起動"

AWS で Cloud Volumes ONTAP を使用するための準備

Cloud Volumes ONTAP の使用を開始するには、 AWS をセットアップし、 NetApp Cloud Central から Cloud Manager ソフトウェアを起動します。AWS で初めて Cloud

Volumes ONTAP システムを起動された場合、 30 日間の無償トライアルが利用できます。

1 ネットワークをセットアップします

1. Cloud Manager と Cloud Volumes ONTAP が複数のエンドポイントに接続できるように、ターゲット vPC からのアウトバウンドインターネットアクセスを有効にします。

   Cloud Manager ではアウトバウンドのインターネットアクセスなしで Cloud Volumes ONTAP を導入できないため、この手順は重要です。アウトバウンド接続を制限する必要がある場合は、のエンドポイントのリストを参照してください "クラウドマネージャ" および "Cloud Volumes ONTAP"。

2. S3 サービスへの vPC エンドポイントをセットアップします。

   Cloud Volumes ONTAP から低コストのオブジェクトストレージにコールドデータを階層化する場合は、VPC エンドポイントが必要です。

2 必要な **AWS** 権限を指定します

NetApp Cloud Central から Cloud Manager を導入する場合は、インスタンスを導入する権限を持つ AWS アカウントを使用する必要があります。

1. AWS IAM コンソールに移動し、の内容をコピーして貼り付け、ポリシーを作成します "AWS 向けの NetApp Cloud Central ポリシー"。
2. IAM ユーザにポリシーを付加します。

3 **AWS Marketplace** でサブスクライブ

"AWS Marketplace で Cloud Manager のサブスクリプションを登録します" Cloud Volumes ONTAP の無償トライアルの終了後にサービスを中断しないようにするため。作成した Cloud Volumes ONTAP PAYGO システムごと、および有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。

独自のライセンスを使用（ BYOL ）して Cloud Volumes ONTAP を起動する場合は、 "その後、 AWS Marketplace でそのサービスに登録する必要があります"。

4 **NetApp Cloud Central** から **Cloud Manager** を起動します

Cloud Volumes ONTAP の導入と管理には、 Cloud Manager ソフトウェアが必要です。から Cloud Manager インスタンスを起動するには数分かかります "Cloud Central にアクセスできます"。

5 **Cloud Manager** を使用して **Cloud Volumes ONTAP** を起動します

Cloud Manager の準備ができたら、 [作成] をクリックし、起動するシステムのタイプを選択して、ウィザードの手順を完了します。25 分経過すると、最初の Cloud Volumes ONTAP システムが起動して実行されま

す。

次のビデオでは、これらの手順を説明しています。

▶ https://docs.netapp.com/ja-jp/occm37//media/video_getting_started_aws.mp4 *(video)*

関連リンク

- "評価中"
- "Cloud Manager のネットワーク要件"
- "Cloud Volumes ONTAP in AWS のネットワーク要件"
- "AWS のセキュリティグループルール"
- "Cloud Manager に AWS アカウントを追加する"
- "Cloud Manager が AWS 権限を使用して実行する処理"
- "AWS での Cloud Volumes ONTAP の起動"
- "AWS Marketplace からの Cloud Manager の起動"

Azure での Cloud Volumes ONTAP の導入

Cloud Volumes ONTAP の利用を開始するには、 Azure をセットアップし、 NetApp Cloud Central から Cloud Manager ソフトウェアを導入します。Cloud Manager の導入手順については、を参照してください "Azure US Government リージョン" およびインチ "Azure ドイツ地域"。

1 ネットワークをセットアップします

Cloud Manager と Cloud Volumes ONTAP が複数のエンドポイントに接続できるように、ターゲット Vnet からアウトバウンドインターネットアクセスを有効にします。

この手順は重要です。 Cloud Manager では、アウトバウンドインターネットアクセスがないと Cloud Volumes ONTAP を導入できないためです。アウトバウンド接続を制限する必要がある場合は、のエンドポイントのリストを参照してください "クラウドマネージャ" および "Cloud Volumes ONTAP"。

2 必要な **Azure** 権限を指定します

NetApp Cloud Central から Cloud Manager を導入する場合は、 Cloud Manager 仮想マシンを導入する権限を持つ Azure アカウントを使用する必要があります。

1. をダウンロードします "Azure 向けの NetApp Cloud Central ポリシー"。
2. 「割り当て可能スコープ」フィールドに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。
3. JSON ファイルを使用して、 Azure で _Azure SetupAsService_という 名前のカスタムロールを作成します。

例： * AZ ロール定義 create - ロール定義 C ： \Policy_For _Setup_as-a-Service _Azure.json *

4. Azure ポータルから、 Cloud Central から Cloud Manager を導入するユーザにカスタムロールを割り当てます。

3 NetApp Cloud Central から Cloud Manager を起動します

Cloud Volumes ONTAP の導入と管理には、 Cloud Manager ソフトウェアが必要です。から Cloud Manager インスタンスを起動するには数分かかります "Cloud Central にアクセスできます"。

4 Cloud Manager を使用して Cloud Volumes ONTAP を起動します

Cloud Manager の準備ができたら、 [作成] をクリックし、導入するシステムのタイプを選択して、ウィザードの手順を完了します。25 分経過すると、最初の Cloud Volumes ONTAP システムが起動して実行されます。

関連リンク

- "評価中"
- "Cloud Manager のネットワーク要件"
- "Azure の Cloud Volumes ONTAP のネットワーク要件"
- "Azure のセキュリティグループルール"
- "Cloud Manager への Azure アカウントの追加"
- "クラウドマネージャーが Azure の権限で行うこと"
- "Azure で Cloud Volumes ONTAP を起動します"
- "Azure Marketplace からの Cloud Manager の起動"

Google Cloud Platform での Cloud Volumes ONTAP の使用を開始する

Cloud Volumes ONTAP の使用を開始するには、 GCP をセットアップしてから、NetApp Cloud Central から Cloud Manager ソフトウェアを導入します。

GCP に Cloud Volumes ONTAP を導入するには、 Cloud Manager が Google Cloud Platform にインストールされている必要があります。

1 ネットワークをセットアップします

Cloud Manager と Cloud Volumes ONTAP が複数のエンドポイントに接続できるように、ターゲット vPC からのアウトバウンドインターネットアクセスを有効にします。

Cloud Manager ではアウトバウンドのインターネットアクセスなしで Cloud Volumes ONTAP を導入できないため、この手順は重要です。アウトバウンド接続を制限する必要がある場合は、のエンドポイントのリストを参照してください "クラウドマネージャ" および "Cloud Volumes ONTAP"。

2 GCP の権限とプロジェクトを設定します

2 組の権限が設定されていることを確認します。

1. Cloud Manager を導入する GCP ユーザがであることを確認します NetApp Cloud Central には、にアクセス許可が含まれています "GCP 向けの Cloud Central ポリシー"。

   "YAML ファイルを使用してカスタムロールを作成できます" ユーザーに添付します。gcloud コマンドラインを使用して、ロールを作成する必要があります。

2. プロジェクトで Cloud Volumes ONTAP システムを作成および管理するために Cloud Manager に必要な権限を持つサービスアカウントをセットアップします。

   手順 6 で、このサービスアカウントを Cloud Manager VM に関連付けます。

   - "GCP で役割を作成します" で定義した権限を含むポリシーを作成します "GCP 向け Cloud Manager ポリシー"。ここでも gcloud コマンドラインを使用する必要があります。

     この YAML ファイルに含まれる権限は、手順 2a の権限とは異なります。

   - "GCP サービスアカウントを作成し、カスタムロールを適用します を作成しました"。
   - Cloud Volumes ONTAP を他のプロジェクトに導入する場合は、 "クラウドでサービスアカウントを追加してアクセスを許可します そのプロジェクトに対するマネージャの役割"。プロジェクトごとにこの手順を繰り返す必要があります。

3 データ階層化用の GCP をセットアップします

Cloud Volumes ONTAP 9.7 から低コストのオブジェクトストレージ（ Google Cloud Storage バケット）にコールドデータを階層化するには、次の 2 つの要件を満たす必要があります。

1. "サービスアカウントを作成します" 事前定義された Storage Admin ロールと Cloud Manager サービスアカウントをユーザとして使用する必要があります。

   このサービスアカウントは、 Cloud Volumes ONTAP 作業環境の作成後に選択する必要があります。このサービスアカウントは、手順 2 で作成したサービスアカウントとは異なります。

2. "プライベート Google アクセス用の Cloud Volumes ONTAP サブネットを設定します"。

Cloud Volumes ONTAP 9.6 でデータ階層化を使用する場合は、 "その後、以下の手順を実行します"。

4 Google Cloud API を有効にします

"プロジェクトで次の Google Cloud API を有効にします"。これらの API は、 Cloud Manager と Cloud Volumes ONTAP の導入に必要です。

- Cloud Deployment Manager V2 API
- Cloud Resource Manager API の略

- Compute Engine API
- Stackdriver Logging API のことです

5 **GCP Marketplace** から登録します

"GCP Marketplace から Cloud Volumes ONTAP に登録します" 無償トライアルの終了後にサービスを中断しないようにするため。作成した Cloud Volumes ONTAP PAYGO システムごとに、このサブスクリプションから課金されます。

6 **NetApp Cloud Central** から **Cloud Manager** を起動します

Cloud Volumes ONTAP の導入と管理には、 Cloud Manager ソフトウェアが必要です。から GCP で Cloud Manager インスタンスを起動するには数分かかります "Cloud Central にアクセスできます"。

クラウドプロバイダとして GCP を選択すると、 Google からアカウントにログインして権限を付与するよう求められます。「許可」をクリックすると、 Cloud Manager の導入に必要なコンピューティング API へのアクセスが許可されます。

7 **Cloud Manager** を使用して **Cloud Volumes ONTAP** を起動します

Cloud Manager の準備ができたら、 [作成] をクリックし、導入するシステムのタイプを選択して、ウィザードの手順を完了します。25 分経過すると、最初の Cloud Volumes ONTAP システムが起動して実行されます。

関連リンク

- "評価中"
- "Cloud Manager のネットワーク要件"
- "Cloud Volumes ONTAP in GCP のネットワーク要件"
- "GCP のファイアウォールルール"
- "Cloud Manager が GCP 権限を使用して実行する処理"
- "GCP での Cloud Volumes ONTAP の起動"
- "Linux ホストに Cloud Manager ソフトウェアをダウンロードしてインストールする"

Cloud Manager をセットアップする

Cloud Central アカウントでのワークスペースとユーザのセットアップ

各 Cloud Manager システムには、 _NetApp Cloud Central アカウント _ が関連付けられています。ユーザが Cloud Manager にアクセスしてワークスペースに Cloud Volumes ONTAP システムを導入できるように、 Cloud Manager システムに関連付けられた Cloud Central アカウントをセットアップします。ユーザを追加するか、複数のユーザとワークスペースを追加するだけです。

アカウントは Cloud Central で管理されるため、ユーザが行った変更は他の Cloud Manager システムやネットアップクラウドデータサービスにも適用されます。 "Cloud Central アカウントの仕組みの詳細については、こちらをご覧ください"。

ワークスペースの追加

Cloud Manager のワークスペースを使用すると、作業環境のセットを他の作業環境や他のユーザから分離できます。たとえば、 2 つのワークスペースを作成し、別々のユーザをワークスペースに関連付けることができます。

手順

1. 「 * アカウント設定 * 」をクリックします。

2. [* ワークスペース *] をクリックします。
3. [新規ワークスペースの追加] をクリックします。
4. ワークスペースの名前を入力し、 * 追加 * をクリックします。

完了後

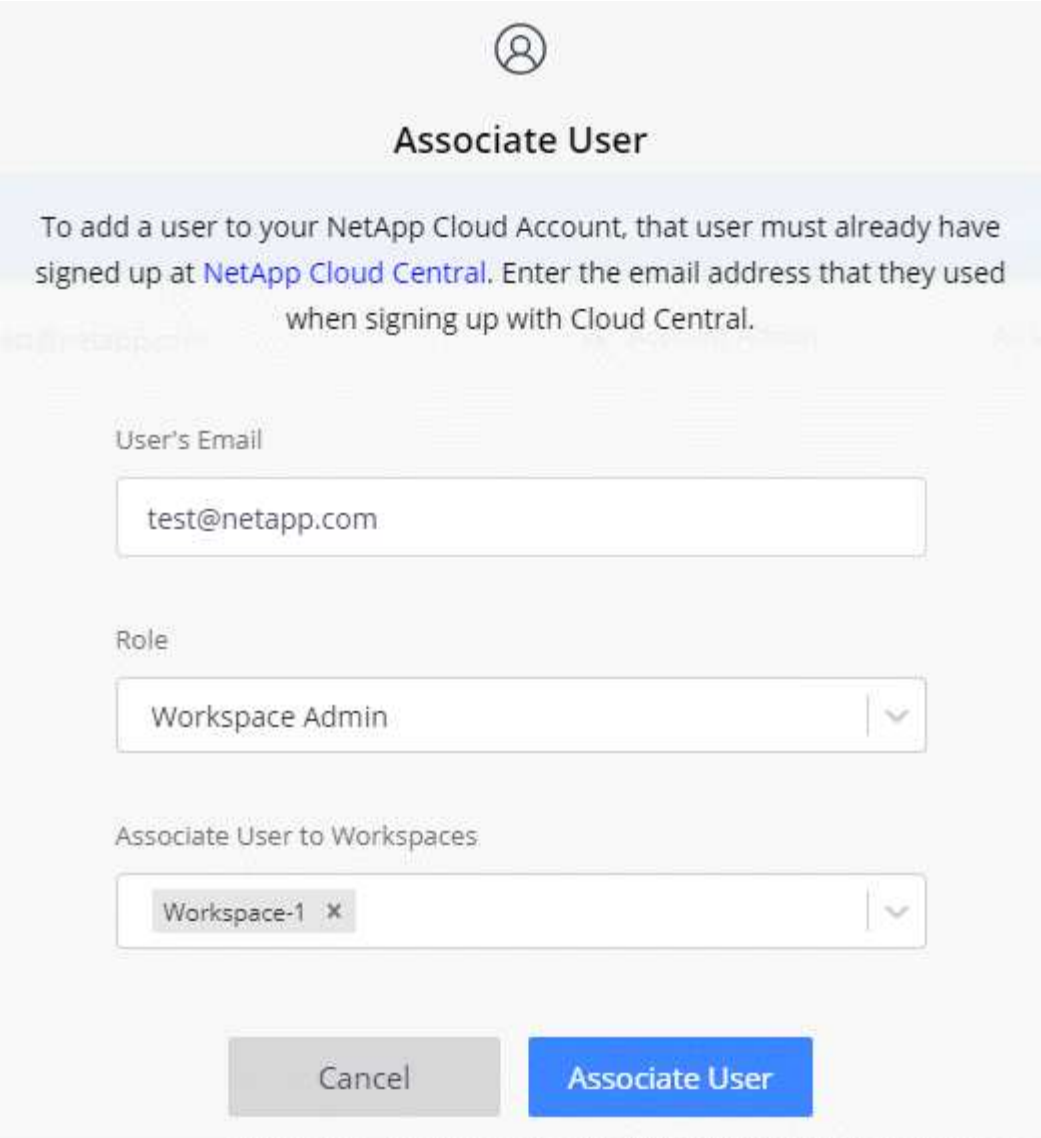
ユーザーとサービスコネクタをワークスペースに関連付けることができるようになりました。

ユーザを追加する

Cloud Central ユーザを Cloud Central アカウントに関連付けて、これらのユーザが Cloud Manager で作業環境を作成および管理できるようにします。

手順

1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp Cloud Central" アカウントを作成します。
2. Cloud Manager で、 * アカウント設定 * をクリックします。
3. [ユーザー] タブで、 [ユーザーの関連付け] をクリックします。
4. ユーザの E メールアドレスを入力し、ユーザのロールを選択します。
   - * アカウント管理者 * ： Cloud Manager で任意の操作を実行できます。
   - * ワークスペース管理者 * ：割り当てられたワークスペースでリソースを作成および管理できます。
5. Workspace Admin を選択した場合は、 1 つ以上のワークスペースを選択してそのユーザーに関連付けます。



6. [ユーザーの関連付け] をクリックします。

結果

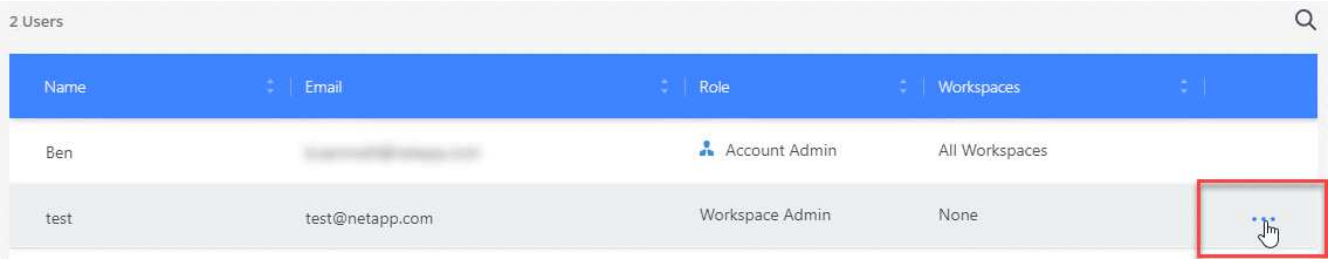
ユーザには、 NetApp Cloud Central の「 Account Association 」というタイトルの E メールが送信されます。 E メールには、 Cloud Manager にアクセスするために必要な情報が記載されています。

ワークスペース管理者とワークスペースの関連付け

ワークスペース管理者は、いつでも追加のワークスペースに関連付けることができます。ユーザーを関連付けると、ワークスペース内の作業環境を作成して表示できます。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. ユーザに対応する行のアクションメニューをクリックします。



3. * ワークスペースの管理 * をクリックします。
4. 1 つ以上のワークスペースを選択し、 * 適用 * をクリックします。

結果

サービスコネクタもワークスペースに関連付けられていれば、ユーザは Cloud Manager からこれらのワークスペースにアクセスできるようになりました。

サービスコネクタとワークスペースの関連付け

サービスコネクタは、 Cloud Manager システムの一部です。クラウドプロバイダに導入された仮想マシンインスタンス上、または設定したオンプレミスホスト上で実行されます。このサービスコネクタをワークスペースに関連付けて、 Workspace 管理者がこれらのワークスペースに Cloud Manager からアクセスできるようにする必要があります。

アカウント管理者のみがいる場合は、サービスコネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。

"ユーザー、ワークスペース、サービスコネクタの詳細をご覧ください"。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. サービスコネクター * をクリックします。
3. 関連付けるサービスコネクタの [ワークスペースの管理 *] をクリックします。
4. 1 つ以上のワークスペースを選択し、 * 適用 * をクリックします。

結果

ワークスペース管理者は、ユーザーがワークスペースにも関連付けられている限り、関連付けられたワークスペースにアクセスできるようになりました。

AWS アカウントのセットアップと Cloud Manager への追加

Cloud Volumes ONTAP を別々の AWS アカウントに導入する場合は、必要な権限を指定し、 Cloud Manager に詳細を追加する必要があります。権限の指定方法は、 Cloud Manager に AWS キーを提供するか、信頼されたアカウントのロールの ARN を提供するかによって異なります。

> Cloud Central から Cloud Manager を導入すると、 Cloud Manager を導入した AWS アカウントが Cloud Manager によって自動的に追加されます。初期アカウントは、既存のシステムに Cloud Manager ソフトウェアを手動でインストールした場合は追加されません。 "AWS のアカウントと権限について説明します"。

- 選択肢 *
- AWS キーを指定して権限を付与します
- 他のアカウントで IAM ロールを想定して権限を付与する

AWS キーを指定して権限を付与します

Cloud Manager に IAM ユーザの AWS キーを提供する場合は、必要な権限をそのユーザに付与する必要があります。Cloud Manager IAM ポリシーは、 Cloud Manager が使用できる AWS アクションとリソースを定義します。

手順

1. から Cloud Manager IAM ポリシーをダウンロードします "Cloud Manager Policies ページ"。
2. IAM コンソールから、 Cloud Manager IAM ポリシーからテキストをコピーアンドペーストして、独自のポリシーを作成します。

   "AWS のドキュメント：「 Creating IAM Policies"

3. IAM ロールまたは IAM ユーザにポリシーを関連付けます。
   - "AWS のドキュメント：「 Creating IAM Roles"
   - "AWS のドキュメント：「 Adding and Removing IAM Policies"

結果

これで、アカウントに必要な権限が付与されました。 これで、 Cloud Manager に追加できます。

他のアカウントで **IAM** ロールを想定して権限を付与する

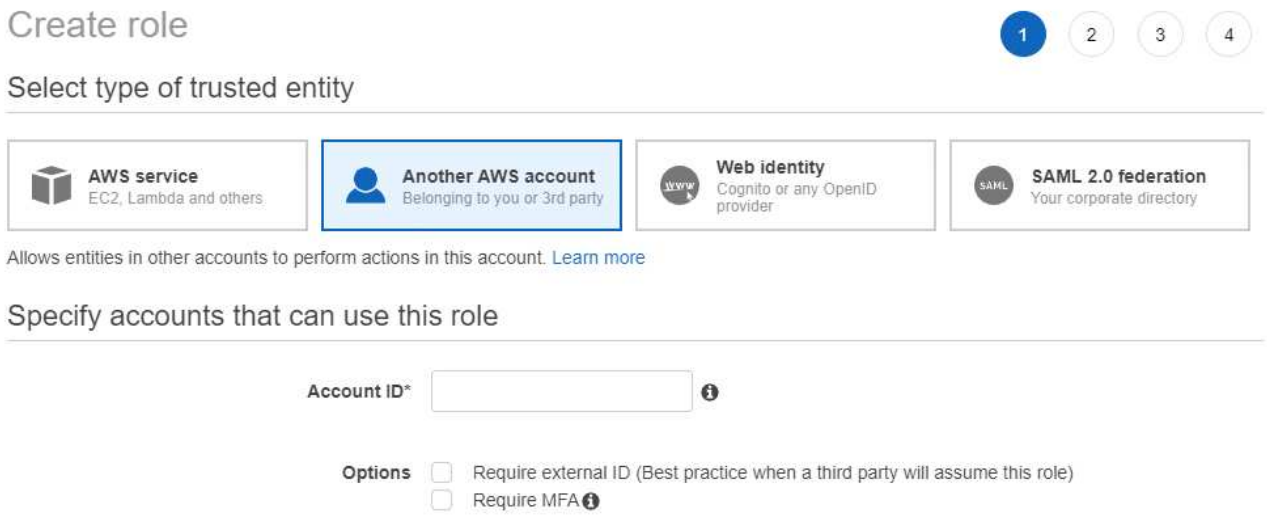
Cloud Manager インスタンスを導入したソース AWS アカウントと他の AWS アカウントの間には、 IAM ロールを使用して信頼関係を設定できます。その後、 Cloud Manager に信頼されたアカウントの IAM ロールの ARN を提供します。

手順

1. Cloud Volumes ONTAP を導入するターゲットアカウントに移動し、 * 別の AWS アカウント * を選択して IAM ロールを作成します。

   必ず次の手順を実行してください。

   - Cloud Manager インスタンスが存在するアカウントの ID を入力します。
   - から入手できる Cloud Manager IAM ポリシーを関連付けます "Cloud Manager Policies ページ"。



2. Cloud Manager インスタンスが存在するソースアカウントに移動し、インスタンスに関連付けられている IAM ロールを選択します。

   a. [信頼関係] 、 [信頼関係の編集 *] の順にクリックします。

   b. ターゲットアカウントで作成したロールの「 STS: AssumeRole 」アクションと ARN を追加します。

      - 例 *

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

結果

これで、アカウントに必要な権限が付与されました。 これで、 Cloud Manager に追加できます。

Cloud Manager に AWS アカウントを追加する

必要な権限を持つ AWS アカウントを指定したら、そのアカウントを Cloud Manager に追加できます。これにより、そのアカウントで Cloud Volumes ONTAP システムを起動できます。

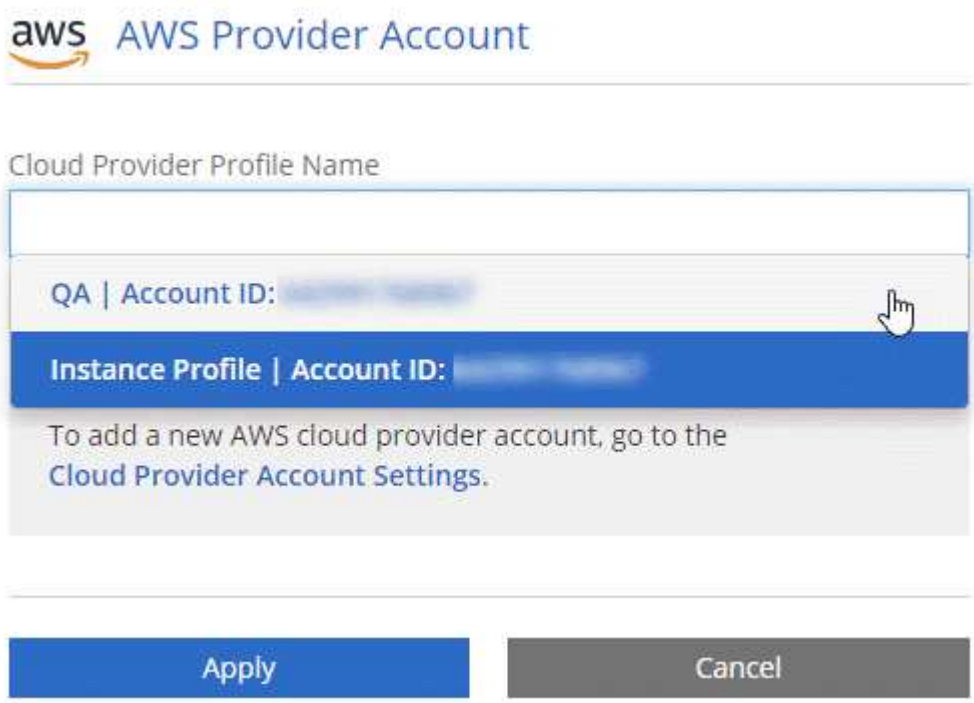
手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クラウドプロバイダとサポートアカウント * を選択します。

2. [Add New Account*] をクリックし、 [* AWS*] を選択します。
3. AWS キーを指定するか、信頼された IAM ロールの ARN を指定するかを選択します。
4. ポリシーの要件が満たされていることを確認し、 * アカウントの作成 * をクリックします。

結果

新しい作業環境を作成するときに、 [詳細と資格情報] ページから別のアカウントに切り替えることができるようになりました。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

Azure アカウントを設定して Cloud Manager に追加

Cloud Volumes ONTAP を別々の Azure アカウントに導入する場合は、それらのアカウントに必要な権限を指定し、アカウントに関する詳細を Cloud Manager に追加する必要があります。

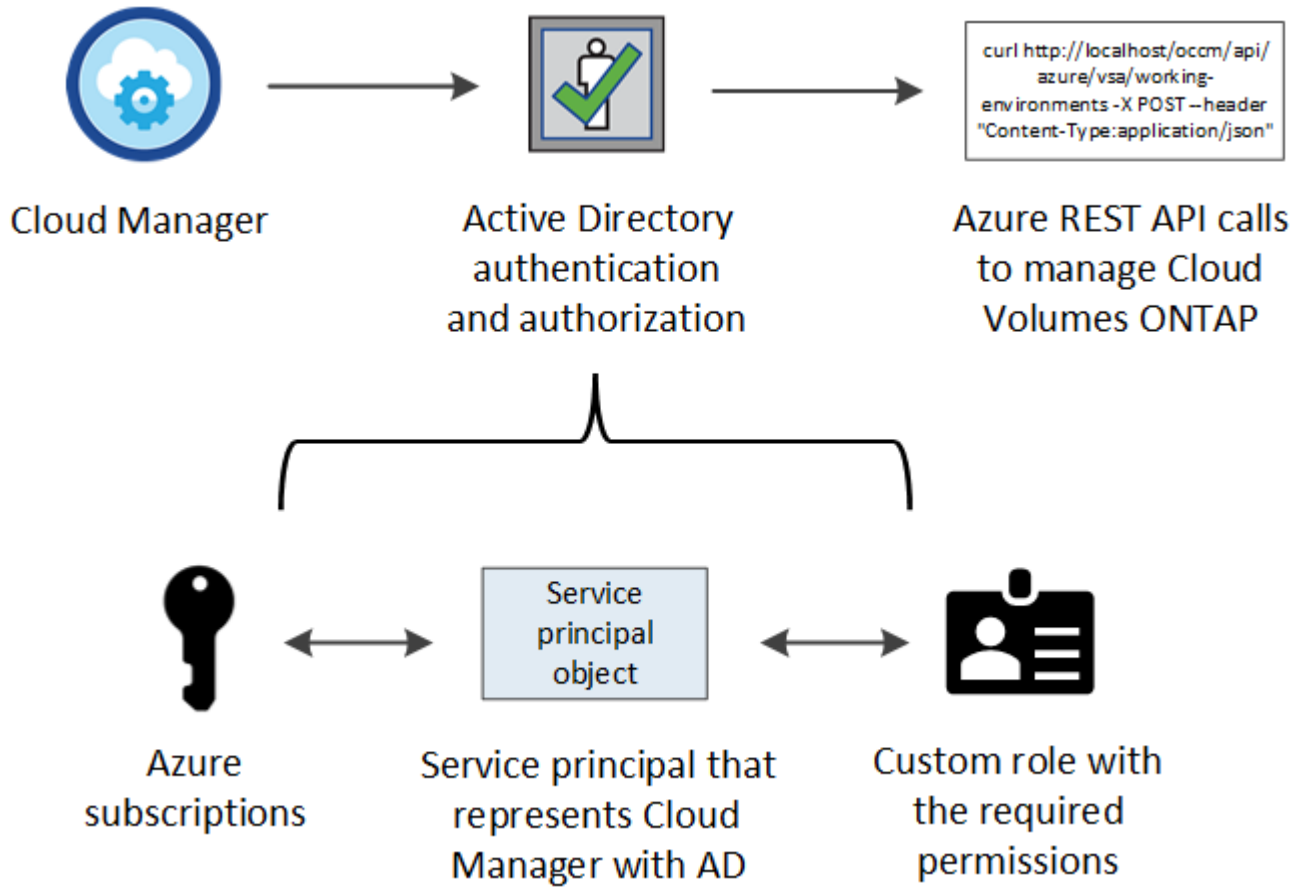
> Cloud Central から Cloud Manager を導入すると、 Cloud Manager を導入した Azure アカウントが Cloud Manager によって自動的に追加されます。初期アカウントは、既存のシステムに Cloud Manager ソフトウェアを手動でインストールした場合は追加されません。 "Azure のアカウントと権限について説明します"。

サービスプリンシパルを使用した **Azure** 権限の付与

Cloud Manager には、 Azure でアクションを実行するための権限が必要です。Azure アカウントに必要な権限を付与するには、 Azure Active Directory でサービスプリンシパルを作成して設定し、 Cloud Manager で必要な Azure クレデンシャルを取得します。

このタスクについて

次の図は、 Cloud Manager が Azure で操作を実行するための権限を取得する方法を示しています。1 つ以上の Azure サブスクリプションに関連付けられたサービスプリンシパルオブジェクトは、 Azure Active Directory の Cloud Manager を表し、必要な権限を許可するカスタムロールに割り当てられます。



手順

1. Azure Active Directory アプリケーションを作成します。
2. アプリケーションをロールに割り当てます。
3. Windows Azure Service Management API 権限を追加します。
4. アプリケーション ID とディレクトリ ID を取得します。
5. クライアントシークレットを作成します。

Azure Active Directory アプリケーションの作成

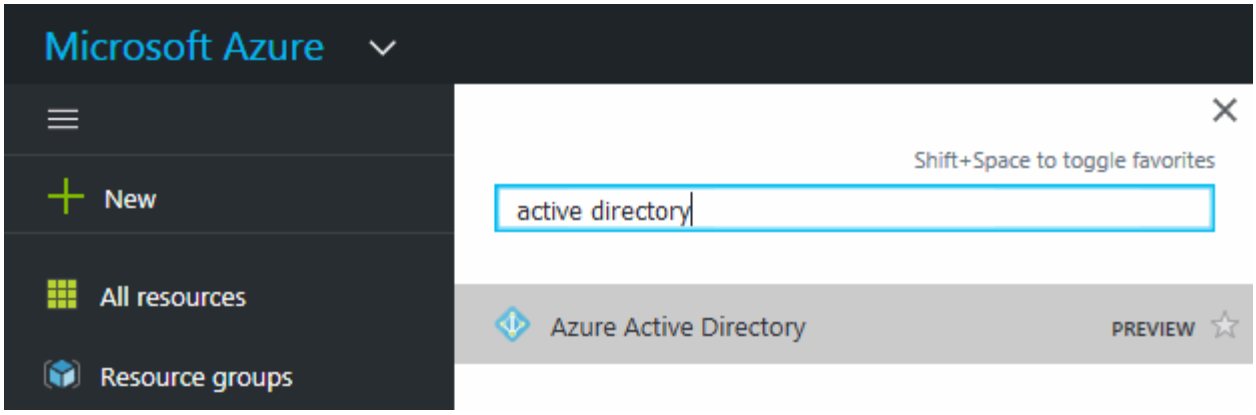
Cloud Manager でロールベースアクセス制御に使用できる Azure Active Directory （ AD ）アプリケーションとサービスプリンシパルを作成します。

作業を開始する前に

Azure で Active Directory アプリケーションを作成してロールに割り当てるための適切な権限が必要です。詳細については、を参照してください "Microsoft Azure のドキュメント：「 Required permissions"。

手順

1. Azure ポータルで、 * Azure Active Directory * サービスを開きます。



2. メニューで、 * アプリ登録 * をクリックします。
3. [新規登録] をクリックします。
4. アプリケーションの詳細を指定します。
   - * 名前 * ：アプリケーションの名前を入力します。
   - * アカウントタイプ * ：アカウントタイプを選択します（ Cloud Manager で使用できます）。
   - * リダイレクト URI **:[*Web**] を選択し、任意の URL を入力します。たとえば、 https://url と入力します
5. [*Register] をクリックします。

結果

AD アプリケーションとサービスプリンシパルを作成しておきます。

アプリケーションをロールに割り当てます

Azure で Cloud Manager に権限を付与するには、サービスプリンシパルを 1 つ以上の Azure サブスクリプションにバインドし、カスタムの「 OnCommand Cloud Manager Operator 」ロールを割り当てる必要があります。

手順

1. カスタムロールを作成します。
   a. をダウンロードします "Cloud Manager Azure ポリシー"。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。

      ユーザが Cloud Volumes ONTAP システムを作成する Azure サブスクリプションごとに ID を追加する必要があります。

      - 例 *

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. JSON ファイルを使用して、 Azure でカスタムロールを作成します。

次の例は、 Azure CLI 2.0 を使用してカスタムロールを作成する方法を示しています。

- AZ 役割定義 create — 役割定義 C ： \Policy_For _Cloud_Manager_Azure_3.7.4.json *

OnCommand Cloud Manager Operator _ という名前のカスタムロールが作成されます。

2. ロールにアプリケーションを割り当てます。

a. Azure ポータルで、 * Subscriptions * サービスを開きます。

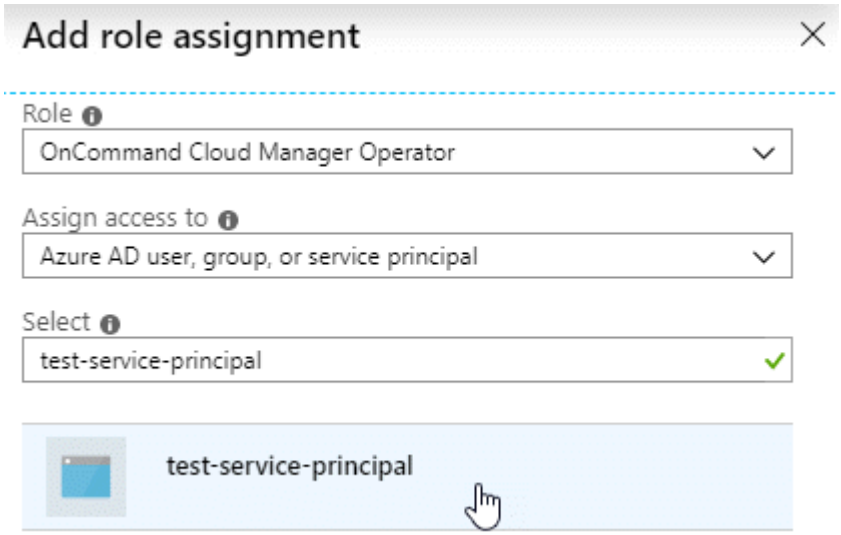
b. サブスクリプションを選択します。

c. [* アクセス制御 (IAM)] 、 [追加] 、 [役割の割り当ての追加 *] の順にクリックします。

d. OnCommand Cloud Manager Operator * ロールを選択します。

e. Azure AD のユーザ、グループ、サービスプリンシパル * は選択したままにします。

f. アプリケーションの名前を検索します（リストをスクロールして探すことはできません）。



g. アプリケーションを選択し、 * 保存 * をクリックします。

Cloud Manager のサービスプリンシパルに、そのサブスクリプションに必要な Azure の権限が付与されるようになりました。

Cloud Volumes ONTAP を複数の Azure サブスクリプションから導入する場合は、サービスプリンシパルを各サブスクリプションにバインドする必要があります。Cloud Manager では、 Cloud Volumes ONTAP の導入時に使用するサブスクリプションを選択できます。

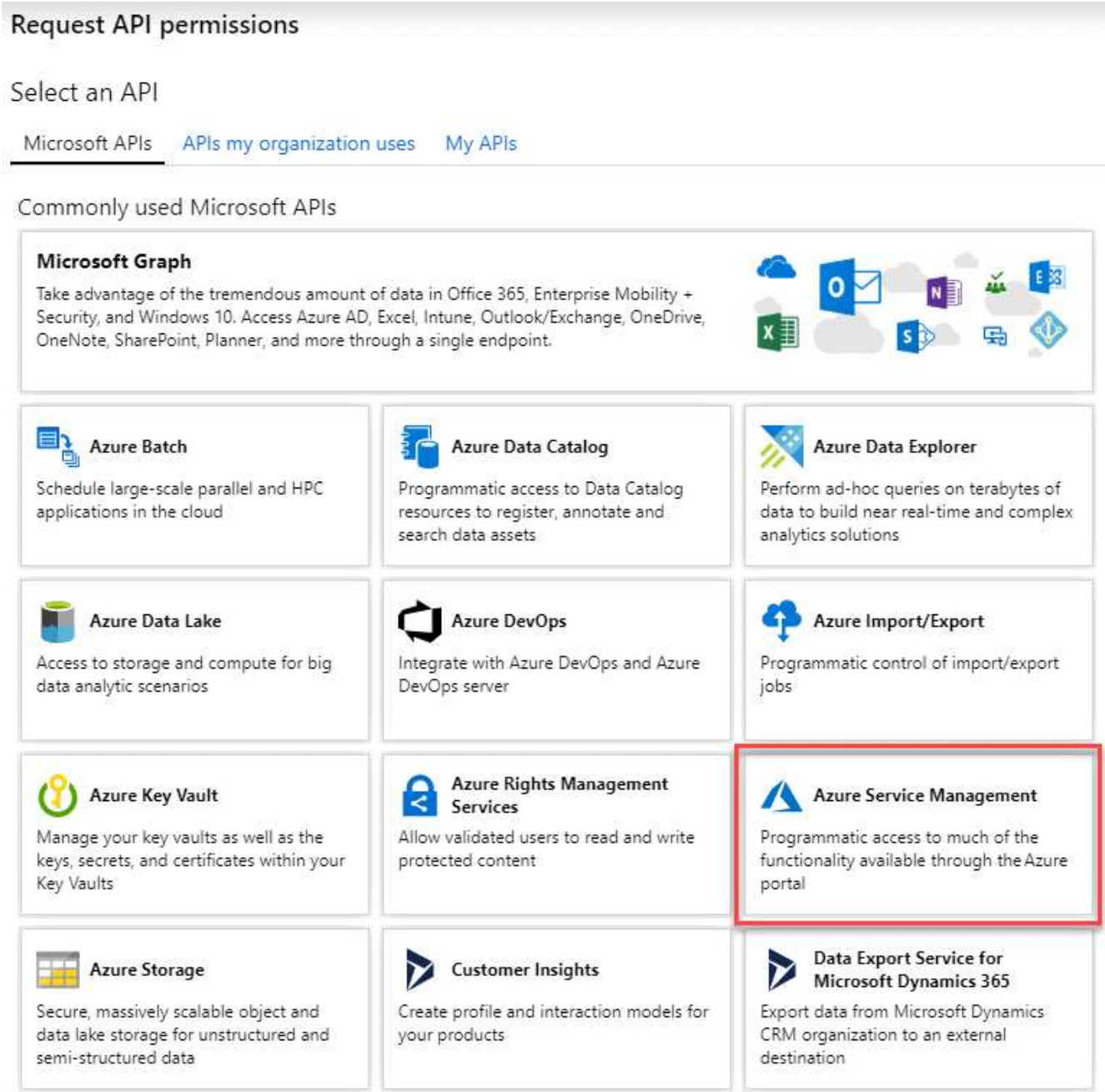
Windows Azure Service Management API 権限を追加しています

サービスプリンシパルに「 Windows Azure Service Management API 」の権限が必要です。

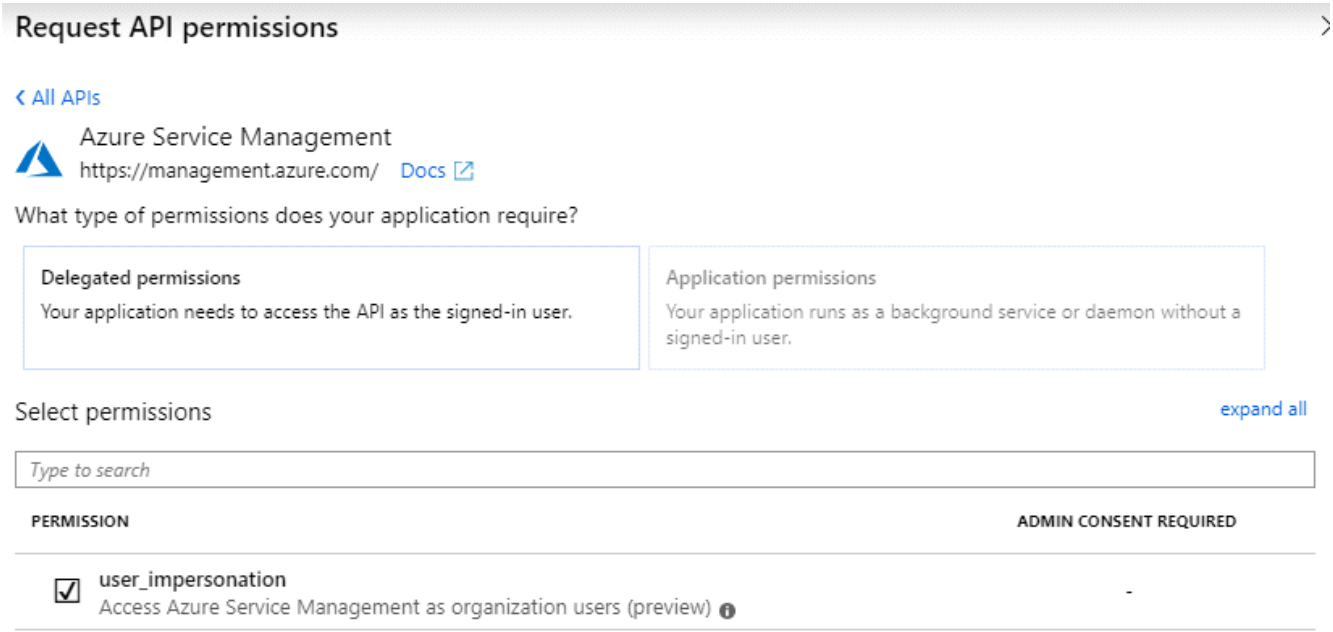
手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックしてアプリケーションを選択します。

2. [API アクセス許可] 、 [アクセス許可の追加] の順にクリックします。
3. Microsoft API* で、 * Azure Service Management * を選択します。



4. [* 組織ユーザーとして Azure サービス管理にアクセスする *] をクリックし、 [* 権限の追加 *] をクリックします。

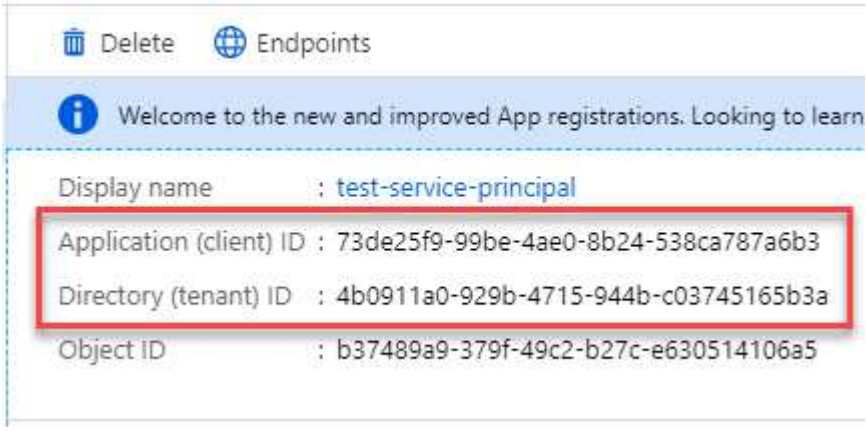


アプリケーション **ID** とディレクトリ **ID** を取得しています

Cloud Manager に Azure アカウントを追加するときは、アプリケーション（クライアント）の ID とディレクトリ（テナント） ID を指定する必要があります。Cloud Manager は、この ID を使用してプログラムによってサインインします。

手順

1. Azure Active Directory * サービスで、 * アプリ登録 * をクリックしてアプリケーションを選択します。
2. アプリケーション（クライアント） ID * とディレクトリ（テナント） ID * をコピーします。



クライアントシークレットの作成

Cloud Manager がクライアントシークレットを使用して Azure AD で認証できるようにするには、クライアントシークレットを作成し、そのシークレットの値を Cloud Manager に指定する必要があります。

> Cloud Manager にアカウントを追加すると、 Cloud Manager はクライアントシークレットをアプリケーションキーとして参照します。

手順

1. Azure Active Directory * サービスを開きます。
2. [* アプリ登録 *] をクリックして、アプリケーションを選択します。
3. ［ * 証明書とシークレット > 新しいクライアントシークレット * ］ をクリックします。
4. シークレットと期間の説明を入力します。
5. [追加（ Add ）] をクリックします。
6. クライアントシークレットの値をコピーします。

結果

これでサービスプリンシパルが設定され、アプリケーション（クライアント） ID 、ディレクトリ（テナント） ID 、およびクライアントシークレットの値をコピーしました。この情報は、 Cloud Manager で Azure アカウントを追加するときに入力する必要があります。

Cloud Manager への Azure アカウントの追加

必要な権限を持つ Azure アカウントを指定したら、そのアカウントを Cloud Manager に追加できます。これにより、そのアカウントで Cloud Volumes ONTAP システムを起動できます。

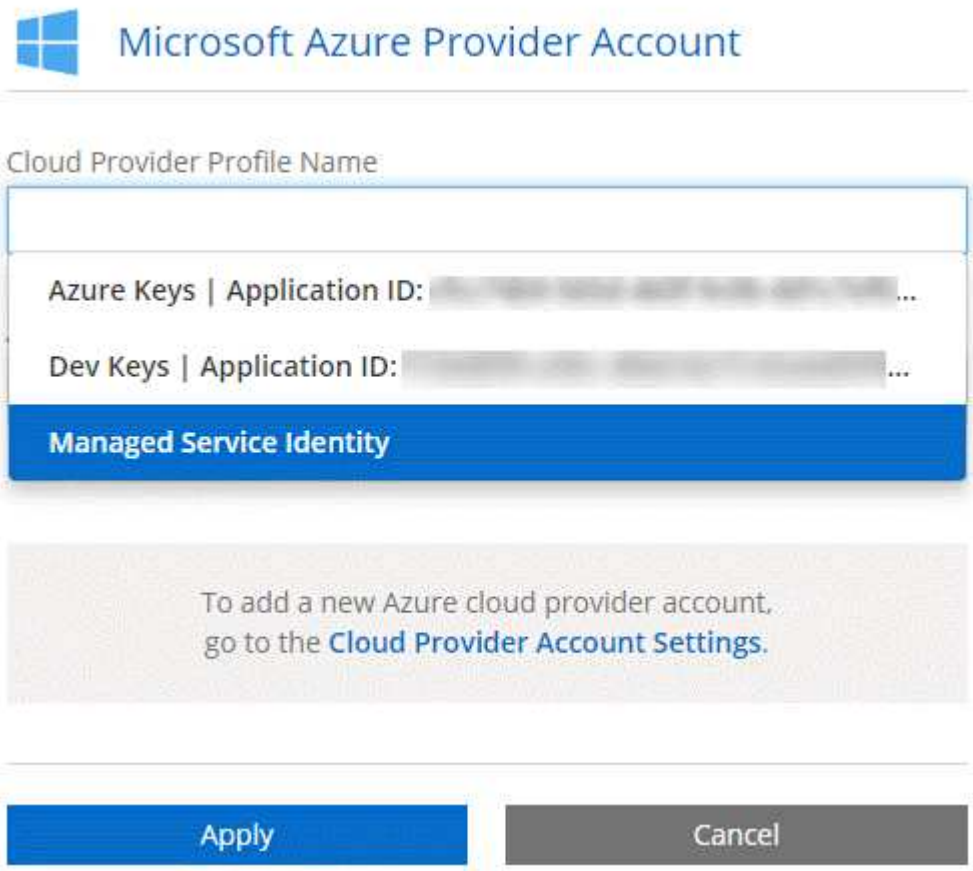
手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クラウドプロバイダとサポートアカウント * を選択します。

2. [新規アカウントの追加] をクリックし、 [Microsoft Azure] を選択します。
3. 必要な権限を付与する Azure Active Directory サービスプリンシパルに関する情報を入力します。
   - アプリケーション ID ：を参照してください アプリケーション ID とディレクトリ ID を取得しています。
   - テナント ID （またはディレクトリ ID ）：を参照してください アプリケーション ID とディレクトリ ID を取得しています。
   - Application Key （クライアントシークレット）：を参照してください [クライアントシークレットの作成]。
4. ポリシーの要件が満たされていることを確認し、 * アカウントの作成 * をクリックします。

結果

新しい作業環境を作成するときに、 [詳細と資格情報] ページから別のアカウントに切り替えることができるようになりました。



ページで [アカウントの切り替え] をクリックした後に、クラウドプロバイダアカウントを選択する方法を示すスクリーンショット。"]

追加の **Azure** サブスクリプションを管理対象 **ID** に関連付ける

Cloud Manager では、 Cloud Volumes ONTAP を導入する Azure アカウントとサブスクリプションを選択できます。管理対象に別の Azure サブスクリプションを選択することはできません を関連付けない限り、アイデンティティプロファイルを作成します "管理された ID" それらの登録と。

このタスクについて

管理対象 ID はです "最初の Azure アカウント" NetApp Cloud Central から Cloud Manager を導入する場合。Cloud Manager を導入すると、 Cloud Central は OnCommand Cloud Manager オペレータロールを作成し、 Cloud Manager 仮想マシンに割り当てました。

手順

1. Azure ポータルにログインします。
2. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP システムを展開するサブスクリプションを選択します。
3. 「 * アクセスコントロール（ IAM ） * 」をクリックします。
    a. [* 追加 **>** 役割の割り当ての追加 *] をクリックして、権限を追加します。

- OnCommand Cloud Manager Operator * ロールを選択します。

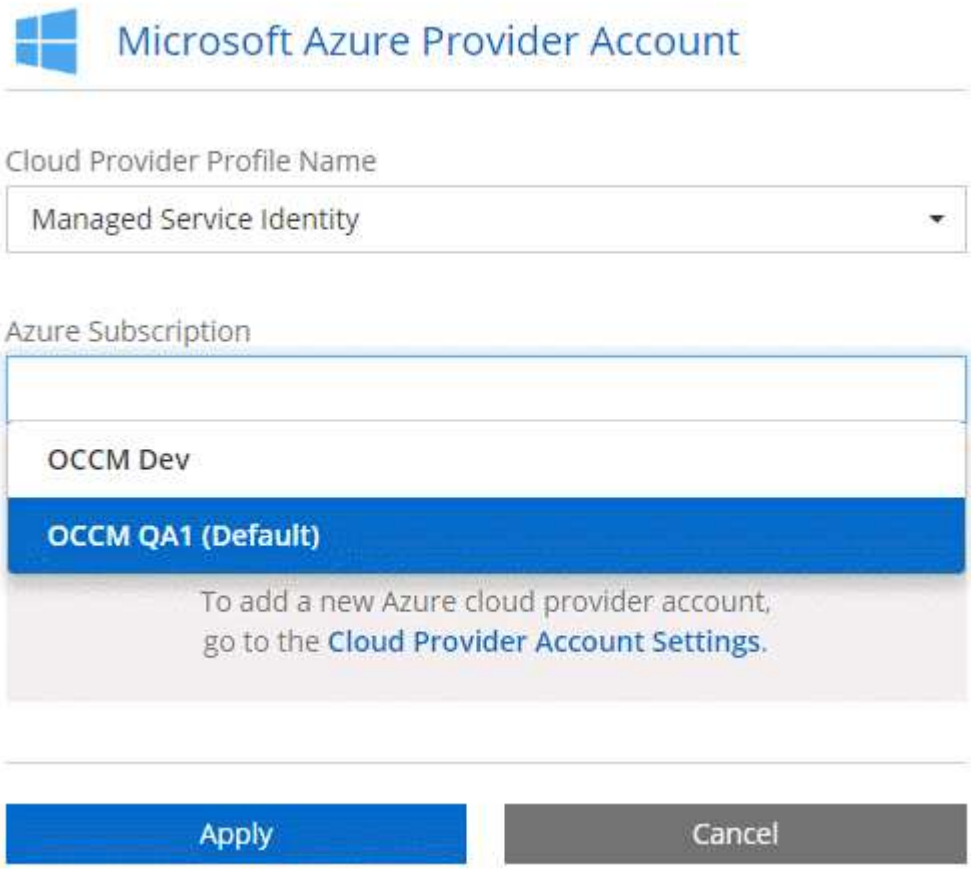
> OnCommand Cloud Manager Operator は、で指定されたデフォルトの名前です "Cloud Manager ポリシー"。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

- 仮想マシン * へのアクセスを割り当てます。
- Cloud Manager 仮想マシンが作成されたサブスクリプションを選択します。
- Cloud Manager 仮想マシンを選択します。
- [保存（ Save ）] をクリックします。

4. 追加のサブスクリプションについても、この手順を繰り返します。

結果

新しい作業環境を作成するときに、管理対象 ID プロファイルに対して複数の Azure サブスクリプションから選択できるようになりました。



GCP アカウントのセットアップと Cloud Manager への追加

有効にする項目 "データの階層化" Cloud Volumes ONTAP システムで、ストレージ管理者権限を持つサービスアカウントのストレージアクセスキーを Cloud Manager に提供する必要があります。Cloud Manager は、アクセスキーを使用して Cloud Storage バケッ

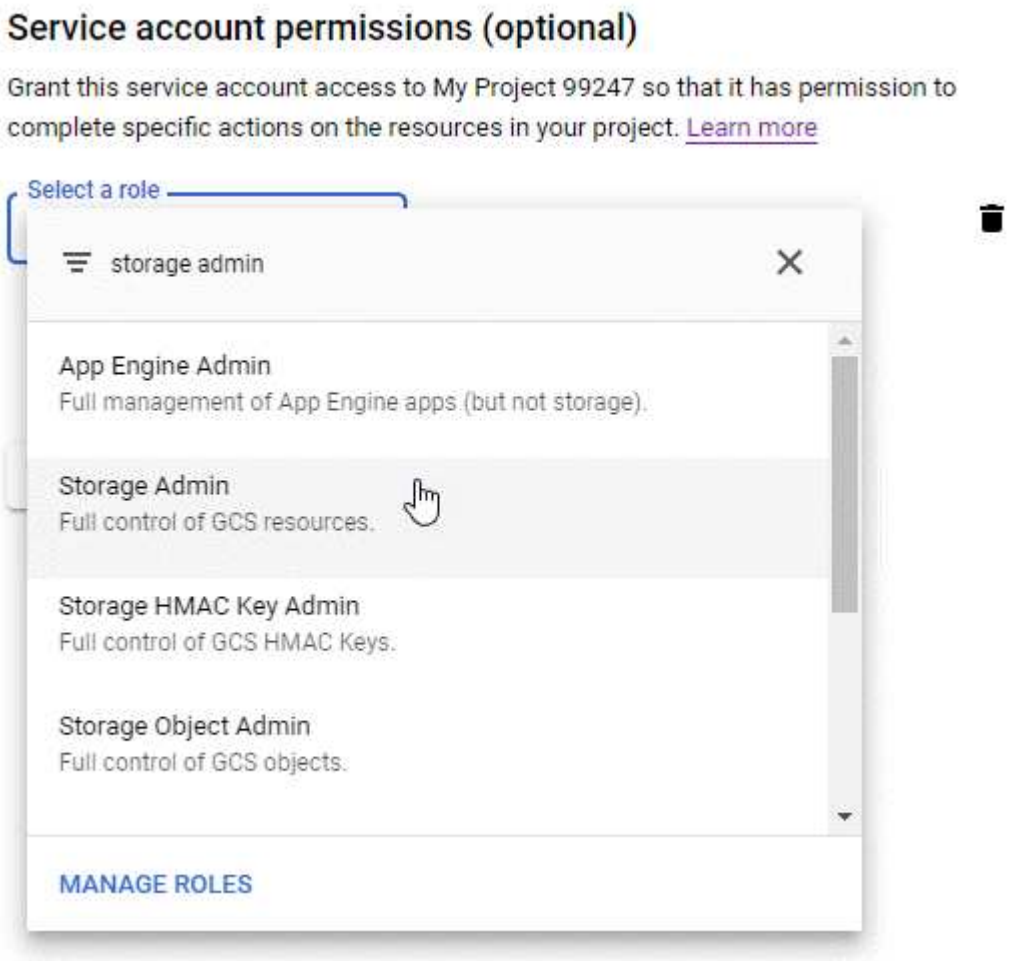
トをセットアップおよび管理し、データを階層化します。

Google のサービスアカウントとアクセスキーを設定する クラウドストレージ

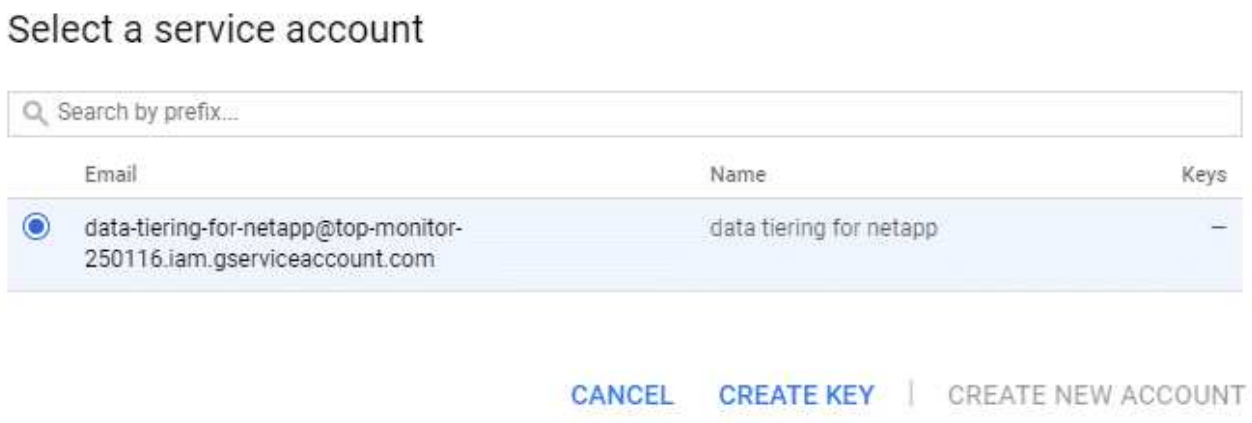
サービスアカウントを使用すると、 Cloud Manager でデータの階層化に使用する Cloud Storage バケットを認証してアクセスできます。キーは、 Google Cloud Storage がリクエストを発行しているユーザーを認識できるようにするために必要です。

手順

1. GCP IAM コンソールを開き、を開きます "Storage Admin ロールを持つサービスアカウントを作成します"。



2. に進みます "GCP Storage Settings （ GCP ストレージ設定）"。
3. プロンプトが表示されたら、プロジェクトを選択します。
4. [*Interoperability *] タブをクリックします。
5. まだ有効にしていない場合は、 * 相互運用アクセスを有効にする * をクリックします。
6. [サービスアカウントのアクセスキー *] で、 [サービスアカウントのキーの作成 *] をクリックします。
7. 手順 1 で作成したサービスアカウントを選択します。



8. [キーの作成 *] をクリックします。
9. アクセスキーとシークレットをコピーします。

   データ階層化用の GCP アカウントを追加する場合は、 Cloud Manager でこの情報を入力する必要があります。

Cloud Manager に **GCP** アカウントを追加する

サービスアカウントのアクセスキーが作成されたら、そのアクセスキーを Cloud Manager に追加できます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クラウドプロバイダとサポートアカウント * を選択します。

2. [Add New Account*] をクリックし、 [* GCP*] を選択します。
3. サービスアカウントのアクセスキーとシークレットを入力します。

   これらのキーを使用して、 Cloud Manager でデータ階層化用の Cloud Storage バケットを設定できます。

4. ポリシーの要件が満たされていることを確認し、 * アカウントの作成 * をクリックします。

次の手順

個々のボリュームを作成、変更、またはレプリケートするときに、それらのボリュームでデータ階層化を有効にできるようになりました。詳細については、を参照してください "使用頻度の低いデータを低コストのオブジェクトストレージに階層化"。

ただし、事前に、 Cloud Volumes ONTAP が存在するサブネットがプライベート Google アクセス用に構成されていることを確認してください。手順については、を参照してください "Google Cloud のドキュメント：「Configuring Private Google Access"。

Cloud Manager へのネットアップサポートサイトのアカウントの追加

BYOL システムを導入するには、 NetApp Support Site のアカウントを Cloud Manager に追加する必要があります。また、従量課金制システムの登録や ONTAP ソフトウェアのアップグレードも必要です。

次のビデオを視聴して、ネットアップサポートサイトのアカウントを Cloud Manager に追加する方法をご確認ください。または、下にスクロールして手順を確認します。

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

手順

1. ネットアップサポートサイトのアカウントがない場合は、 "1 名で登録します"。
2. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * クラウドプロバイダとサポートアカウント * を選択します。

3. [Add New Account*] をクリックし、 [* NetApp Support Site*] を選択します。
4. アカウントの名前を指定し、ユーザ名とパスワードを入力します。
   - お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。
   - BYOL システムを導入する場合は、次の点に注意してください。
     - BYOL システムのシリアル番号にアクセスする権限がアカウントに必要です。
     - セキュアな BYOL サブスクリプションを購入した場合は、セキュアな NSS アカウントが必要です。
5. [アカウントの作成] をクリックします。 *

次の手順

新しい Cloud Volumes ONTAP システムの作成時や既存のシステムの登録時に、ユーザがアカウントを選択できるようになりました。

- "AWS での Cloud Volumes ONTAP の起動"
- "Azure で Cloud Volumes ONTAP を起動します"
- "従量課金制システムの登録"
- "Cloud Manager によるライセンスファイルの管理方法について説明します"

セキュアアクセスのための HTTPS 証明書のインストール

デフォルトでは、 Cloud Manager は Web コンソールへの HTTPS アクセスに自己署名証明書を使用します。認証局（ CA ）によって署名された証明書をインストールできます。これにより、自己署名証明書よりも優れたセキュリティ保護が提供されます。

手順

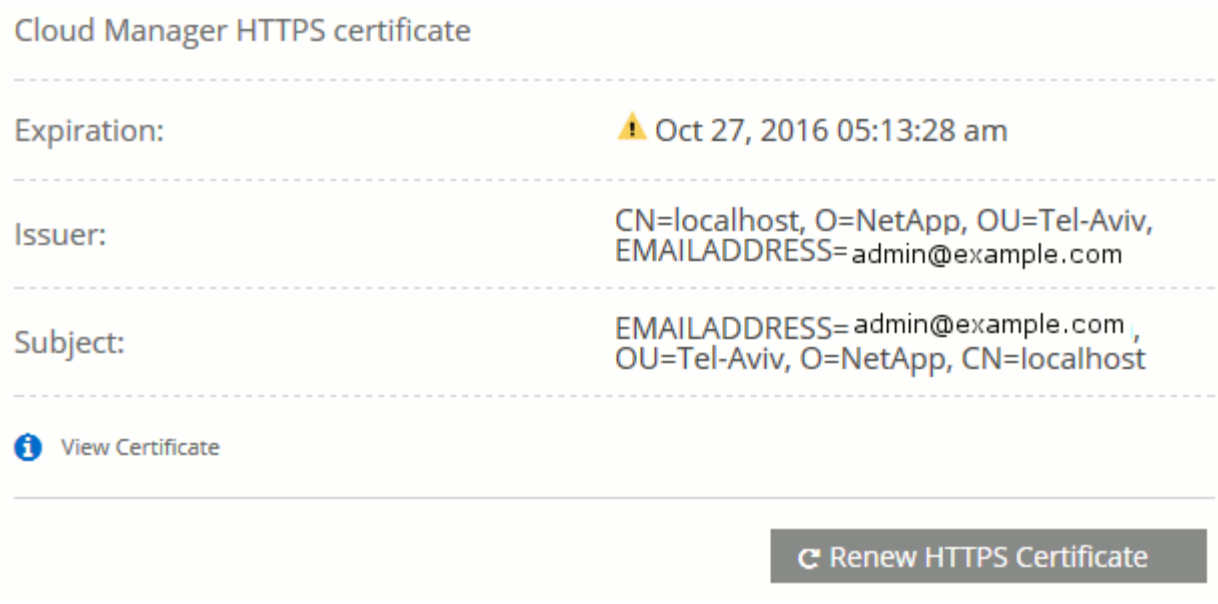
1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * HTTPS セットアップ * を選択します。

2. [HTTPS Setup] ページで、証明書署名要求（ CSR ）を生成するか、独自の CA 署名付き証明書をインストールして、証明書をインストールします。

オプション	説明
CSR を生成します	a. Cloud Manager ホストのホスト名または DNS （共通名）を入力し、 * CSR の生成 * をクリックします。 証明書署名要求が表示されます。 b. CSR を使用して、 SSL 証明書要求を CA に送信します。 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。 c. 署名済み証明書の内容をコピーし、 [証明書] フィールドに貼り付けて、 [**Install**] をクリックします。
独自の CA 署名付き証明書をインストールします	a. 「 CA 署名証明書のインストール」を選択します。 b. 証明書ファイルと秘密鍵の両方をロードし、 * Install * をクリックします。 証明書では、 Privacy Enhanced Mail （ PEM ） Base-64 エンコード X.509 形式を使用する必要があります。

結果

Cloud Manager は、 CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供するようになりました。次の図は、セキュアアクセス用に設定された Cloud Manager システムを示しています。



AWS KMS のセットアップ

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、 AWS Key Management Service （ KMS ）を設定する必要があります。

手順

1. アクティブな Customer Master Key （ CMK ）が存在することを確認します。

   CMK は、 AWS 管理の CMK または顧客管理の CMK にすることができます。Cloud Manager および Cloud Volumes ONTAP と同じ AWS アカウントにすることも、別の AWS アカウントにすることもできます。

   "AWS ドキュメント：「 Customer Master Keys （ CMK ；カスタマーマスターキー）」"

2. 各 CMK のキーポリシーを変更します。変更するには、 Cloud Manager に a_key user_権限 を付与する IAM ロールを追加します。

   IAM ロールをキーユーザとして追加すると、 Cloud Volumes ONTAP で CMK を使用する権限が Cloud Manager に付与されます。

   "AWS のドキュメント：「キーの編集"

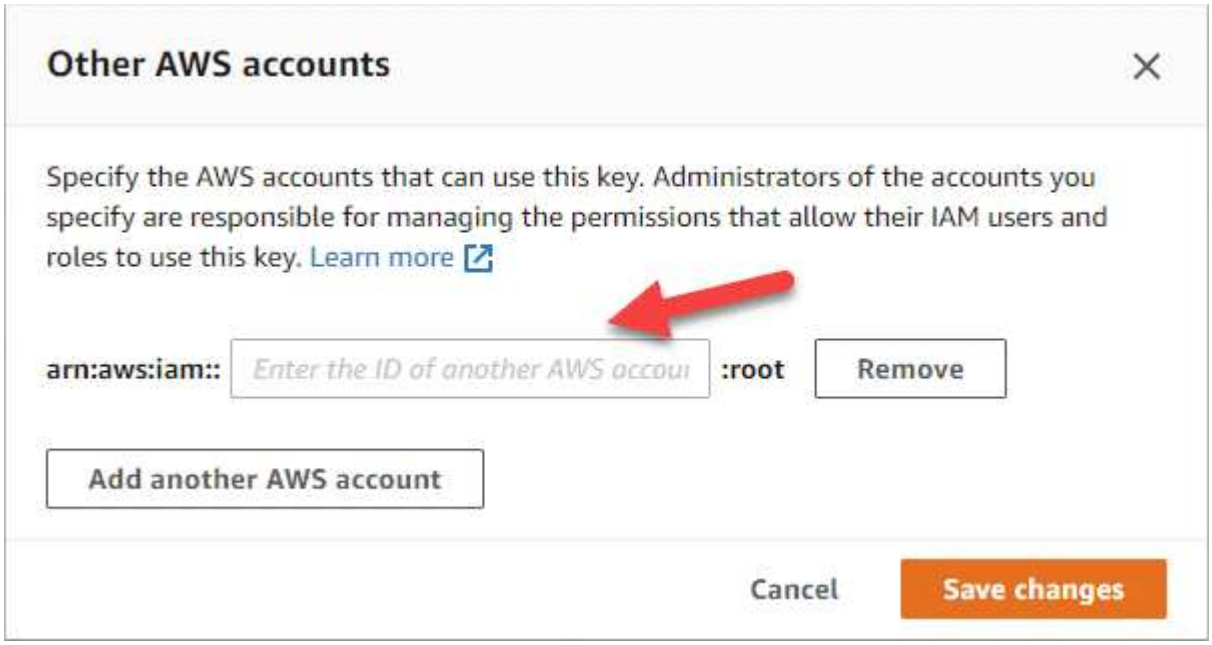
3. CMK が別の AWS アカウントにある場合は、次の手順を実行します。

   a. CMK が存在するアカウントから KMS コンソールにアクセスします。
   b. キーを選択します。
   c. General configuration * ペインで、キーの ARN をコピーします。

      Cloud Volumes ONTAP システムの作成時には、 Cloud Manager の ARN の指定が必要になります。

   d. その他の AWS アカウント * ペインで、 Cloud Manager に権限を付与する AWS アカウントを追加します。

ほとんどの場合、 Cloud Manager が配置されているアカウントです。Cloud Manager が AWS にインストールされていない場合、 Cloud Manager に AWS アクセスキーを指定したアカウントになります。



e. 次に、 Cloud Manager に権限を付与する AWS アカウントに切り替えて、 IAM コンソールを開きます。

f. 以下の権限を含む IAM ポリシーを作成します。

g. Cloud Manager に権限を付与する IAM ロールまたは IAM ユーザにポリシーを関連付けます。

   次のポリシーは、 Cloud Manager が外部 AWS アカウントから CMK を使用するために必要な権限を提供します。「リソース」セクションで、リージョンとアカウント ID を必ず変更してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
このプロセスの詳細については、を参照してください "AWS ドキュメント：「外部 AWS アカウントによる CMK へのアクセスの許可"。

ネットワーク要件

Cloud Manager のネットワーク要件

Cloud Manager が AWS 、 Microsoft Azure 、または Google Cloud Platform に Cloud Volumes ONTAP システムを導入できるように、ネットワークをセットアップします。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。

> ネットワークでインターネットへのすべての通信にプロキシサーバが使用されている場合、Cloud Manager はセットアップ時にプロキシを指定するように要求します。[設定] ページからプロキシサーバを指定することもできます。を参照してください "プロキシサーバを使用するように Cloud Manager を設定しています"。

ターゲットネットワークへの接続

Cloud Manager では、 Cloud Volumes ONTAP を導入する VPC および VNet へのネットワーク接続が必要です。

たとえば、企業ネットワークに Cloud Manager をインストールした場合は、 Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

アウトバウンドインターネットアクセス

Cloud Manager で Cloud Volumes ONTAP を導入および管理するには、アウトバウンドインターネットアクセスが必要です。また、 Web ブラウザから Cloud Manager にアクセスする場合や、 Linux ホストで Cloud Manager インストーラを実行する場合にも、アウトバウンドインターネットアクセスが必要です。

次のセクションでは、特定のエンドポイントについて説明します。

AWS で Cloud Volumes ONTAP を管理するエンドポイント

Cloud Manager で Cloud Volumes ONTAP を AWS に導入して管理する場合、次のエンドポイントに接続するには、アウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
AWS サービス（ amazonaws.com ）： • クラウド形成 • 柔軟なコンピューティングクラウド（ EC2 ） • キー管理サービス（ KMS ） • セキュリティトークンサービス（ STS ） • シンプルなストレージサービス（ S3 ） 正確なエンドポイントは、 Cloud Volumes ONTAP を導入する地域によって異なります。 "詳細については、 AWS のマニュアルを参照してください。"	Cloud Manager で Cloud Volumes ONTAP を AWS に導入して管理できるようにします。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com	Cloud Manager は、マニフェスト、テンプレート、 Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
\ https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	S3 へのバックアップを許可するユーザのリストに AWS アカウント ID を追加します。
¥ https://support.netapp.com/aods/asupmessage ¥ https://support.netapp.com/asupprod/post/1.0/postAsup	ネットアップ AutoSupport との通信：
https://support.netapp.com/svcmw https://support.netapp.com/servicegw/Entitlement	システムライセンスとサポート登録を行うためのネットアップとの通信
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。
¥ https://packages.cloud.google.com/yum ¥ https://github.com/NetApp/trident/releases/download/	Cloud Volumes ONTAP システムを Kubernetes クラスタに接続するために必要です。エンドポイントを使用して NetApp Trident をインストールできます。

エンドポイント	目的
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • https://repo.typafe.org にアクセスします サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

Azure で Cloud Volumes ONTAP を管理するエンドポイント

Microsoft Azure で Cloud Volumes ONTAP を導入および管理する場合、 Cloud Manager では、次のエンドポイントに接続するためにアウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com	Cloud Manager では、ほとんどの Azure リージョンに Cloud Volumes ONTAP を導入して管理できます。
https://management.microSoftazure.de https://login.microsoftonline.de	Cloud Manager は、 Azure Germany リージョンに Cloud Volumes ONTAP を導入して管理できます。
https://management.usgovcloudapi.net/ https://login.microsoftonline.com	Cloud Manager は、 Azure US GOV リージョンに Cloud Volumes ONTAP を導入して管理できます。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com	Cloud Manager は、マニフェスト、テンプレート、 Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
https://mysupport.netapp.com をご覧ください	ネットアップ AutoSupport との通信：
https://support.netapp.com/svcmw https://support.netapp.com/servicegw/Entitlement	システムライセンスとサポート登録を行うためのネットアップとの通信
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。

エンドポイント	目的
¥ https://packages.cloud.google.com/yum ¥ https://github.com/NetApp/trident/releases/download/	Cloud Volumes ONTAP システムを Kubernetes クラスタに接続するために必要です。エンドポイントを使用して NetApp Trident をインストールできます。
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • https://repo.typafe.org にアクセスします サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

GCP で Cloud Volumes ONTAP を管理するためのエンドポイント

Cloud Manager で Cloud Volumes ONTAP を GCP に導入して管理する場合、次のエンドポイントに接続するには、アウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
\ https://www.googleapis.com	Cloud Manager から Google API に連絡して GCP で Cloud Volumes ONTAP の導入と管理を行うことができます。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com	Cloud Manager は、マニフェスト、テンプレート、 Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
https://mysupport.netapp.com をご覧ください	ネットアップ AutoSupport との通信：
https://support.netapp.com/svcmw https://support.netapp.com/servicegw/Entitlement	システムライセンスとサポート登録を行うためのネットアップとの通信
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。

エンドポイント	目的
¥ https://packages.cloud.google.com/yum ¥ https://github.com/NetApp/trident/releases/download/	Cloud Volumes ONTAP システムを Kubernetes クラスタに接続するために必要です。エンドポイントを使用して NetApp Trident をインストールできます。
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • https://repo.typafe.org にアクセスします サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

Web ブラウザからアクセスするエンドポイント

ユーザは Web ブラウザから Cloud Manager にアクセスする必要があります。Web ブラウザを実行するマシンは、次のエンドポイントに接続する必要があります。

エンドポイント	目的
Cloud Manager ホスト	Cloud Manager コンソールをロードするには、 Web ブラウザでホストの IP アドレスを入力する必要があります。 クラウドプロバイダへの接続に応じて、ホストに割り当てられたプライベート IP またはパブリック IP を使用できます。 • プライベート IP は、 VPN とがある場合に機能します 仮想ネットワークへの直接アクセス • パブリック IP は、あらゆるネットワークシナリオで機能します いずれの場合も、セキュリティグループのルールで許可された IP またはサブネットからのアクセスのみを許可することで、ネットワークアクセスを保護する必要があります。
¥ https://auth0.com ¥ https://cdn.auth0.com ¥ https://netapp-cloud-account.auth0.com ¥ https://services.cloud.netapp.com	Web ブラウザはこれらのエンドポイントに接続し、 NetApp Cloud Central を介してユーザ認証を一元化します。
\ https://widget.intercom.io	製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。

Linux ホストに **Cloud Manager** をインストールするエンドポイント

Cloud Manager インストーラは、インストールプロセス中に次の URL にアクセスする必要があります。

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm

- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

ポートおよびセキュリティグループ

- Cloud Central または Marketplace イメージから Cloud Manager を導入する場合は、次を参照してください。
  - "AWS の Cloud Manager のセキュリティグループルール"
  - "Azure の Cloud Manager のセキュリティグループルール"
  - "GCP の Cloud Manager のファイアウォールルール"
- 既存の Linux ホストに Cloud Manager をインストールする場合は、を参照してください "Cloud Manager ホストの要件"。

Cloud Volumes ONTAP in AWS のネットワーク要件

Cloud Volumes ONTAP システムが適切に動作するように AWS ネットワークをセットアップします。

Cloud Volumes ONTAP の一般的な AWS ネットワーク要件

AWS では、次の要件を満たす必要があります。

Cloud Volumes ONTAP ノードのアウトバウンドインターネットアクセス

Cloud Volumes ONTAP ノードでは、ネットアップ AutoSupport にメッセージを送信するために、アウトバウンドインターネットアクセスが必要です。ネットアップ AutoSupport は、ストレージの健全性をプロアクティブに監視します。

Cloud Volumes ONTAP から AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの AWS HTTP/HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

NAT インスタンスがある場合は、プライベートサブネットからインターネットへの HTTPS トラフィックを許可する着信セキュリティグループルールを定義する必要があります。

HA メディエータのアウトバウンドインターネットアクセス

HA メディエータインスタンスは、 AWS EC2 サービスへのアウトバウンド接続を持っている必要があります。これにより、ストレージのフェイルオーバーを支援できます。接続を提供するには、パブリック IP アドレスを追加するか、プロキシサーバを指定するか、または手動オプションを使用します。

手動オプションには、 NAT ゲートウェイまたはターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを指定できます。VPC エンドポイントの詳細については、を参照してください "AWS ドキュメント：「 Interface VPC Endpoints 」（ AWS PrivateLink ）"。

IP アドレスの数

Cloud Manager から Cloud Volumes ONTAP に次の数の IP アドレスが AWS で割り当てられます。

- シングルノード： IP アドレス × 6
- 単一の AZ にまたがる HA ペア： 15 個のアドレス
- 複数の AZ にまたがる HA ペア： 15 または 16 個の IP アドレス

  Cloud Manager は、単一のノードシステム上に SVM 管理 LIF を作成しますが、単一の AZ 内の HA ペア上には作成しません。複数の AZ にまたがる HA ペア上に SVM 管理 LIF を作成するかどうかを選択できます。

> LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

セキュリティグループ

Cloud Manager ではセキュリティグループを作成する必要がないため、セキュリティグループを作成する必要はありません。自分で使用する必要がある場合は、を参照してください "セキュリティグループのルール"。

Cloud Volumes ONTAP から **AWS S3** への接続によるデータ階層化

EBS をパフォーマンス階層として使用し、 AWS S3 を容量階層として使用する場合は、 Cloud Volumes ONTAP が S3 に接続されていることを確認する必要があります。この接続を提供する最善の方法は、 S3 サービスへの vPC エンドポイントを作成することです。手順については、を参照してください "AWS のドキュメント：「 Creating a Gateway Endpoint"。

vPC エンドポイントを作成するときは、 Cloud Volumes ONTAP インスタンスに対応するリージョン、 vPC 、およびルートテーブルを必ず選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、 Cloud Volumes ONTAP は S3 サービスに接続できません。

問題が発生した場合は、を参照してください "AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"

他のネットワーク内の **ONTAP** システムへの接続

AWS の Cloud Volumes ONTAP システムと他のネットワークの ONTAP システムの間でデータをレプリケートするには、 AWS VPC と他のネットワーク（ Azure VNet や企業ネットワークなど）の間に VPN 接続が必要です。手順については、を参照してください "AWS ドキュメント：「 Setting Up an AWS VPN Connection"。

CIFS 用の **DNS** と **Active Directory**

CIFS ストレージをプロビジョニングする場合は、 AWS で DNS と Active Directory をセットアップするか、オンプレミスセットアップを AWS に拡張する必要があります。

DNS サーバは、 Active Directory 環境に名前解決サービスを提供する必要があります。デフォルトの EC2 DNS サーバを使用するように DHCP オプションセットを設定できます。このサーバは、 Active Directory 環境で使用される DNS サーバであってはなりません。

手順については、を参照してください "AWS ドキュメント：「 Active Directory Domain Services on the AWS Cloud ： Quick Start Reference Deployment"。

複数の **AZS** での **Cloud Volumes ONTAP HA** の **AWS** ネットワーク要件

複数の可用性ゾーン（ AZS ）を使用する Cloud Volumes ONTAP HA 構成には、 AWS ネットワークの追加要件が適用されます。HA ペアを起動する前に、これらの要件を確認する必要があります。これは、 Cloud Manager でネットワークの詳細を入力する必要があるためです。

HA ペアの仕組みについては、を参照してください "ハイアベイラビリティペア"。

可用性ゾーン

この HA 導入モデルでは、複数の AZS を使用してデータの高可用性を確保します。各 Cloud Volumes ONTAP インスタンスと、 HA ペア間の通信チャネルを提供するメディエータインスタンスには、専用の AZ を使用する必要があります。

NAS データおよびクラスタ **/ SVM** 管理用のフローティング **IP** アドレス

複数の AZ に展開された HA configurations では、障害が発生した場合にノード間で移行するフローティング IP アドレスを使用します。VPC の外部からネイティブにアクセスすることはできません。ただし、その場合は除きます "AWS 転送ゲートウェイを設定します"。

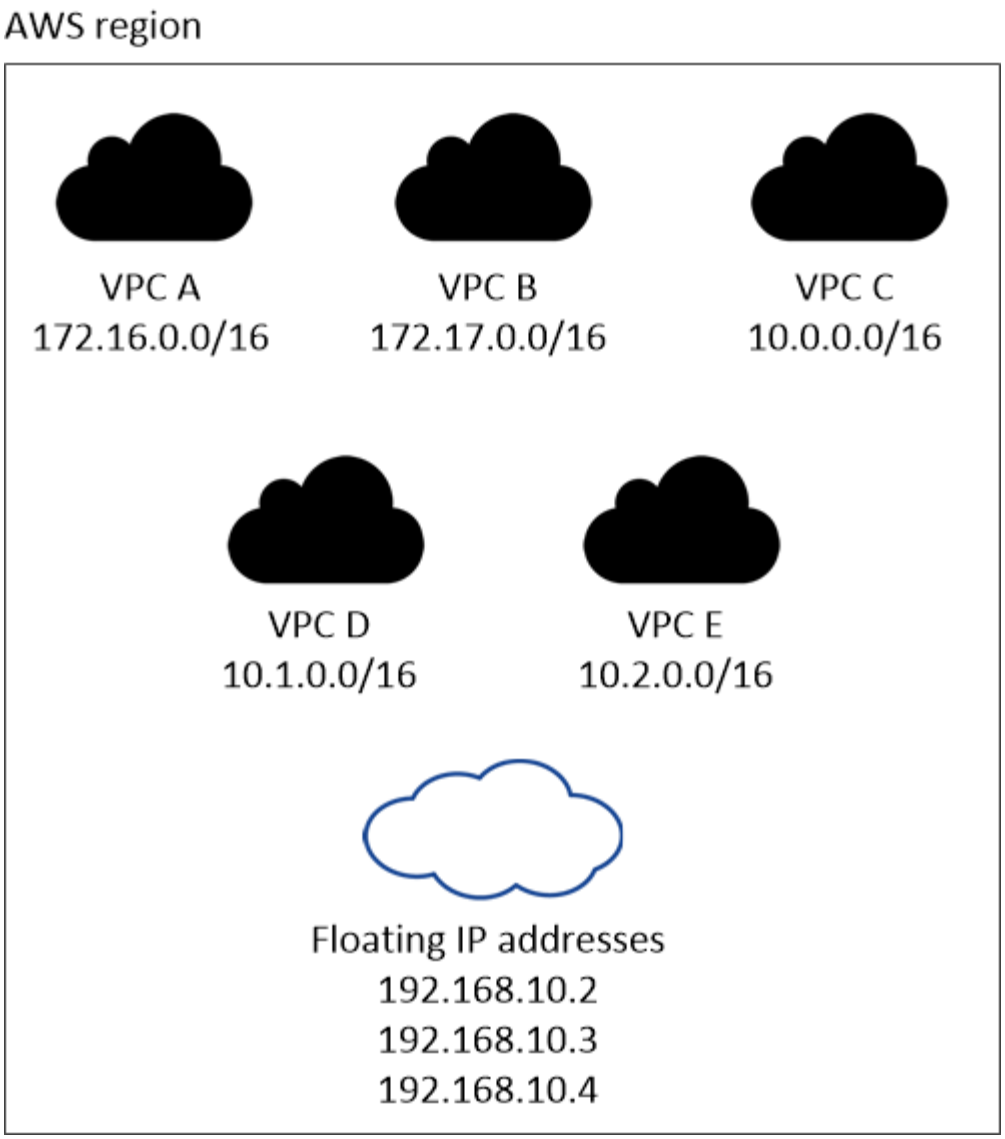
フローティング IP アドレスの 1 つはクラスタ管理用、 1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。SVM 管理用の 4 つ目のフローティング IP アドレスはオプションです。

> SnapCenter for Windows または SnapDrive を HA ペアで使用する場合は、 SVM 管理 LIF 用にフローティング IP アドレスが必要です。システムの導入時に IP アドレスを指定しなかった場合は、あとで LIF を作成できます。詳細については、を参照してください "Cloud Volumes ONTAP のセットアップ"。

Cloud Volumes ONTAP HA 作業環境を作成するときに、 Cloud Manager でフローティング IP アドレスを入力する必要があります。Cloud Manager は、システムの起動時に IP アドレスを HA ペアに割り当てます。

フローティング IP アドレスは、 HA 構成を導入する AWS リージョン内のどの VPC の CIDR ブロックにも属していない必要があります。フローティング IP アドレスは、リージョン内の VPC の外部にある論理サブネットと考えてください。

次の例は、 AWS リージョンのフローティング IP アドレスと VPC の関係を示しています。フローティング IP アドレスはどの VPC の CIDR ブロックにも属しておらず、ルーティングテーブルを介してサブネットにルーティングできます。



Cloud Manager は、 iSCSI アクセス用と、 VPC 外のクライアントからの NAS アクセス用に、自動的に静的 IP アドレスを作成します。これらの種類の IP アドレスの要件を満たす必要はありません。

外部からのフローティング **IP** アクセスを可能にする中継ゲートウェイ **VPC**

"AWS 転送ゲートウェイを設定します" HA ペアが配置されている VPC の外部から HA ペアのフローティング IP アドレスにアクセスできるようにします。

ルートテーブル

Cloud Manager でフローティング IP アドレスを指定したあと、それらのフローティング IP アドレスへのルートを含むルーティングテーブルを選択する必要があります。これにより、 HA ペアへのクライアントアクセスが可能になります。

vPC （メインルートテーブル）内のサブネットのルートテーブルが 1 つだけの場合、 Cloud Manager はそのルートテーブルにフローティング IP アドレスを自動的に追加します。ルーティングテーブルが複数ある場合は、 HA ペアの起動時に正しいルーティングテーブルを選択することが非常に重要です。そうしないと、一部のクライアントが Cloud Volumes ONTAP にアクセスできない場合があります。

たとえば、異なるルートテーブルに関連付けられた 2 つのサブネットがあるとします。ルーティングテー

ブル A を選択し、ルーティングテーブル B は選択しなかった場合、ルーティングテーブル A に関連付けられたサブネット内のクライアントは HA ペアにアクセスできますが、ルーティングテーブル B に関連付けられたサブネット内のクライアントはアクセスできません。

ルーティングテーブルの詳細については、を参照してください "AWS のドキュメント：「 Route Tables"。

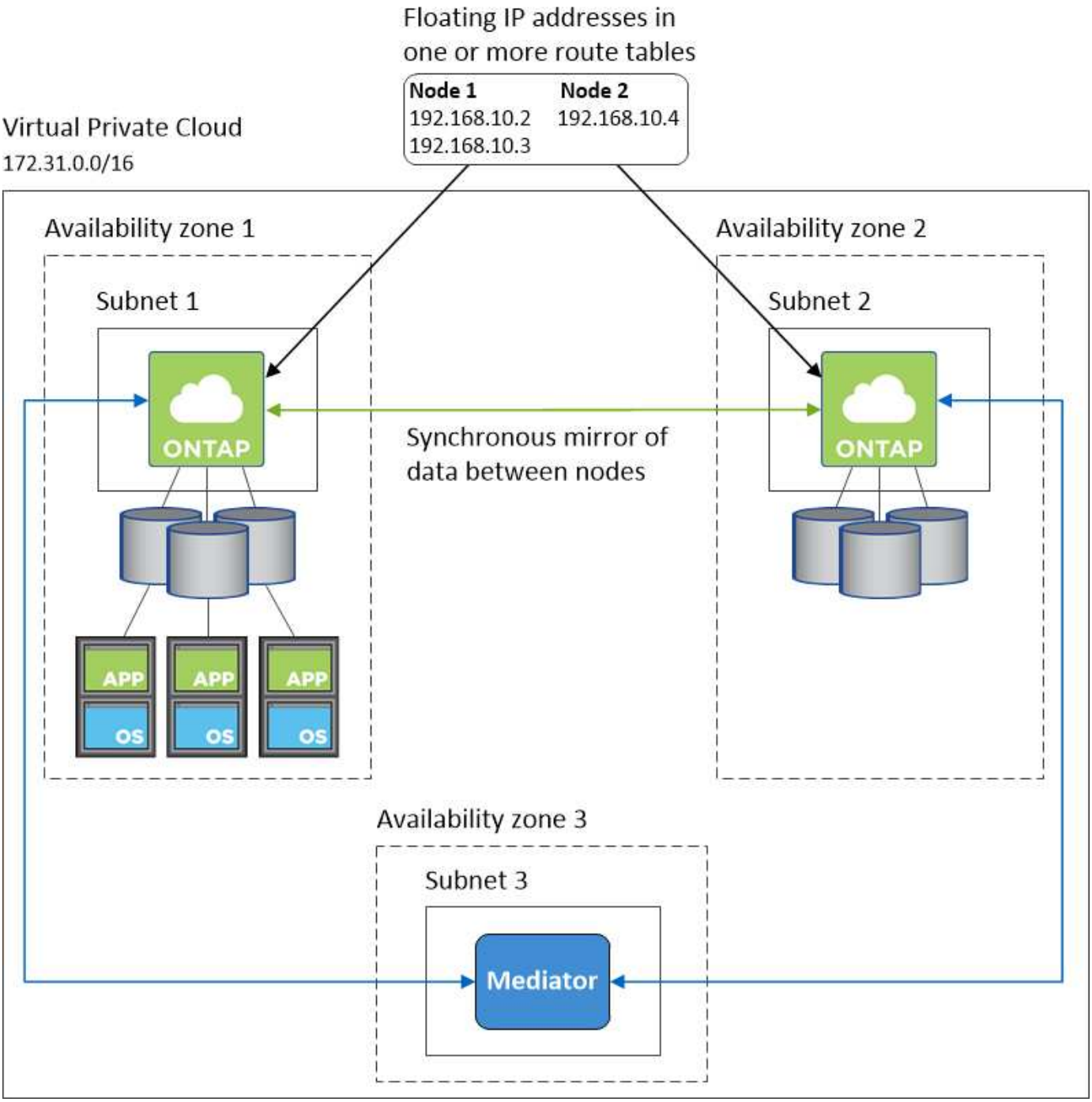
ネットアップの管理ツールとの連携

複数の AZ に展開された HA 構成でネットアップ管理ツールを使用するには、次の 2 つの接続オプションがあります。

1. ネットアップの管理ツールは、別の VPC とに導入できます "AWS 転送ゲートウェイを設定します"。ゲートウェイを使用すると、 VPC の外部からクラスタ管理インターフェイスのフローティング IP アドレスにアクセスできます。
2. NAS クライアントと同様のルーティング設定を使用して、同じ VPC にネットアップ管理ツールを導入できます。

設定例

次の図は、アクティブ / パッシブ構成として動作する AWS の最適な HA 構成を示しています。



vPC 設定の例

Cloud Manager と Cloud Volumes ONTAP を AWS に導入する方法を理解するには、最も一般的な VPC 構成を確認する必要があります。

- パブリックサブネットとプライベートサブネット、および NAT デバイスを備えた vPC
- プライベートサブネットとネットワークへの VPN 接続を備えた vPC

パブリックサブネットとプライベートサブネット、および **NAT** デバイスを備えた **vPC**

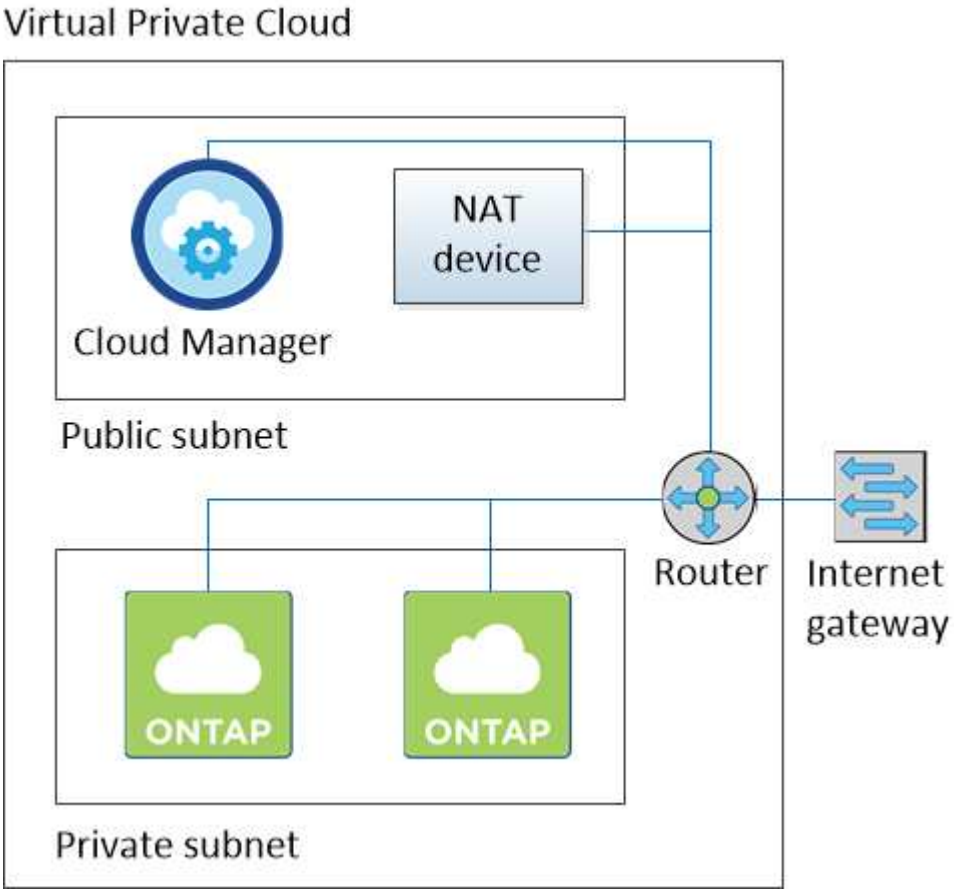
この vPC 設定には、パブリックサブネットとプライベートサブネット、 vPC をインターネットに接続するインターネットゲートウェイ、プライベートサブネットからのアウトバウンドインターネットトラフィックを有

効にするパブリックサブネット内の NAT ゲートウェイまたは NAT インスタンスが含まれます。この設定では、パブリックサブネットまたはプライベートサブネットで Cloud Manager を実行できますが、パブリックサブネットは、 vPC 外部のホストからのアクセスを許可するため、推奨されます。その後、プライベートサブネットで Cloud Volumes ONTAP インスタンスを起動できます。

NAT デバイスの代わりに、 HTTP プロキシを使用してインターネット接続を提供できます。

このシナリオの詳細については、を参照してください "AWS ドキュメント：シナリオ 2 ：「 VPC with Public and Private Subnets （ NAT ）」"。

次の図は、プライベートサブネットで実行されているパブリックサブネットおよびシングルノードシステムで実行されている Cloud Manager を示しています。



プライベートサブネットとネットワークへの **VPN** 接続を備えた **vPC**

この VPC 構成はハイブリッドクラウド構成で、 Cloud Volumes ONTAP はプライベート環境の拡張機能となります。この設定には、プライベートサブネットと、 VPN 接続を使用してネットワークに接続された仮想プライベートゲートウェイが含まれます。VPN トンネルを介したルーティングにより、 EC2 インスタンスはネットワークとファイアウォールを介してインターネットにアクセスできます。Cloud Manager は、プライベートサブネットまたはデータセンターで実行できます。次に、プライベートサブネットで Cloud Volumes ONTAP を起動します。

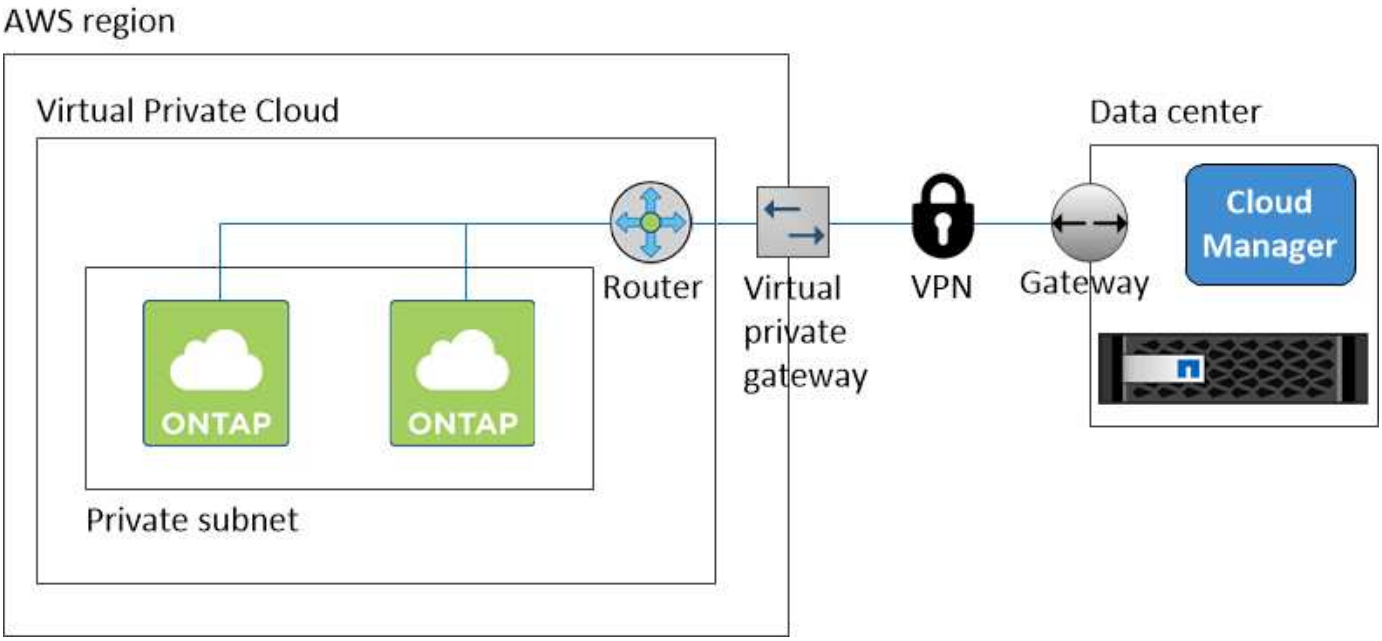
また、この構成でプロキシサーバを使用して、インターネットアクセスを許可することもできます。プロキシサーバは、データセンターまたは AWS に配置できます。

データセンター内の FAS システムと AWS 内の Cloud Volumes ONTAP システムの間でデータをレプリケー

トする場合は、リンクをセキュアにするために VPN 接続を使用する必要があります。

このシナリオの詳細については、を参照してください "AWS ドキュメント：シナリオ 4 ：プライベートサブネットのみと AWS Managed VPN Access を使用した VPC"。

次の図は、データセンターで実行されている Cloud Manager と、プライベートサブネットで実行されているシングルノードシステムを示しています。



での **HA** ペアの **AWS** 転送ゲートウェイのセットアップ 複数の **AZ**

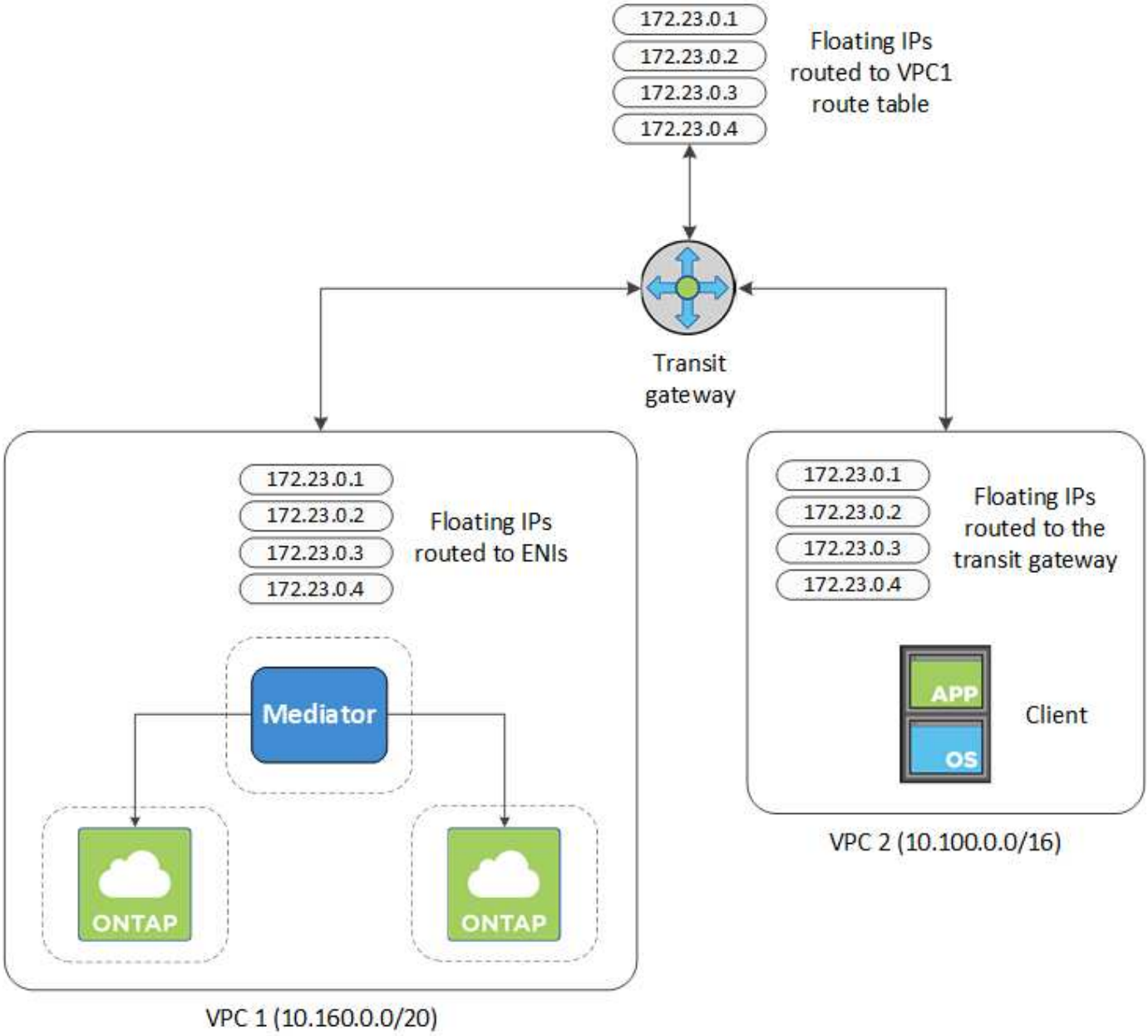
HA ペアが配置されている VPC の外部から HA ペアのフローティング IP アドレスにアクセスできるように、 AWS トランジットゲートウェイを設定します。

Cloud Volumes ONTAP HA 構成が複数の AWS アベイラビリティゾーンに分散されている場合は、 VPC 内からの NAS データアクセス用にフローティング IP アドレスが必要です。これらのフローティング IP アドレスは、障害の発生時にノード間で移行できますが、 VPC の外部からネイティブにアクセスすることはできません。VPC の外部からのデータアクセスはプライベート IP アドレスで提供されますが、自動フェイルオーバーは提供されません。

クラスタ管理インターフェイスとオプションの SVM 管理 LIF にもフローティング IP アドレスが必要です。

AWS 転送ゲートウェイを設定すると、 HA ペアが配置された VPC の外部からフローティング IP アドレスにアクセスできるようになります。つまり、 VPC の外部にある NAS クライアントとネットアップの管理ツールからフローティング IP にアクセスできます。

以下に、トランジットゲートウェイによって接続された 2 つの VPC の例を示します。HA システムは 1 つの VPC に存在し、クライアントはもう一方の VPC に存在します。その後、フローティング IP アドレスを使用して NAS ボリュームをクライアントにマウントできます。



以下に、同様の構成を設定する手順を示します。

手順

1. "トランジットゲートウェイを作成し、 VPC をに接続します ゲートウェイ"。
2. HA ペアのフローティング IP アドレスを指定して、転送ゲートウェイのルートテーブルにルートを作成します。

   フローティング IP アドレスは、 Cloud Manager の Working Environment Information ページで確認できます。次に例を示します。

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management :	172.23.0.1
Data (nfs,cifs) :	**Node 1:** 172.23.0.2 | **Node 2:** 172.23.0.3

Access

SVM Management :	172.23.0.4

次の図は、中継ゲートウェイのルートテーブルを示しています。このルートには、 2 つの VPC の CIDR ブロックへのルートと、 Cloud Volumes ONTAP で使用される 4 つのフローティング IP アドレスが含まれます。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details | Associations | Propagations | **Routes** | Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route | Replace route | Delete route

Filter by attributes or search by keyword

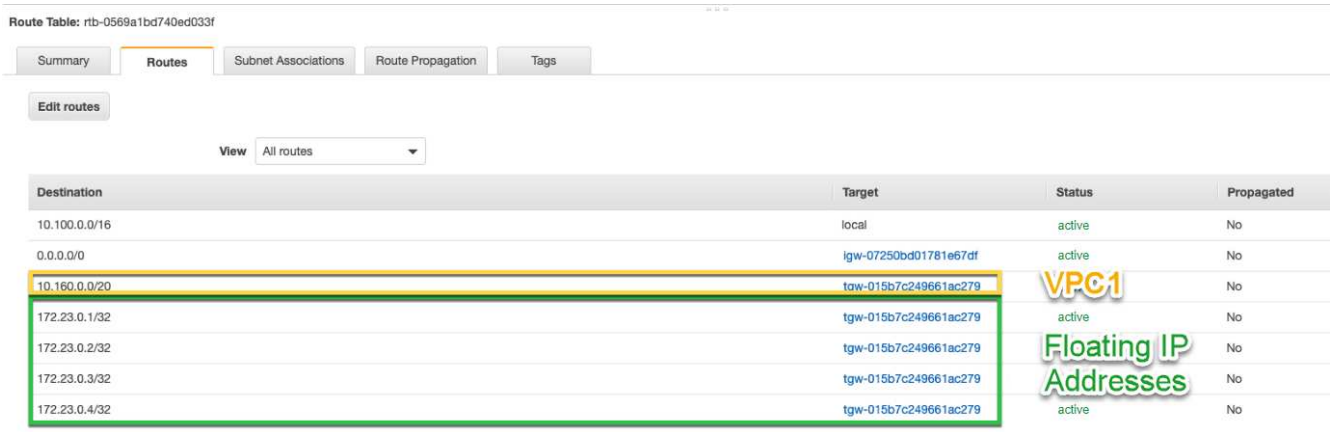
CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 | vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	Floating IP Addresses	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603		static	active

3. フローティング IP アドレスにアクセスする必要がある VPC のルーティングテーブルを変更します。

   a. フローティング IP アドレスにルートエントリを追加します。

   b. HA ペアが存在する VPC の CIDR ブロックにルートエントリを追加します。

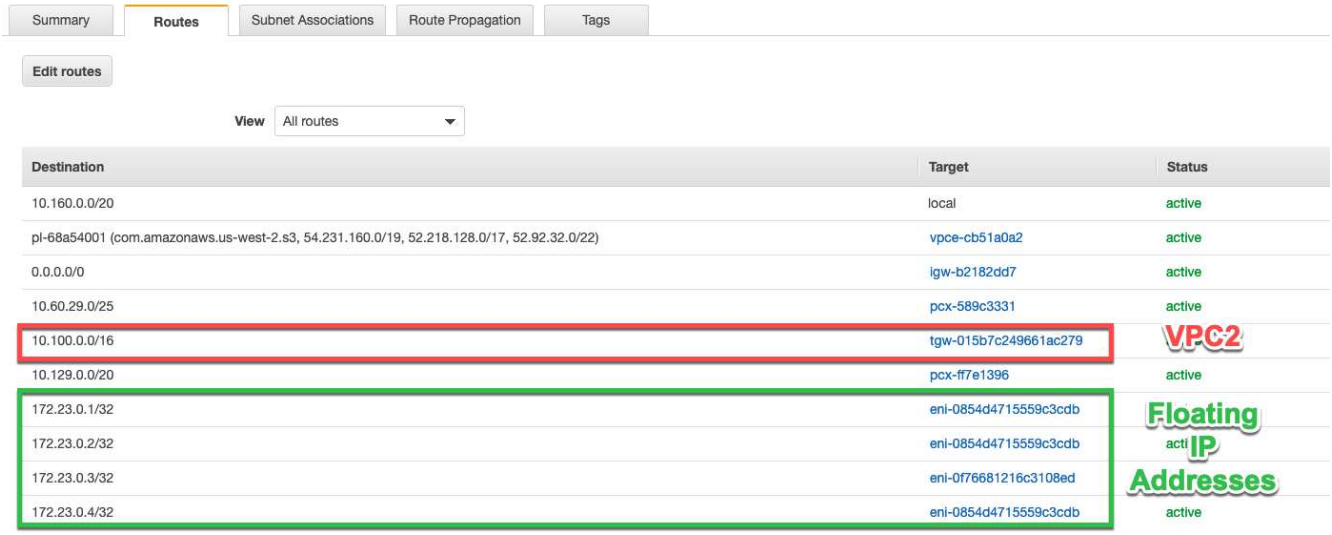
      次の図は、 VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



4. フローティング IP アドレスへのアクセスが必要な VPC へのルートを追加して、 HA ペアの VPC のルーティングテーブルを変更します。

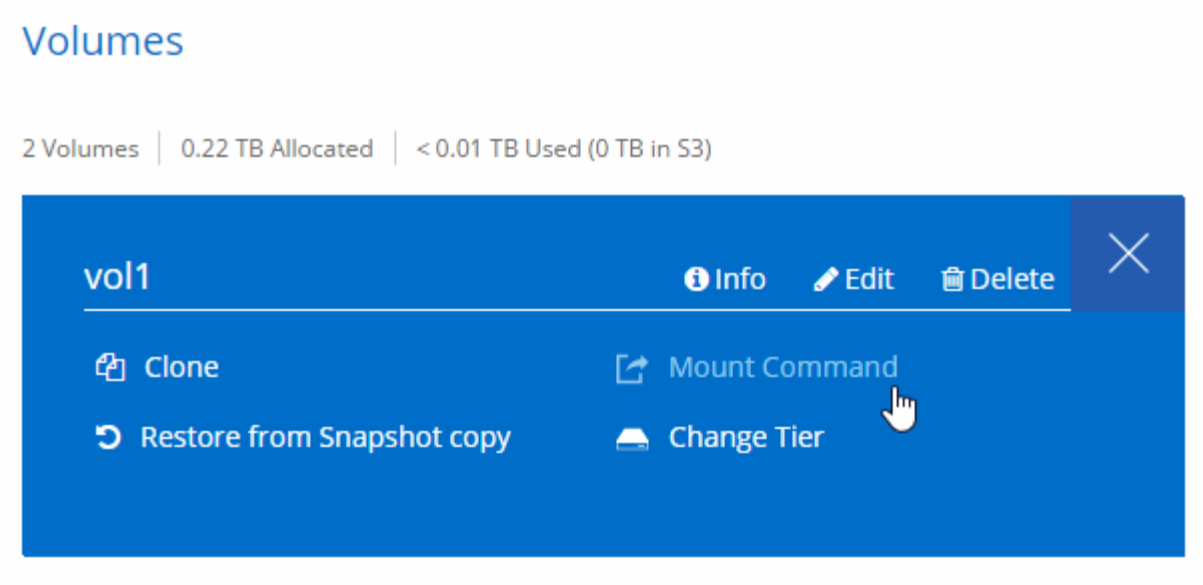
   VPC 間のルーティングが完了するため、この手順は重要です。

   次の例は、 VPC 1 のルートテーブルを示しています。フローティング IP アドレスへのルートと、クライアントが配置されている VPC 2 へのルートが含まれます。フローティング IP は、 HA ペアの導入時に Cloud Manager によってルートテーブルに自動的に追加されます。



5. フローティング IP アドレスを使用して、ボリュームをクライアントにマウントします。

   Cloud Manager で正しい IP アドレスを確認するには、ボリュームを選択して * Mount command * をクリックします。



- 関連リンク *
- "AWS におけるハイアベイラビリティペア"
- "Cloud Volumes ONTAP in AWS のネットワーク要件"

Azure の Cloud Volumes ONTAP のネットワーク要件

Cloud Volumes ONTAP システムが適切に動作するように Azure ネットワークをセットアップします。

Cloud Volumes ONTAP 用のアウトバウンドインターネットアクセス

Cloud Volumes ONTAP では、ネットアップ AutoSupport にメッセージを送信するためにアウトバウンドインターネットアクセスが必要です。ネットアップ AutoSupport は、ストレージの健全性をプロアクティブに監視します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

セキュリティグループ

Cloud Manager ではセキュリティグループを作成する必要がないため、セキュリティグループを作成する必要はありません。自分で使用する必要がある場合は、を参照してください "セキュリティグループのルール"。

IP アドレスの数

Cloud Manager が Azure の Cloud Volumes ONTAP に次の数の IP アドレスを割り当てます。

- シングルノード： 5 つの IP アドレス
- HA ペア： IP アドレス × 16

  Cloud Manager では、 HA ペア上に SVM 管理 LIF が作成されますが、 Azure のシングルノードシステ

ム上には作成されません。

> LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

クラウドボリューム **ONTAP** から **Azure BLOB** ストレージへの接続により、データ階層化を実現します

コールドデータを Azure BLOB ストレージに階層化する場合は、 Cloud Manager に必要な権限があるかぎりパフォーマンス階層と大容量階層の間の接続を設定する必要はありません。Cloud Manager ポリシーに以下の権限が設定されている場合、 Cloud Manager は VNet サービスエンドポイントを有効にします。

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

これらの権限は最新のに含まれています "Cloud Manager ポリシー"。

データ階層化の設定の詳細については、を参照してください "コールドデータを低コストのオブジェクトストレージに階層化する"。

他のネットワーク内の **ONTAP** システムへの接続

Azure の Cloud Volumes ONTAP システムと他のネットワークの ONTAP システムの間でデータをレプリケートするには、 Azure VNet と他のネットワーク（ AWS VPC や企業ネットワークなど）の間に VPN 接続が必要です。

手順については、を参照してください "Microsoft Azure のドキュメント：「 Create a Site-to-Site connection in the Azure portal"。

Cloud Volumes ONTAP in GCP のネットワーク要件

Cloud Volumes ONTAP システムが正常に動作するように、 Google Cloud Platform ネットワークをセットアップします。

共有 **VPC**

Cloud Manager と Cloud Volumes ONTAP は、 Google Cloud Platform の共有 VPC でサポートされています。

共有 VPC を使用すると、複数のプロジェクトの仮想ネットワークを設定し、一元管理できます。ホストプロジェクト _ で共有 VPC ネットワークをセットアップし、サービスプロジェクト _ で Cloud Manager と Cloud Volumes ONTAP の仮想マシンインスタンスを導入できます。 "Google Cloud のドキュメント：「 Shared VPC Overview"。

共有 VPC ホストプロジェクトの Cloud Manager サービスアカウントには、次の権限のみを付与する必要があります。

Compute.firewall.* compute.networks.* compute.subnetworks 。 *

Cloud Manager は、ホストプロジェクトのファイアウォール、 VPC 、およびサブネットを照会するためにこれらの権限を必要とします。

Cloud Volumes ONTAP 用のアウトバウンドインターネットアクセス

Cloud Volumes ONTAP では、ネットアップ AutoSupport にメッセージを送信するためにアウトバウンドインターネットアクセスが必要です。ネットアップ AutoSupport は、ストレージの健全性をプロアクティブに監視します。

Cloud Volumes ONTAP が AutoSupport メッセージを送信できるように、ルーティングポリシーとファイアウォールポリシーで次のエンドポイントへの HTTP / HTTPS トラフィックを許可する必要があります。

- \ https://support.netapp.com/aods/asupmessage
- \ https://support.netapp.com/asupprod/post/1.0/postAsup

IP アドレスの数

Cloud Manager は、 GCP の Cloud Volumes ONTAP に 5 つの IP アドレスを割り当てます。

Cloud Manager では、 GCP の Cloud Volumes ONTAP 用の SVM 管理 LIF は作成されません。

> LIF は、物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、 SVM 管理 LIF が必要です。

ファイアウォールルール

ファイアウォールルールを作成する必要はありません。ファイアウォールルールは Cloud Manager で自動的に作成されます。自分で使用する必要がある場合は、を参照してください "GCP ファイアウォールルール"。

の **Cloud Volumes ONTAP** から **Google Cloud Storage** への接続 データ階層化

コールドデータを Google Cloud Storage バケットに階層化する場合は、 Cloud Volumes ONTAP が配置されているサブネットをプライベート Google アクセス用に構成する必要があります。手順については、を参照してください "Google Cloud のドキュメント：「 Configuring Private Google Access"。

Cloud Manager でデータの階層化を設定するための追加の手順については、を参照してください "コールドデータを低コストのオブジェクトストレージに階層化する"。

他のネットワーク内の **ONTAP** システムへの接続

GCP 内の Cloud Volumes ONTAP システムと他のネットワーク内の ONTAP システムの間でデータをレプリケートするには、 VPC と他のネットワーク（たとえば社内ネットワーク）の間に VPN 接続が必要です。

手順については、を参照してください "Google Cloud のドキュメント：「 Cloud VPN Overview"。

追加の導入オプション

Cloud Manager ホストの要件

独自のホストに Cloud Manager をインストールする場合は、オペレーティングシステムの要件、ポートの要件など、構成のサポートを確認する必要があります。

Cloud Manager は GCP 内の自分のホストにインストールできますが、オンプレミスネットワークにはインストールできません。GCP に Cloud Volumes ONTAP を導入するには、 GCP に Cloud Manager をインストールする必要があります。

専用のホストが必要です

他のアプリケーションと共有しているホストでは、 Cloud Manager はサポートされません。専用のホストである必要があります。

サポートされている **AWS EC2** インスタンスタイプ

- t2.medium
- t3.medium （推奨）
- m4.large のいずれかです
- m5.xlarge のように指定します
- m5.2xlarge
- m5.mc
- m5.8xlarge

サポートされる **Azure VM** サイズ

A2 、 D2 v2 、または D2 v3 （可用性に基づく）

サポートされている **GCP** マシンタイプ

vCPU が 2 個以上、メモリが 4GB 以上のマシンタイプ。

サポートされているオペレーティングシステム

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4.
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  Red Hat Enterprise Linux システムは、 Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、システムは、 Cloud Manager のインストール中に必要なサードパーティソフトウェアをアップデートするためのリポジトリにアクセスできません。

  Cloud Manager は、これらのオペレーティングシステムの英語版でサポートされています。

ハイパーバイザー

認定済みのベアメタルハイパーバイザーまたはホスト型ハイパーバイザー CentOS または Red Hat Enterprise Linux を実行しますhttps://access.redhat.com/certified-hypervisors["Red Hat ソリューション：「 Which hypervisors are certified to run Red Hat Enterprise Linux ？」"^]

CPU

2.27 GHz 以上（2 コア

RAM

4 GB

空きディスク容量

50 GB

アウトバウンドインターネットアクセス

Cloud Manager をインストールする場合、および Cloud Manager を使用して Cloud Volumes ONTAP を導入する場合は、アウトバウンドインターネットアクセスが必要です。エンドポイントのリストについては、を参照してください "Cloud Manager のネットワーク要件"。

ポート

次のポートを使用できる必要があります。

- HTTP アクセスの場合は 80
- 443 ： HTTPS アクセス用
- 3306 （Cloud Manager データベース用
- クラウドマネージャ API プロキシの場合は 8080

他のサービスがこれらのポートを使用している場合、 Cloud Manager のインストールは失敗します。

> ポート 3306 との競合が発生する可能性があります。MySQL の別のインスタンスがホストで実行されている場合、デフォルトではポート 3306 が使用されます。既存の MySQL インスタンスが使用するポートを変更する必要があります。

Cloud Manager のインストール時に、デフォルトの HTTP ポートと HTTPS ポートを変更できます。MySQL データベースのデフォルトポートは変更できません。HTTP ポートと HTTPS ポートを変更する場合は、ユーザがリモートホストから Cloud Manager Web コンソールにアクセスできることを確認する必要があります。

- セキュリティグループを変更して、ポート経由の着信接続を許可します。
- Cloud Manager Web コンソールへの URL を入力するときにポートを指定します。

既存の **Linux** ホストに **Cloud Manager** をインストールする

Cloud Manager を導入する最も一般的な方法は、 Cloud Central またはクラウドプロバイダのマーケットプレイスから入手する方法です。ただし、自社ネットワークまたはクラウドにある既存の Linux ホストに Cloud Manager ソフトウェアをダウンロードしてインストールすることもできます。

> Cloud Manager は GCP 内の自分のホストにインストールできますが、オンプレミスネットワークにはインストールできません。GCP に Cloud Volumes ONTAP を導入するには、 GCP に Cloud Manager をインストールする必要があります。

作業を開始する前に

- Red Hat Enterprise Linux システムは、 Red Hat サブスクリプション管理に登録する必要があります。登録されていない場合、システムは、 Cloud Manager のインストール中に必要なサードパーティソフトウェアをアップデートするためのリポジトリにアクセスできません。
- Cloud Manager インストーラは、インストールプロセス中に複数の URL にアクセスします。アウトバウンドインターネットアクセスがこれらのエンドポイントに許可されていることを確認する必要があります。を参照してください "Cloud Manager のネットワーク要件"。

このタスクについて

- Cloud Manager のインストールにはルート権限は必要ありません。
- Cloud Manager は AWS コマンドラインツール（AWSCLI）をインストールして、ネットアップのサポートからのリカバリ手順を有効にします。

  AWSCLI のインストールに失敗したというメッセージが表示された場合は、このメッセージを無視しても問題ありません。Cloud Manager は、ツールを使用せずに正常に運用できます。

- ネットアップサポートサイトで入手できるインストーラは、それよりも古いバージョンの場合があります。インストール後に新しいバージョンが利用可能になると、 Cloud Manager は自動的に更新されます。

手順

1. ネットワーク要件を確認します。
   - "Cloud Manager のネットワーク要件"
   - "Cloud Volumes ONTAP in AWS のネットワーク要件"
   - "Azure の Cloud Volumes ONTAP のネットワーク要件"
   - "Cloud Volumes ONTAP in GCP のネットワーク要件"
2. レビュー "Cloud Manager ホストの要件"。
3. からソフトウェアをダウンロードします "ネットアップサポートサイト"をクリックし、 Linux ホストにコピーします。

   AWS の EC2 インスタンスに接続してファイルをコピーする方法については、を参照してください "AWS ドキュメント：「 Connecting to Your Linux Instance Using SSH"。

4. スクリプトを実行する権限を割り当てます。
   - 例 *

```
 chmod +x OnCommandCloudManager-V3.7.0.sh
. インストールスクリプトを実行します。
```

```
./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
[proxyport=port] [proxyuser=user_name] [proxypwd=password]
```

silent 情報の入力を求めずにインストールを実行します。

proxy _ は、 Cloud Manager ホストがプロキシサーバの背後にある場合に指定する必要があります。

proxyport_ は、プロキシサーバのポートです。

proxyUser は、ベーシック認証が必要な場合に、プロキシサーバのユーザ名です。

_proxypwd_は 、指定したユーザー名のパスワードです。

5. silent パラメータを指定しなかった場合は、「 * Y * 」と入力してスクリプトを続行し、プロンプトが表示されたら HTTP ポートと HTTPS ポートを入力します。

   HTTP ポートと HTTPS ポートを変更する場合は、ユーザがリモートホストから Cloud Manager Web コンソールにアクセスできることを確認する必要があります。

   - セキュリティグループを変更して、ポート経由の着信接続を許可します。
   - Cloud Manager Web コンソールへの URL を入力するときにポートを指定します。

     Cloud Manager がインストールされました。プロキシサーバを指定した場合、インストールの最後に Cloud Manager Service （ OCCM ）が 2 回再起動します。

6. Web ブラウザを開き、次の URL を入力します。

   https://ipaddress:port

   ipaddress _ には、 Cloud Manager ホストの設定に応じて、ローカルホスト、プライベート IP アドレス、またはパブリック IP アドレスを指定できます。たとえば、 Cloud Manager がパブリック IP アドレスのないパブリッククラウドにある場合は、 Cloud Manager ホストに接続されているホストからプライベート IP アドレスを入力する必要があります。

   デフォルトの HTTP （ 80 ）ポートまたは HTTPS （ 443 ）ポートを変更した場合は、 port_is 必須です。たとえば、 HTTPS ポートが 8443 に変更された場合はと入力します https://_ipaddress:8443

7. NetApp Cloud Central に登録するか、ログインします。
8. ログインしたら、 Cloud Manager をセットアップします。
   a. この Cloud Manager システムに関連付ける Cloud Central アカウントを指定してください。

      "Cloud Central アカウントについて詳しくは、こちらをご覧ください"。

   b. システムの名前を入力します。

完了後

Cloud Manager がクラウドプロバイダに Cloud Volumes ONTAP を導入できるように、権限を設定します。

- AWS "AWS アカウントをセットアップして、に追加します Cloud Manager の略"。
- Azure "Azure アカウントをセットアップして、に追加します Cloud Manager の略"。
- GCP ： Cloud Manager がプロジェクト内で Cloud Volumes ONTAP システムを作成および管理するために必要な権限を持つサービスアカウントを設定します。
  a. "GCP で役割を作成します" で定義した権限を含むポリシーを作成します "GCP 向け Cloud Manager ポリシー"。
  b. "GCP サービスアカウントを作成し、カスタムロールを適用します を作成しました"。
  c. "このサービスアカウントを Cloud Manager VM に関連付けます"。
  d. Cloud Volumes ONTAP を他のプロジェクトに導入する場合は、 "クラウドでサービスアカウントを追加してアクセスを許可します そのプロジェクトに対するマネージャの役割"。プロジェクトごとにこの手順を繰り返す必要があります。

AWS Marketplace からの Cloud Manager の起動

を使用して、 AWS で Cloud Manager を起動することを推奨します "NetApp Cloud Central"必要に応じて、 AWS Marketplace から起動できます。

AWS Marketplace から Cloud Manager を起動しても、 Cloud Manager は NetApp Cloud Central と統合されたままです。 "統合の詳細については、こちらをご覧ください。"。

このタスクについて

以下の手順では、 EC2 コンソールからインスタンスを起動する方法について説明します。このコンソールでは、 IAM ロールを Cloud Manager インスタンスに関連付けることができます。これは、 * ウェブサイトからの起動 * アクションを使用しては実行できません。

手順

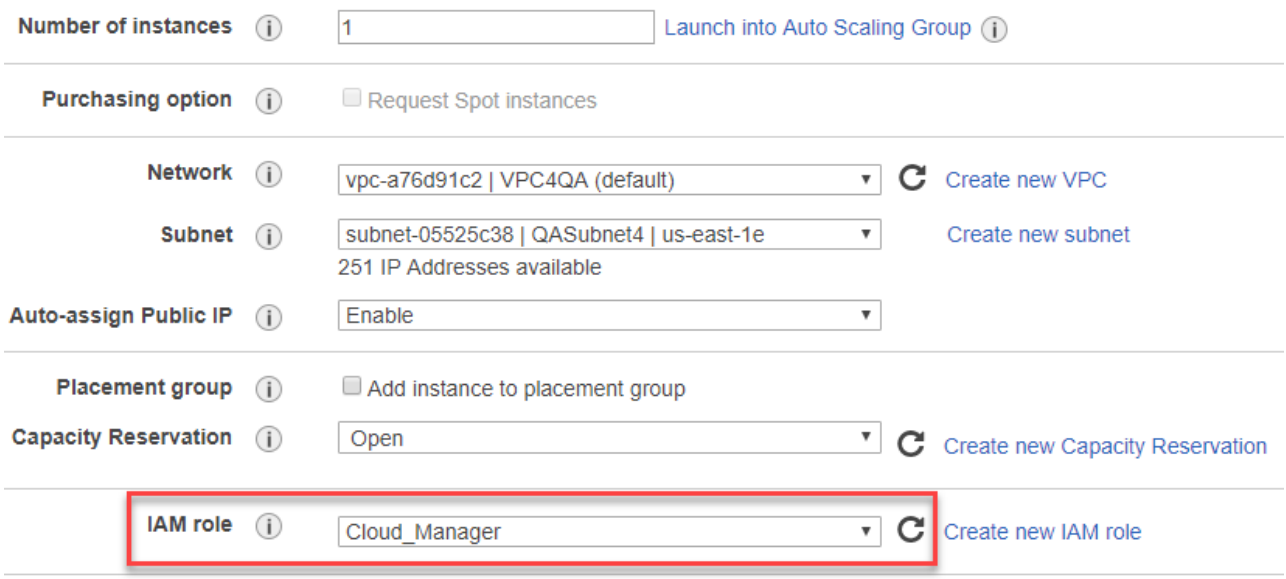
1. EC2 インスタンス用の IAM ポリシーとロールを作成します。
   a. 次のサイトから Cloud Manager IAM ポリシーをダウンロードします。

      "NetApp Cloud Manager ： AWS 、 Azure 、 GCP ポリシー"

   b. IAM コンソールから、 Cloud Manager IAM ポリシーからテキストをコピーアンドペーストして、独自のポリシーを作成します。
   c. ロールタイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーをロールに付加します。
2. "AWS Marketplace でサブスクライブ" Cloud Volumes ONTAP の無償トライアルの終了後にサービスを中断しないようにするため。お客様が作成した Cloud Volumes ONTAP 9.6 以降の PAYGO システムと、有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。
3. 次に、に進みます "AWS Marketplace の Cloud Manager のページ" AMI から Cloud Manager を導入
4. [Marketplace] ページで [* Continue to Subscribe*] をクリックし、 [* Continue to Configuration*] をクリックします。
5. デフォルトのオプションを変更し、 [* Continue to Launch] をクリックします。
6. [アクションの選択 **]** で **[** EC2 で起動] を選択し、 [* 起動 *] をクリックします。
7. プロンプトに従って、インスタンスを設定および導入します。
   - * インスタンスタイプを選択 * ：リージョンの可用性に応じて、サポートされているインスタンスタイプ（ t3.medium を推奨）のいずれかを選択します。

     "サポートされているインスタンスタイプのリストを確認します"。

   - * Configure Instance * ： VPC とサブネット、手順 1 で作成した IAM ロール、および要件に合ったその他の設定オプションを選択します。



- * Add Storage* ：デフォルトのストレージ・オプションをそのまま使用します。
- * Add Tags* ：必要に応じて、インスタンスのタグを入力します。
- * セキュリティグループの設定 * ： Cloud Manager インスタンスに必要な接続方法を、 SSH 、 HTTP 、 HTTPS のいずれかで指定します。
- * 復習 * ：選択内容を確認して、 * 起動 * をクリックします。

  AWS は、指定した設定でソフトウェアを起動します。Cloud Manager インスタンスとソフトウェアは、約 5 分で実行されます。

8. Cloud Manager 仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   http://ipaddress:80

9. ログインしたら、 Cloud Manager をセットアップします。
   a. この Cloud Manager システムに関連付ける Cloud Central アカウントを指定してください。

      "Cloud Central アカウントについて詳しくは、こちらをご覧ください"。

   b. システムの名前を入力します。

結果

Cloud Manager のインストールとセットアップが完了しました。

Azure Marketplace から Cloud Manager を導入する

を使用して Azure に Cloud Manager を導入することを推奨します "NetApp Cloud Central"必要に応じて、 Azure Marketplace から導入することもできます。

Cloud Manager の導入手順については、を参照してください "Azure US Government リージョン" およびインチ "Azure ドイツ地域"。

> Azure Marketplace から Cloud Manager を導入した場合でも、 Cloud Manager は NetApp Cloud Central と統合されます。 "統合の詳細については、こちらをご覧ください。"。

Azure での Cloud Manager の導入

Cloud Manager をインストールしてセットアップし、それを使用して Azure の Cloud Volumes ONTAP を起動できるようにする必要があります。

手順

1. "Cloud Manager の Azure Marketplace ページにアクセスします。"。

2. [* Get it Now* (今すぐ取得)] をクリックし、 [* Continue * (続行)] をクリックします。
3. Azure ポータルで、 * Create * をクリックし、手順に従って仮想マシンを設定します。

   VM を設定する際には、次の点に注意してください。

   - Cloud Manager は、 HDD または SSD ディスクのいずれかで最適なパフォーマンスを実現できます。
   - 推奨される仮想マシンサイズの中から 1 つを選択してください： A2 、 D2 v2 、または D2 v3 （可用性に基づく）。
   - ネットワークセキュリティグループの場合、 Cloud Manager は、 SSH 、 HTTP 、および HTTPS を使用したインバウンド接続を必要とします。

     "Cloud Manager のセキュリティグループルールの詳細については、こちらをご覧ください"。

   - [* 管理] で、 [* オン *] を選択して、 Cloud Manager に対して * システム割り当ての管理 ID * を有効にします。

     この設定は重要です。管理対象の ID を使用すると、 Cloud Manager 仮想マシンはクレデンシャルを提供することなく Azure Active Directory に自身を識別できます。 "Azure リソース用の管理対象 ID の詳細については、こちらをご覧ください"。

4. [* Review + create * （レビュー + 作成）] ページで選択内容を確認し、 [* Create * （作成）] をクリックして展開を開始します。

   指定した設定で仮想マシンが展開されます。Virtual Machine と Cloud Manager ソフトウェアは、約 5 分で実行されます。

5. Cloud Manager 仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   http://ipaddress:80

6. ログインしたら、 Cloud Manager をセットアップします。
   a. この Cloud Manager システムに関連付ける Cloud Central アカウントを指定してください。

      "Cloud Central アカウントについて詳しくは、こちらをご覧ください"。

   b. システムの名前を入力します。

結果

Cloud Manager のインストールとセットアップが完了しました。Cloud Volumes ONTAP を Azure に導入するには、 Azure の権限を付与する必要があります。

Cloud Manager への Azure の権限の付与

Azure に Cloud Manager を導入した場合は、を有効にしておく必要があります "システムによって割り当てられた管理 ID"。ここで、必要な Azure 権限を付与する必要があります。そのためには、カスタムロールを作成してから、 1 つ以上のサブスクリプションの Cloud Manager 仮想マシンにそのロールを割り当てます。

手順

1. Cloud Manager ポリシーを使用してカスタムロールを作成します。

   a. をダウンロードします "Cloud Manager Azure ポリシー"。

   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。

      ユーザが Cloud Volumes ONTAP システムを作成する Azure サブスクリプションごとに ID を追加する必要があります。

      - 例 *

      「譲渡対象」：「 / 契約 / D333AF45-0D07-4154-943D-C25FBZZZZ 」、「 / 契約 / 契約 /54B91999-B3E6-4599-908E-416E0ZZZZ 」、「 / 契約 /E471C-3B42-4AE7-9B59-CE5BBZZZZ 」

c. JSON ファイルを使用して、 Azure でカスタムロールを作成します。

次の例は、 Azure CLI 2.0 を使用してカスタムロールを作成する方法を示しています。

- AZ 役割定義 create — 役割定義 C ： \Policy_For _Cloud_Manager_Azure_3.7.4.json *

これで、 OnCommand Cloud Manager Operator という名前のカスタムロールが作成され、 Cloud Manager 仮想マシンに割り当てることができるようになりました。

2. 1 つ以上のサブスクリプションの役割を Cloud Manager 仮想マシンに割り当てます。

a. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP システムを展開するサブスクリプションを選択します。

b. 「 * アクセスコントロール（ IAM ） * 」をクリックします。

c. [* 追加 > 役割の割り当ての追加 *] をクリックして、権限を追加します。

- OnCommand Cloud Manager Operator * ロールを選択します。

> OnCommand Cloud Manager Operator は、で指定されたデフォルトの名前です "Cloud Manager ポリシー"。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

- 仮想マシン * へのアクセスを割り当てます。
- Cloud Manager 仮想マシンが作成されたサブスクリプションを選択します。
- Cloud Manager 仮想マシンを選択します。
- [保存（ Save ）] をクリックします。

d. 追加のサブスクリプションから Cloud Volumes ONTAP を導入する場合は、そのサブスクリプションに切り替えてから、これらの手順を繰り返します。

結果

Cloud Manager には、クラウドボリューム ONTAP を Azure に導入して管理するために必要な権限が付与されました。

Azure US Government リージョンでの Cloud Manager の導入

Cloud Manager を米国政府機関のリージョンで運用開始するには、まず Azure Government Marketplace から Cloud Manager を導入します。次に、 Cloud Volumes ONTAP システムを導入して管理するために Cloud Manager に必要な権限を指定します。

サポートされている Azure US Government リージョンのリストについては、を参照してください "Cloud Volume グローバルリージョン"。

Azure US Government Marketplace からの Cloud Manager の導入

Cloud Manager は、 Azure US Government Marketplace のイメージとして提供されています。

手順

1. サブスクリプションで Azure Government Marketplace が有効になっていることを確認します。
   a. Enterprise Administrator としてポータルにログインします。
   b. 「 * Manage * 」（管理）に移動します。
   c. [* 加入の詳細 *] で、 [* Azure Marketplace] の横にある鉛筆アイコンをクリックします。
   d. [有効] を選択します。
   e. [保存（ Save ）] をクリックします。

      "Microsoft Azure のドキュメント：「 Azure Government Marketplace"

2. Azure US Government ポータルで OnCommand Cloud Manager を検索してください。
3. [* Create] をクリックし、手順に従って仮想マシンを設定します。

   仮想マシンを構成するときは、次の点に注意してください。

   - Cloud Manager は、 HDD または SSD ディスクのいずれかで最適なパフォーマンスを実現できます。
   - 推奨される仮想マシンサイズの中から 1 つを選択してください： A2 、 D2 v2 、または D2 v3 （可用性に基づく）。
   - ネットワーク・セキュリティー・グループには、「 * 詳細設定 * 」を選択するのが最適です。
     - Advanced * オプションを指定すると、 Cloud Manager に必要なインバウンドルールを含む新しいセキュリティグループが作成されます。Basic を選択した場合は、を参照してください "セキュリティグループのルール" をクリックして必要なルールを選択してください。
4. 概要ページで選択内容を確認し、 * 作成 * をクリックして展開を開始します。

   指定した設定で仮想マシンが展開されます。Virtual Machine と Cloud Manager ソフトウェアは、約 5 分で実行されます。

5. Cloud Manager 仮想マシンに接続しているホストから Web ブラウザを開き、次の URL を入力します。

   http://ipaddress:80

6. ログインしたら、 Cloud Manager をセットアップします。
   a. この Cloud Manager システムに関連付ける Cloud Central アカウントを指定してください。

      "Cloud Central アカウントについて詳しくは、こちらをご覧ください"。

   b. システムの名前を入力します。

結果

Cloud Manager のインストールとセットアップが完了しました。Cloud Volumes ONTAP を Azure に導入するには、 Azure の権限を付与する必要があります。

管理対象 **ID** を使用した **Cloud Manager** への **Azure** 権限の付与

アクセス許可を設定する最も簡単な方法は、を有効にすることです "管理された ID" Cloud Manager 仮想マシンで、必要な権限を仮想マシンに割り当てます。必要に応じて、別の方法がになります "サービスプリンシパルを使用して Azure 権限を付与します"。

手順

1. Cloud Manager 仮想マシンで管理対象 ID を有効にします。
   a. Cloud Manager 仮想マシンに移動して、 * Identity * を選択します。
   b. [システム割り当て済み *] で、 [* オン *] をクリックし、 [* 保存 *] をクリックします。
2. Cloud Manager ポリシーを使用してカスタムロールを作成します。
   a. をダウンロードします "Cloud Manager Azure ポリシー"。
   b. 割り当て可能なスコープに Azure サブスクリプション ID を追加して、 JSON ファイルを変更します。

      ユーザが Cloud Volumes ONTAP システムを作成する Azure サブスクリプションごとに ID を追加する

必要があります。

- 例 *

「譲渡対象」：「 / 契約 / D333AF45-0D07-4154-943D-C25FBZZZZ 」、「 / 契約 / 契約 /54B91999-B3E6-4599-908E-416E0ZZZZ 」、「 / 契約 /E471C-3B42-4AE7-9B59-CE5BBZZZZ 」

c. JSON ファイルを使用して、 Azure でカスタムロールを作成します。

次の例は、 Azure CLI 2.0 を使用してカスタムロールを作成する方法を示しています。

- AZ 役割定義 create — 役割定義 C ： \Policy_For _Cloud_Manager_Azure_3.7.4.json *

これで、 OnCommand Cloud Manager Operator という名前のカスタムロールが作成され、 Cloud Manager 仮想マシンに割り当てることができるようになりました。

3. 1 つ以上のサブスクリプションの役割を Cloud Manager 仮想マシンに割り当てます。

a. [サブスクリプション] サービスを開き、 Cloud Volumes ONTAP システムを展開するサブスクリプションを選択します。

b. 「 * アクセスコントロール（ IAM ） * 」をクリックします。

c. [* 追加] をクリックし、 [* 役割の割り当ての追加 *] をクリックして、権限を追加します。

- OnCommand Cloud Manager Operator * ロールを選択します。

> OnCommand Cloud Manager Operator は、で指定されたデフォルトの名前です "Cloud Manager ポリシー"。ロールに別の名前を選択した場合は、代わりにその名前を選択します。

- 仮想マシン * へのアクセスを割り当てます。
- Cloud Manager 仮想マシンが作成されたサブスクリプションを選択します。
- 仮想マシンの名前を入力し、選択します。
- [保存（ Save ）] をクリックします。

d. 追加のサブスクリプションから Cloud Volumes ONTAP を導入する場合は、そのサブスクリプションに切り替えてから、これらの手順を繰り返します。

結果

Cloud Manager には、クラウドボリューム ONTAP を Azure に導入して管理するために必要な権限が付与されました。

Azure ドイツリージョンへの Cloud Manager のインストール

Azure Marketplace は Azure Germany 地域ではご利用いただけません。そのため、Cloud Manager インストーラをネットアップのサポートサイトからダウンロードし、地域の既存の Linux ホストにインストールする必要があります。

手順

1. "Azure のネットワーク要件を確認します。"。
2. "Cloud Manager のホスト要件を確認します。"。

3. "Cloud Manager をダウンロードしてインストールします。"。
4. "サービスプリンシパルを使用して Cloud Manager に Azure 権限を付与します"。

完了後

Cloud Manager は、他の地域と同様に、 Azure Germany 地域に Cloud Volumes ONTAP を導入する準備が整いました。ただし、最初に追加のセットアップを実行することもできます。

Cloud Manager を起動して実行します

Cloud Manager は常時実行されている必要があります。

Cloud Manager は、 Cloud Volumes ONTAP の健全性と課金において重要な要素です。Cloud Manager の電源がオフになっている場合、 Cloud Manager との通信が失われてから 4 日以上が経過すると Cloud Volumes ONTAP システムがシャットダウンします。

Cloud Volumes ONTAP を導入します

Cloud Volumes ONTAP システムを作成する前に

Cloud Manager を使用して Cloud Volumes ONTAP システムを作成および管理する前に、 Cloud Manager 管理者がネットワークを準備し、 Cloud Manager をインストールしてセットアップしておく必要があります。

Cloud Volumes ONTAP の導入を開始する前に、次の条件を満たす必要があります。

- Cloud Manager と Cloud Volumes ONTAP のネットワーク要件を満たしている。
- Cloud Manager に、選択したクラウドプロバイダで処理を実行する権限がある。
- AWS の場合は、適切な AWS Marketplace ページに登録しています。
  - PAYGO システムを導入する場合や、アドオン機能を有効にする場合は、次の手順を実行します。 "Cloud Manager （ Cloud Volumes ONTAP 用）のページです"。
  - BYOL システムを導入する場合は、次の手順を実行します。 "AWS Marketplace のシングルノードまたは HA のページ"。
- Cloud Manager がインストールされました。

関連リンク

- "AWS の概要"
- "Azure の導入を開始します"
- "GCP の概要"
- "Cloud Manager のセットアップ"

Cloud Manager にログインしています

Cloud Manager システムに接続されている任意の Web ブラウザから Cloud Manager にログインできます。を使用してログインする必要があります "NetApp Cloud Central" ユーザアカウント

手順

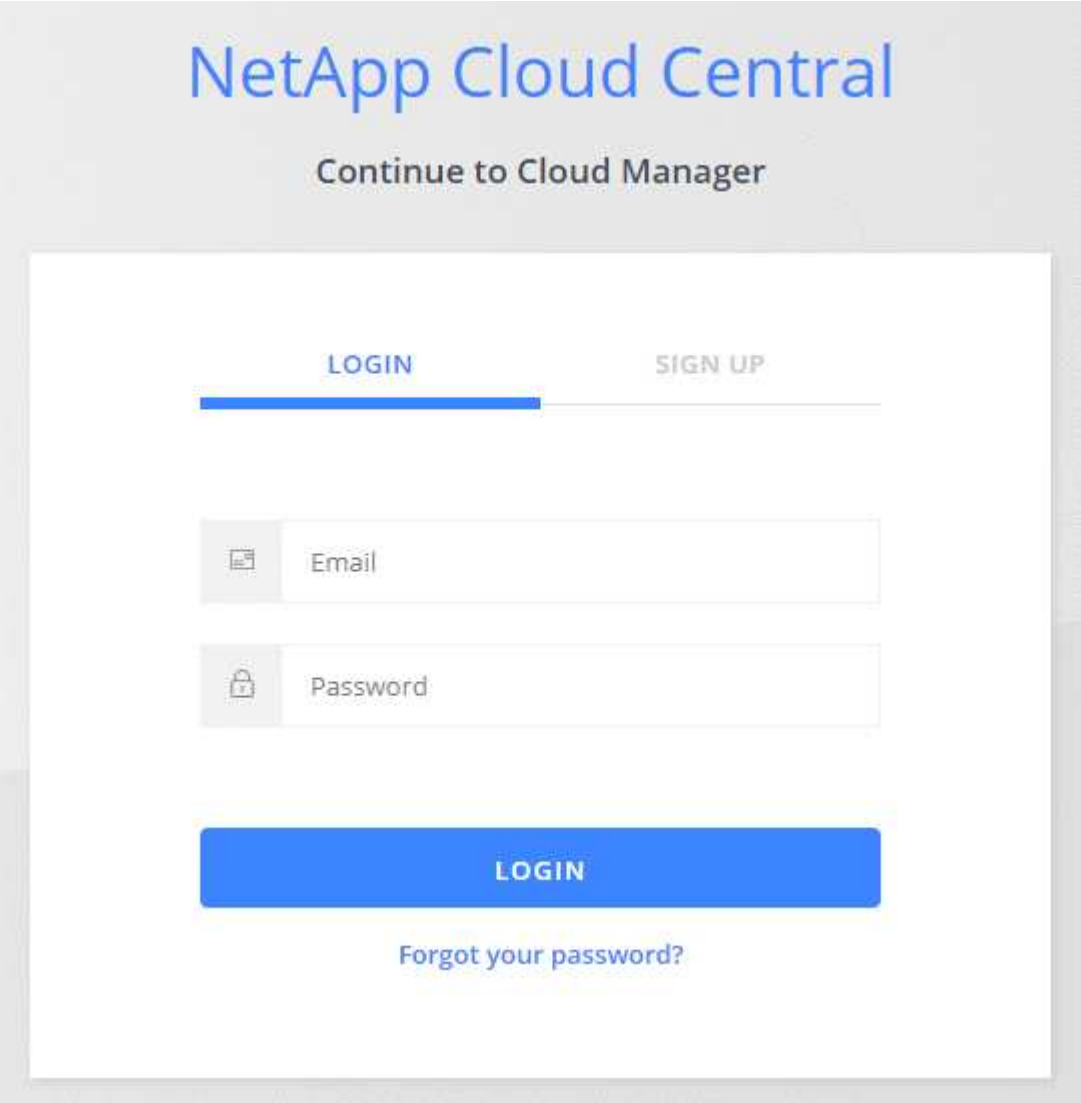
1. Web ブラウザを開き、にログインします "NetApp Cloud Central"。

   この手順では、自動的に Fabric View に移動します。表示されない場合は、 * Fabric View* をクリックします。

2. アクセスする Cloud Manager システムを選択します。

   システムが表示されない場合は、 Cloud Manager システムに関連付けられている Cloud Central アカウントにアカウント管理者が追加したことを確認してください。

3. NetApp Cloud Central のクレデンシャルを使用して Cloud Manager にログインします。



Cloud Volumes ONTAP 構成を計画

Cloud Volumes ONTAP を導入する場合は、ワークロード要件に一致する事前設定済みのシステムを選択するか、独自の構成を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

ライセンスタイプの選択

Cloud Volumes ONTAP には、従量課金制とお客様所有のライセンスを使用（ BYOL ）の 2 種類の料金プランがあります。従量課金制の場合は、 Explore 、 Standard 、 Premium の 3 つのライセンスから選択できます。ライセンスごとに容量とコンピューティングのオプションが異なります。

- "AWS の Cloud Volumes ONTAP 9.7 でサポートされている構成"
- "Cloud Volumes ONTAP 9.7 で Azure でサポートされる構成"
- "GCP の Cloud Volumes ONTAP 9.7 でサポートされている構成"

ストレージの制限を理解する

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

- "AWS の Cloud Volumes ONTAP 9.7 でのストレージの制限"
- "Cloud Volumes ONTAP 9.7 の Azure のストレージ制限"
- "GCP の Cloud Volumes ONTAP 9.7 でのストレージの制限"

書き込み速度の選択

Cloud Manager では、シングルノードの Cloud Volumes ONTAP システムの書き込み速度設定を選択できます。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。

通常の書き込み速度と高速書き込み速度の差

通常の書き込み速度を選択すると、データはディスクに直接書き込まれるため、計画外のシステム停止が発生した場合にデータが失われる可能性が低くなります。

高速書き込みを選択すると、データはディスクに書き込まれる前にメモリにバッファされるため、書き込みパフォーマンスが向上します。このキャッシュにより、計画外のシステム停止が発生した場合にデータが失われる可能性があります。

計画外のシステム停止が発生した場合に失われる可能性があるデータの量は、最後の 2 つの整合ポイントの範囲です。整合ポイントとは、バッファされたデータをディスクに書き込むことです。整合ポイントは、書き込みログがいっぱいになったとき、または 10 秒後（どちらか早い方）に発生します。ただし、 AWS EBS ボリュームのパフォーマンスは、整合ポイントの処理時間に影響を与える可能性があります。

高速書き込みを使用する場合

高速書き込みは、ワークロードに高速書き込みパフォーマンスが必要な場合に最適です。また、予期しないシステム停止が発生した場合にも、データ損失のリスクに耐えることができます。

高速書き込みを使用する場合の推奨事項

高速書き込みを有効にする場合は、アプリケーション層で書き込み保護を確保する必要があります。

ボリューム使用プロファイルの選択

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。Cloud Manager でボリュームを作成する場合は、これらの機能を有効にするプロファイルを選択するか、無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に

割り当てられます。

重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの格納に必要な物理容量を削減します。

AWS の計画

システムのサイズを決定し、入力する必要があるネットワーク情報を確認して、 AWS に Cloud Volumes ONTAP を導入する計画を立てます。

- AWS でのシステムのサイジング
- AWS ネットワーク情報ワークシート

AWS でのシステムのサイジング

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。インスタンスタイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意する必要があります。

インスタンスタイプ

- ワークロードの要件を、各 EC2 インスタンスタイプの最大スループットと IOPS に合わせます。
- 複数のユーザが同時にシステムに書き込む場合は、要求を管理するのに十分な CPU を備えたインスタンスタイプを選択します。
- 読み取りが多いアプリケーションがある場合は、十分な RAM が搭載されたシステムを選択します。
  - "AWS ドキュメント：「 Amazon EC2 Instance Types"
  - "AWS のドキュメント：「 Amazon EBS – Optimized instances"

EBS ディスクタイプ

汎用 SSD は、 Cloud Volumes ONTAP で最も一般的なディスクタイプです。EBS ディスクのユースケースについては、を参照してください "AWS ドキュメント：「 EBS Volume Types"。

EBS ディスクサイズ

Cloud Volumes ONTAP システムを起動するときに初期ディスクサイズを選択する必要があります。その後、次の操作を実行できます "システムの容量を Cloud Manager で管理できます"必要に応じて "アグリゲートを自分で作成する"、次の点に注意してください。

- アグリゲート内のディスクはすべて同じサイズである必要があります。
- EBS ディスクのパフォーマンスはディスクサイズに依存します。サイズによって、 SSD ディスクのベースライン IOPS と最大バースト期間、および HDD ディスクのベースラインスループットとバーストスループットが決まります。
- 最終的には、必要なパフォーマンスを継続的に提供するディスクサイズを選択する必要があります。

- 4 TB のディスクを 6 台使用するなど、大容量のディスクを選択した場合でも、 EC2 インスタンスの帯域幅が制限に達する可能性があるため、すべての IOPS が得られないことがあります。

  EBS ディスクのパフォーマンスの詳細については、を参照してください "AWS ドキュメント：「 EBS Volume Types"。

AWS での Cloud Volumes ONTAP システムのサイジングに関する詳細については、次のビデオを参照してください。

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

AWS ネットワーク情報ワークシート

AWS で Cloud Volumes ONTAP を起動する場合は、 VPC ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

Cloud Volumes ONTAP のネットワーク情報

AWS 情報	あなたの価値
地域	
vPC	
サブネット	
セキュリティグループ（独自のグループを使用している場合）	

複数の **AZS** 内の **HA** ペアのネットワーク情報

AWS 情報	あなたの価値
地域	
vPC	
セキュリティグループ（独自のグループを使用している場合）	
ノード 1 の可用性ゾーン	
ノード 1 のサブネット	
ノード 2 の可用性ゾーン	
ノード 2 のサブネット	
メディエータ可用性ゾーン	
メディエータサブネット	
メディエータのキーペア	
クラスタ管理ポートのフローティング IP アドレス	
ノード 1 のデータの浮動 IP アドレス	

AWS 情報	あなたの価値
ノード 2 のデータの浮動 IP アドレス	
フローティング IP アドレスのルートテーブル	

Azure の計画

システムのサイズを決定し、入力する必要があるネットワーク情報を確認して、 Azure への Cloud Volumes ONTAP の導入を計画します。

- Azure でのシステムのサイジング
- Azure ネットワーク情報ワークシート

Azure でのシステムのサイジング

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。VM タイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

仮想マシンのタイプ

でサポートされている仮想マシンタイプを確認します "Cloud Volumes ONTAP リリースノート" サポートされている各 VM タイプの詳細を確認します。各 VM タイプがサポートするデータディスクの数には制限があることに注意してください。

- "Azure のドキュメント：「汎用仮想マシンのサイズ"
- "Azure のドキュメント：「 Memory optimized virtual machine sizes"

Azure のディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する場合は、 ONTAP がディスクとして使用する基盤となるクラウドストレージを選択する必要があります。

HA システムでは、 Premium ページ BLOB を使用します。一方、シングルノードシステムでは、次の 2 種類の Azure Managed Disks を使用できます。

- _Premium SSD Managed Disks （プレミアム SSD 管理ディスク） - I/O 負荷の高いワークロードに高パフォーマンスを提供し、コストを高めます。
- _ 標準 SSD 管理ディスク _ 低 IOPS を必要とするワークロードに一貫したパフォーマンスを提供します。
- _Standard HDD Managed Disks_are a good choice if you need high iops and want to Reduce your costs （高 IOPS が必要なく、コストを削減したい場合に最適です。）

  これらのディスクのユースケースの詳細については、を参照してください "Microsoft Azure のドキュメント：「 Introduction to Microsoft Azure Storage"。

Azure のディスクサイズ

Cloud Volumes ONTAP インスタンスを起動するときは、アグリゲートのデフォルトのディスクサイズを選択する必要があります。Cloud Manager では、このディスクサイズを初期アグリゲートに使用します。ま

た、簡易プロビジョニングオプションを使用した場合に作成される追加のアグリゲートにも使用します。別のディスクサイズを使用するアグリゲートを作成できます デフォルトでは、です "高度な割り当てオプションを使用する"。

アグリゲート内のディスクはすべて同じサイズである必要があります。

ディスクサイズを選択する際には、いくつかの要素を考慮する必要があります。ディスクサイズは、ストレージのコスト、アグリゲートに作成できるボリュームのサイズ、 Cloud Volumes ONTAP で使用可能な総容量、ストレージパフォーマンスに影響します。

Azure Premium ストレージのパフォーマンスは、ディスクサイズに依存します。ディスク容量が大きいほど、 IOPS とスループットが向上します。たとえば、 1 TB のディスクを選択すると、 500 GB のディスクよりも高いパフォーマンスを低コストで実現できます。

標準ストレージのディスクサイズにはパフォーマンスの違いはありません。必要な容量に基づいてディスクサイズを選択する必要があります。

ディスクサイズ別の IOPS とスループットについては、 Azure を参照してください。

- "Microsoft Azure ： Managed Disks の価格"
- "Microsoft Azure ： Page Blob の価格設定"

Azure ネットワーク情報ワークシート

Cloud Volumes ONTAP を Azure に導入する場合は、仮想ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

Azure の情報	あなたの価値
地域	
仮想ネットワーク（ Vnet ）	
サブネット	
Network Security Group （独自のグループを使用している場合）	

GCP 計画

システムのサイズを決定し、入力する必要があるネットワーク情報を確認して、 Google Cloud Platform への Cloud Volumes ONTAP の導入を計画します。

- GCP でシステムのサイジングを行う
- GCP ネットワーク情報ワークシート

GCP でシステムのサイジングを行う

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。マシンタイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

マシンのタイプ

でサポートされているマシンタイプを確認します "Cloud Volumes ONTAP リリースノート" 次に、サポートされている各マシンタイプについて Google の詳細を確認します。ワークロードの要件を、マシンタイプの vCPU とメモリの数と一致させます。各 CPU コアは、ネットワークパフォーマンスを向上させることに注意してください。

詳細については、以下を参照してください。

- "Google Cloud ドキュメント： N1 標準マシンタイプ"
- "Google Cloud のドキュメント：「 Performance"

GCP ディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する際には、 Cloud Volumes ONTAP がディスクに使用する基盤となるクラウドストレージを選択する必要があります。ディスクタイプには、 _Zonal SSD persistent disks _ または _Zonal standard persistent disks _ を指定できます。

SSD 永続ディスクはランダム IOPS の高い処理速度を必要とするワークロードに最適ですが、標準的な永続ディスクは経済的で、シーケンシャル読み取り / 書き込み処理にも対応できます。詳細については、を参照してください "Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD ）」"。

GCP ディスクサイズ

Cloud Volumes ONTAP システムを導入する際には、初期ディスクサイズを選択する必要があります。そのあと、システムの容量を Cloud Manager で管理できるようになりますが、アグリゲートを手動で作成する場合は、次の点に注意してください。

- アグリゲート内のディスクはすべて同じサイズである必要があります。
- パフォーマンスを考慮しながら、必要なスペースを判断します。
- パーシステントディスクのパフォーマンスは、システムで使用可能なディスクサイズと vCPU の数に応じて自動的に拡張されます。

  詳細については、以下を参照してください。

  - "Google Cloud のドキュメント：「ゾーン永続ディスク（標準および SSD ）」"
  - "Google Cloud のドキュメント：「 Optimizing Persistent Disk and Local SSD Performance"

GCP ネットワーク情報ワークシート

GCP で Cloud Volumes ONTAP を導入する場合は、仮想ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

GCP 情報	あなたの価値
地域	
ゾーン	
vPC ネットワーク	
サブネット	

GCP 情報	あなたの価値
ファイアウォールポリシー（独自のポリシーを使用している場合）	

Cloud Manager システム ID を確認する

作業を開始する際に、ネットアップの担当者から Cloud Manager システム ID の入力を求められることがあります。この ID は通常、ライセンスの取得やトラブルシューティングの目的で使用されます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックします。

2. サポートダッシュボード * をクリックします。

   システム ID が右上に表示されます。

   - 例 *

Cloud Volumes ONTAP で Flash Cache を有効にしています

AWS および Azure の一部の Cloud Volumes ONTAP 構成にはローカルの NVMe ストレージが含まれています。このストレージは、 Cloud Volumes ONTAP でパフォーマンスを向上させるために _Flash Cache _ として使用されます。

Flash Cacheとは

Flash Cache は、最近読み取られたユーザデータとネットアップのメタデータをリアルタイムでインテリジェントにキャッシングすることで、データへのアクセスを高速化します。データベース、 E メール、ファイルサービスなど、ランダムリードが大量に発生するワークロードに効果的です。

制限

- Flash Cache のパフォーマンス向上を利用するには、すべてのボリュームで圧縮を無効にする必要があります。
- 再起動後のキャッシュの再ウォームアップは、 Cloud Volumes ONTAP ではサポートされていません。

AWS での Cloud Volumes ONTAP での Flash Cache の有効化

Flash Cache は、 AWS で Cloud Volumes ONTAP Premium および BYOL を使用してサポートされています。

手順

1. 新規または既存の Cloud Volumes ONTAP Premium または BYOL システムがある EC2 インスタンスタイプを選択します。
    - c5d.csi
    - c5d.9xlarge
    - r5d.2xlarge
2. Flash Cache のパフォーマンス向上を利用するには、すべてのボリュームで圧縮を無効にします。

    Cloud Manager からボリュームを作成するときに Storage Efficiency を使用しないようにするか、ボリュームを作成してから実行するように選択します "CLI を使用してデータ圧縮を無効にします"。

Azure での Cloud Volumes ONTAP での Flash Cache の有効化

Flash Cache は、シングルノードシステムで Cloud Volumes ONTAP BYOL を使用してサポートされています。

手順

1. Azure で、単一ノードの Cloud Volumes ONTAP BYOL システムを使用した Standard_L8s_v2 VM タイプを選択します。
2. Flash Cache のパフォーマンス向上を利用するには、すべてのボリュームで圧縮を無効にします。

    Cloud Manager からボリュームを作成するときに Storage Efficiency を使用しないようにするか、ボリュームを作成してから実行するように選択します "CLI を使用してデータ圧縮を無効にします"。

AWS での Cloud Volumes ONTAP の起動

Cloud Volumes ONTAP は単一システム構成で起動することも、 AWS で HA ペアとして起動することもできます。

AWS Marketplace からのサブスクライブ

AWS Marketplace で登録して Cloud Volumes ONTAP の料金を支払うか、 Cloud Volumes ONTAP BYOL を導入できるようにします。

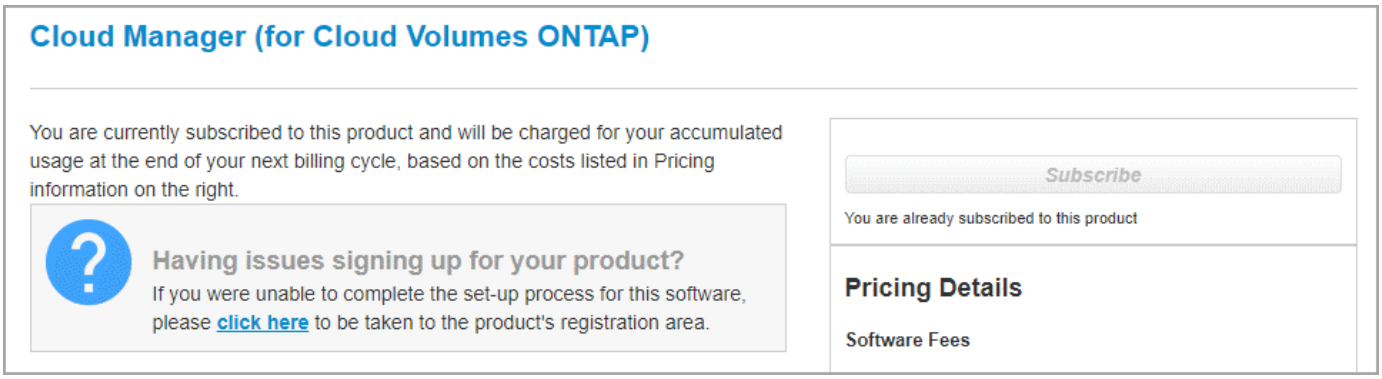
PAYGO のサブスクライブ

"AWS Marketplace でサブスクライブ" Cloud Volumes ONTAP の無償トライアルの終了後にサービスを中断しないようにするため。お客様が作成した Cloud Volumes ONTAP 9.6 以降の PAYGO システムと、有効にしたアドオン機能ごとに、このサブスクリプションから料金が請求されます。

次のビデオは、サブスクリプションプロセスを示しています。

▶ https://docs.netapp.com/ja-jp/occm37//media/video_subscribing_aws.mp4 *(video)*

> 複数の IAM ユーザが同じ AWS アカウントで作業する場合は、各ユーザにサブスクライブする必要があります。最初のユーザがサブスクライブしたあと、次の図に示すように、 AWS にはすでに登録されているユーザが表示されます。AWS アカウント用のサブスクリプションが作成されている間は、各 IAM ユーザが自分自身をサブスクリプションに関連付ける必要があります。以下のメッセージが表示された場合は、 * ここをクリック * リンクをクリックして Cloud Central にアクセスし、処理を完了してください。



BYOL のサブスクリプション

独自のライセンスを使用（ BYOL ）して Cloud Volumes ONTAP を起動する場合は、 "その後、 AWS Marketplace でそのサービスに登録する必要があります"。

"各 AWS Marketplace のページについては、こちらをご覧ください"。

AWS での単一クラウドボリューム ONTAP システムの起動

Cloud Volumes ONTAP を AWS で起動する場合は、 Cloud Manager で新しい作業環境を作成する必要があります。

作業を開始する前に

- 設定を選択し、管理者から AWS ネットワーク情報を取得して準備を完了しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP 構成を計画"。
- BYOL システムを起動する場合は、 20 桁のシリアル番号（ライセンスキー）が必要です。
- CIFS を使用する場合は、 DNS と Active Directory を設定しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP in AWS のネットワーク要件"。

このタスクについて

作業環境を作成した直後に、 Cloud Manager は指定された vPC でテストインスタンスを起動して接続を確認します。成功すると、 Cloud Manager はすぐにインスタンスを終了し、 Cloud Volumes ONTAP システムの

導入を開始します。Cloud Manager が接続を確認できない場合、作業環境の作成は失敗します。テストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシーの場合）のいずれかです。

手順

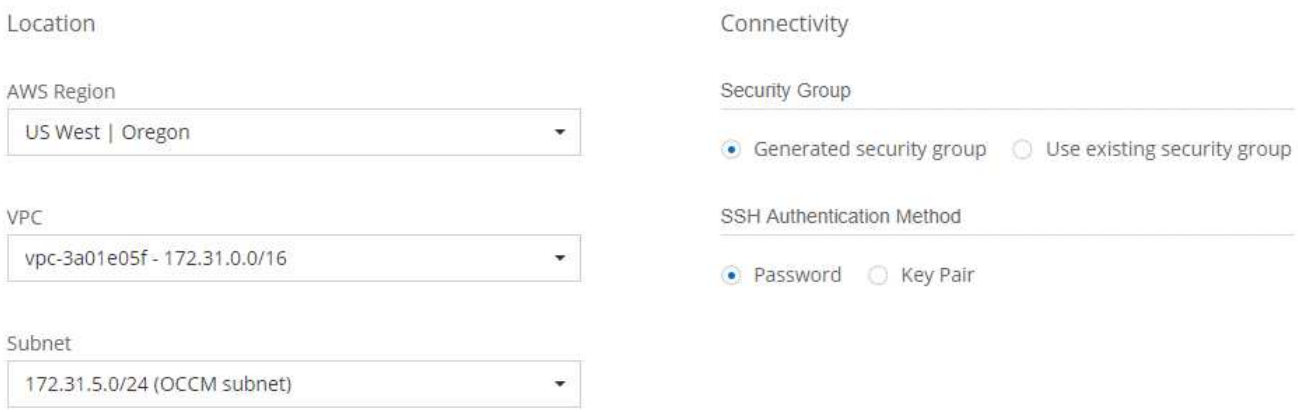
1. [作業環境] ページで、 [* Cloud Volumes ONTAP の作成 *] をクリックし、画面の指示に従います。
2. * 作業環境の定義 * ：「 * Amazon Web Services * 」と「 * Cloud Volumes ONTAP * 」を選択します。
3. * 詳細とクレデンシャル * ：必要に応じて、 AWS アカウントと Marketplace サブスクリプションを変更し、作業環境名を入力してタグを追加し、パスワードを入力します。

   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
アカウント：	別のアカウントを選択することもできます "Cloud Manager に AWS アカウントを追加しました"。
Marketplace サブスクリプション	課金される AWS アカウントを変更する場合は、別のサブスクリプションを選択してください。新しいサブスクリプションを追加するには "AWS Marketplace で提供されているサービスに移動します"。
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Amazon EC2 インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
タグを追加します	AWS タグは、 AWS リソースのメタデータです。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 AWS リソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
クレデンシャル	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。

4. * サービス *: この Cloud Volumes ONTAP システムで使用しない個々のサービスを有効または無効にしておきます。
   - "S3 へのバックアップに関する詳細情報"。
   - "Cloud Compliance の詳細はこちらをご覧ください"。
5. * Location & Connectivity * ： AWS のワークシートに記録したネットワーク情報を入力します。

   次の図は、入力済みのページを示しています。



6. * データ暗号化 * ：データ暗号化なし、または AWS で管理する暗号化を選択します。

   AWS で管理する暗号化の場合は、アカウントまたは別の AWS アカウントから別の Customer Master Key （ CMK ；カスタマーマスターキー）を選択できます。

   > Cloud Volumes ONTAP システムの作成後に AWS のデータ暗号化方式を変更することはできません。

   "Cloud 用の AWS KMS の設定方法については、こちらをご覧ください Volume ONTAP の略"。

   "サポートされている暗号化テクノロジの詳細を確認してください"。

7. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

   ライセンスの仕組みについては、を参照してください "ライセンス"。

   NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

8. * 構成済みパッケージ * ： Cloud Volumes ONTAP をすばやく起動するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

9. * IAM Role * ： Cloud Manager でロールを作成する場合は、デフォルトのオプションを使用してください。

   独自のポリシーを使用する場合は、それが満たされている必要があります "Cloud Volumes ONTAP ノードのポリシーの要件"。

10. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンス、インスタンスタイプ、インスタンステナンシーを選択します。

    インスタンスの起動後に必要な変更があった場合は、後でライセンスまたはインスタンスタイプを変更できます。

選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、 Cloud Volumes ONTAP 9.4 RC1 と 9.4 GA を選択した場合、更新が行われます。9.3 から 9.4 など、あるリリースから別のリリースへの更新は行われません。

11. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、 S3 の階層化を有効にするかどうかを指定します。

    ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

    ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

    ディスクの種類とサイズの選択については、を参照してください "AWS でのシステムのサイジング"。

12. * Write Speed & WORM * ：「 * Normal * 」または「 * High * write speed 」を選択し、必要に応じて Write Once 、 Read Many （ WORM ）ストレージをアクティブにします。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

13. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

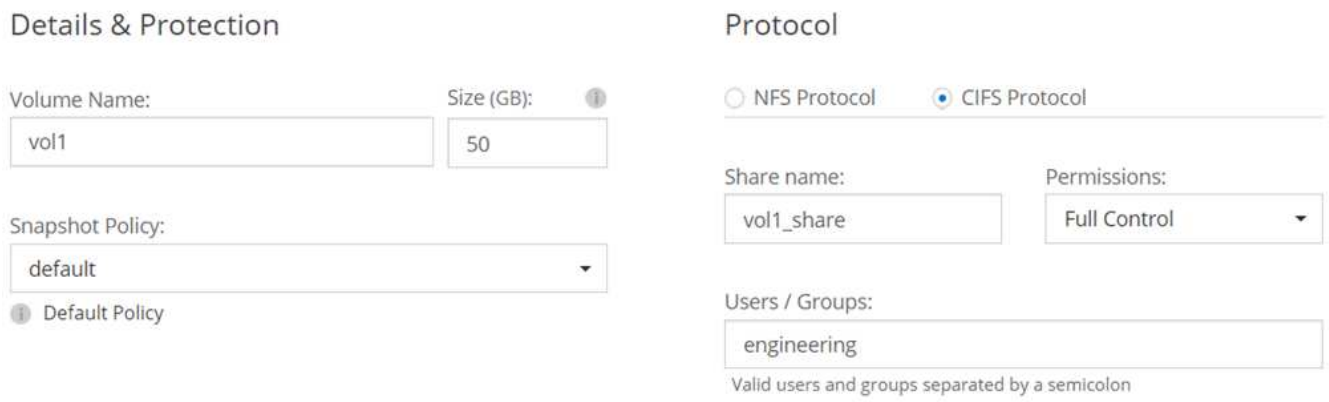
    iSCSI 用のボリュームを作成する場合は、この手順を省略できます。Cloud Manager では、 NFS と CIFS 専用のボリュームを設定します。

    このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。

フィールド	説明
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



14. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「 * OU=computers 、 OU=corp * 」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

15. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にするかどうかを選択し、 S3 階層化ポリシーを編集します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

16. * レビューと承認 *: 選択内容を確認して確認します。

    a. 設定の詳細を確認します。

    b. 詳細情報 * をクリックして、 Cloud Manager で購入するサポートと AWS リソースの詳細を確認します。

    c. [* I understand … * （理解しています … * ）] チェックボックスを選択

    d. [Go*] をクリックします。

結果

Cloud Manager が Cloud Volumes ONTAP インスタンスを起動します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP インスタンスの起動時に問題が発生した場合は、障害メッセージを確認してください。また、作業環境を選択して、 [環境の再作成] をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

AWS での Cloud Volumes ONTAP HA ペアの起動

Cloud Volumes ONTAP HA ペアを AWS で起動する場合は、 Cloud Manager で HA 作業環境を作成する必要があります。

作業を開始する前に

- 設定を選択し、管理者から AWS ネットワーク情報を取得して準備を完了しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP 構成を計画"。
- BYOL ライセンスを購入した場合は、ノードごとに 20 桁のシリアル番号（ライセンスキー）が必要です。
- CIFS を使用する場合は、 DNS と Active Directory を設定しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP in AWS のネットワーク要件"。

このタスクについて

作業環境を作成した直後に、 Cloud Manager は指定された vPC でテストインスタンスを起動して接続を確認します。成功すると、 Cloud Manager はすぐにインスタンスを終了し、 Cloud Volumes ONTAP システムの導入を開始します。Cloud Manager が接続を確認できない場合、作業環境の作成は失敗します。テストインスタンスは、 t2.nano （デフォルトの vPC テナンシーの場合）または m3.medium （専用の vPC テナンシー

の場合）のいずれかです。

手順

1. [作業環境] ページで、 [* Cloud Volumes ONTAP の作成 *] をクリックし、画面の指示に従います。
2. * 作業環境の定義 * ：「 * Amazon Web Services * 」と「 * Cloud Volumes ONTAP HA * 」を選択します。
3. * 詳細とクレデンシャル * ：必要に応じて、 AWS アカウントと Marketplace サブスクリプションを変更し、作業環境名を入力してタグを追加し、パスワードを入力します。

   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

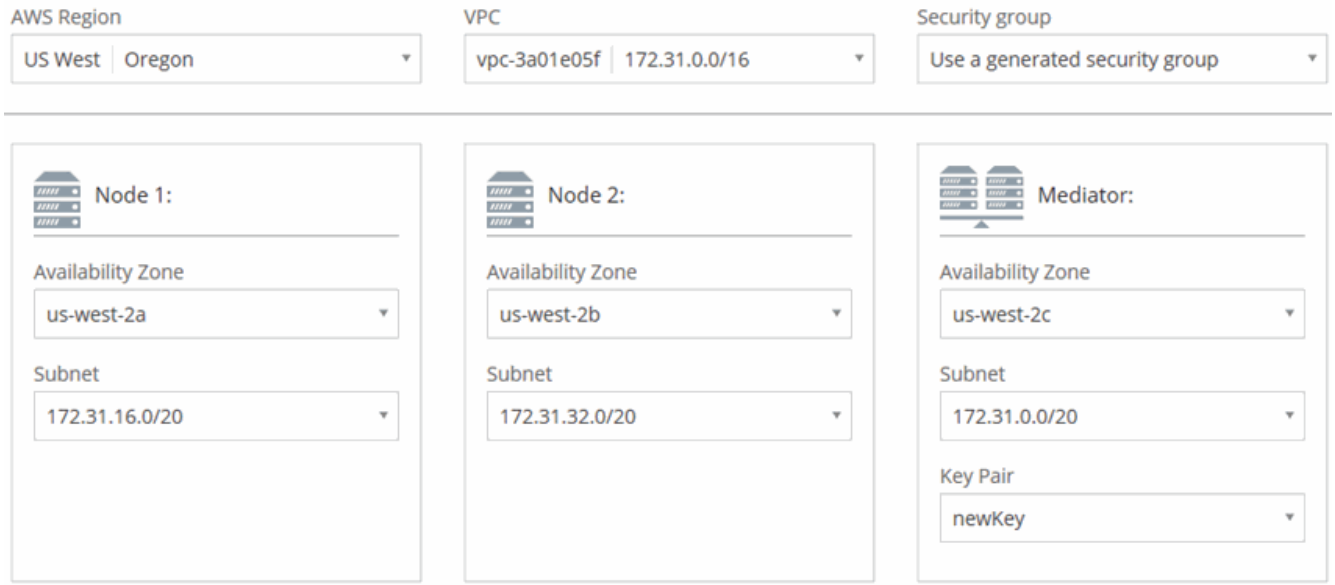
フィールド	説明
アカウント：	別のアカウントを選択することもできます "Cloud Manager に AWS アカウントを追加しました"。
Marketplace サブスクリプション	課金される AWS アカウントを変更する場合は、別のサブスクリプションを選択してください。新しいサブスクリプションを追加するには "AWS Marketplace で提供されているサービスに移動します"。
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Amazon EC2 インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
タグを追加します	AWS タグは、 AWS リソースのメタデータです。Cloud Manager は、 Cloud Volumes ONTAP インスタンスおよびインスタンスに関連付けられた各 AWS リソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "AWS ドキュメント：「 Tagging your Amazon EC2 Resources"。
クレデンシャル	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。

4. * サービス *: この Cloud Volumes ONTAP システムで使用しない個々のサービスを有効または無効にしておきます。
   - "S3 へのバックアップに関する詳細情報"。
   - "Cloud Compliance の詳細はこちらをご覧ください"。
5. *HA 導入モデル *: HA 構成を選択します。

   導入モデルの概要については、を参照してください "AWS での Cloud Volumes ONTAP HA"。

6. * Region & VPC * ： AWS ワークシートに記録したネットワーク情報を入力します。

   次の図は、複数の AZ 構成に対応するページを示しています。



7. * 接続と SSH 認証 * ： HA ペアとメディエーターの接続方法を選択します。
8. * フローティング IP * ：複数の AZ を選択した場合は、フローティング IP アドレスを指定します。

   IP アドレスは、その地域のすべての VPC の CIDR ブロックの外側にある必要があります。詳細については、を参照してください "複数の AZS での Cloud Volumes ONTAP HA の AWS ネットワーク要件"。

9. * ルートテーブル * ：複数の AZ を選択した場合は、フローティング IP アドレスへのルートを含むルーティングテーブルを選択します。

   複数のルートテーブルがある場合は、正しいルートテーブルを選択することが非常に重要です。そうしないと、一部のクライアントが Cloud Volumes ONTAP HA ペアにアクセスできない場合があります。ルーティングテーブルの詳細については、を参照してください "AWS のドキュメント：「 Route Tables"。

10. * データ暗号化 * ：データ暗号化なし、または AWS で管理する暗号化を選択します。

    AWS で管理する暗号化の場合は、アカウントまたは別の AWS アカウントから別の Customer Master Key （ CMK ；カスタマーマスターキー）を選択できます。

    Cloud Volumes ONTAP システムの作成後に AWS のデータ暗号化方式を変更することはできません。

    "Cloud 用の AWS KMS の設定方法については、こちらをご覧ください Volume ONTAP の略"。

    "サポートされている暗号化テクノロジの詳細を確認してください"。

11. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

    ライセンスの仕組みについては、を参照してください "ライセンス"。

    NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

12. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムをすばやく起動するには、パッケージを 1 つ

選択するか、 * 独自の構成を作成 * をクリックします。

いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

13. * IAM Role * ：デフォルトのオプションをそのまま使用し、 Cloud Manager で役割を作成する必要があります。

    独自のポリシーを使用する場合は、それが満たされている必要があります "Cloud Volumes ONTAP ノードと HA のポリシー要件 メディエーター"。

14. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンス、インスタンスタイプ、インスタンステナンシーを選択します。

    インスタンスの起動後に必要な変更があった場合は、後でライセンスまたはインスタンスタイプを変更できます。

    > 選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、 Cloud Volumes ONTAP 9.4 RC1 と 9.4 GA を選択した場合、更新が行われます。9.3 から 9.4 など、あるリリースから別のリリースへの更新は行われません。

15. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、 S3 の階層化を有効にするかどうかを指定します。

    ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

    ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

    ディスクの種類とサイズの選択については、を参照してください "AWS でのシステムのサイジング"。

16. * WORM * ：必要に応じて、 Write Once Read Many （ WORM ）ストレージをアクティブにします。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

17. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

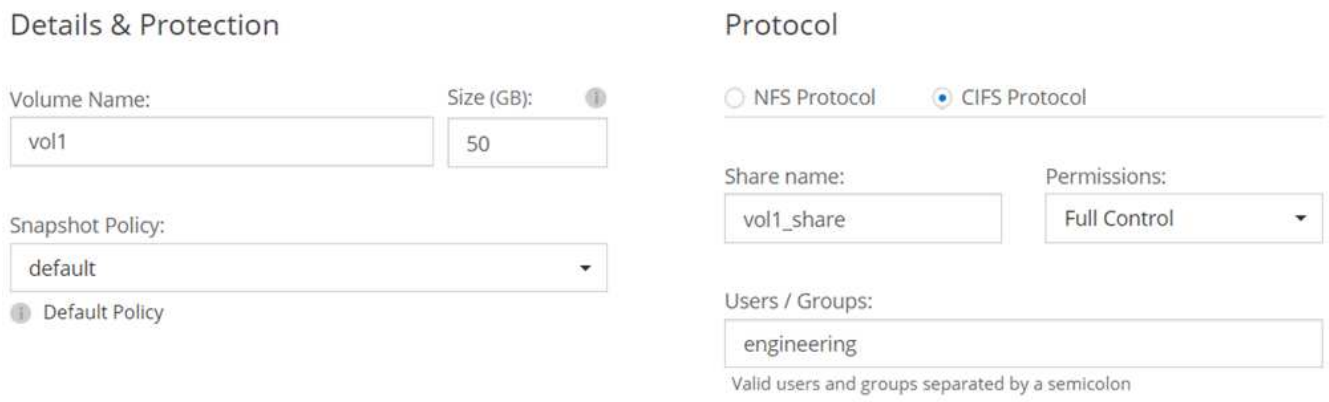
    iSCSI 用のボリュームを作成する場合は、この手順を省略できます。Cloud Manager では、 NFS と CIFS 専用のボリュームを設定します。

    このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。

フィールド	説明
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



18. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

フィールド	説明
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「 * OU=computers 、OU=corp * 」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

19. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にするかどうかを選択し、 S3 階層化ポリシーを編集します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

20. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. 詳細情報 * をクリックして、 Cloud Manager で購入するサポートと AWS リソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

Cloud Manager が Cloud Volumes ONTAP HA ペアを起動します。タイムラインで進行状況を追跡できます。

HA ペアの起動で問題が発生した場合は、障害メッセージを確認します。また、作業環境を選択して、 [環境の再作成] をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

Azure で Cloud Volumes ONTAP を起動します

Cloud Manager で Cloud Volumes ONTAP の作業環境を作成することで、 Azure で単一ノードシステムまたは HA ペアを起動できます。

作業を開始する前に

- Azure アカウントに必要な権限があることを確認してください。特に、以前のリリースからアップグレードし、初めて HA システムを導入する場合には、十分です。

  最新の権限はにあります "Azure 向けの NetApp Cloud Central ポリシー"。

- 設定を選択し、ネットワーク管理者から Azure ネットワーク情報を入手しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP 構成を計画"。
- BYOL システムを導入するには、ノードごとに 20 桁のシリアル番号（ライセンスキー）が必要です。

このタスクについて

Azure で Cloud Volumes ONTAP システムを作成すると、リソースグループ、ネットワークインターフェイス、ストレージアカウントなどの Azure オブジェクトがいくつか作成されます。ウィザードの最後にあるリソースの概要を確認できます。

手順

1. [作業環境] ページで、 [* Cloud Volumes ONTAP の作成 *] をクリックし、画面の指示に従います。
2. * 作業環境の定義 * ：「 * Microsoft Azure * 」を選択し、シングルノードまたは HA ペアを選択します。
3. * 詳細とクレデンシャル * ：必要に応じて Azure アカウントまたはサブスクリプションを変更し、クラスタ名とリソースグループ名を指定し、必要に応じてタグを追加してから、クレデンシャルを指定します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
アカウントを切り替えます	必要に応じて、別のアカウントまたはサブスクリプションを選択できます "設定して Cloud Manager に追加"。
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Azure 仮想マシンの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
リソースグループ名	[デフォルトを使用する *] をオフにした場合は、新しいリソースグループの名前を入力できます。既存のリソースグループを使用する場合は、 API を使用する必要があります。
タグ	タグは、 Azure リソースのメタデータです。Cloud Manager は、 Cloud Volumes ONTAP システムおよびシステムに関連付けられた各 Azure リソースにタグを追加します。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "Microsoft Azure のドキュメント：「 Using tags to organize your Azure resources"。
クレデンシャル	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。

4. * サービス * ：クラウドコンプライアンスを有効にしておくか、この Cloud Volumes ONTAP システムで使用しない場合は無効にします。

   "Cloud Compliance の詳細はこちらをご覧ください"。

5. * 場所と接続 * ：場所とセキュリティグループを選択し、チェックボックスを選択して Cloud Manager とターゲットの場所の間のネットワーク接続を確認します。
6. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

   ライセンスの仕組みについては、を参照してください "ライセンス"。

   NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

7. * 事前構成されたパッケージ *: パッケージの 1 つをシェル化して Cloud Volumes ONTAP システムを迅速に配備するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

8. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンスを選択して、仮想マシンのタイプを選択します。

   システムの起動後に必要な変更があった場合は、後でライセンスまたは仮想マシンのタイプを変更できます。

   > 選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、 Cloud Volumes ONTAP 9.5 RC1 と 9.5 GA を選択した場合、更新が行われます。あるリリースから別のリリース（ 9.4 から 9.5 など）への更新は行われません。

9. * Azure Marketplace からサブスクライブ * ： Cloud Manager で Cloud Volumes ONTAP のプログラムによる導入を有効にできなかった場合は、以下の手順に従ってください。
10. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、 BLOB ストレージへのデータ階層化を有効にするかどうかを指定します。

    ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

    ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

    ディスクの種類とサイズの選択については、を参照してください "Azure でのシステムのサイジング"。

11. * Write Speed & WORM * ：「 * Normal * 」または「 * High * write speed 」を選択し、必要に応じて Write Once 、 Read Many （ WORM ）ストレージをアクティブにします。

    > 書き込み速度の選択はシングルノードシステムでのみサポートされます。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

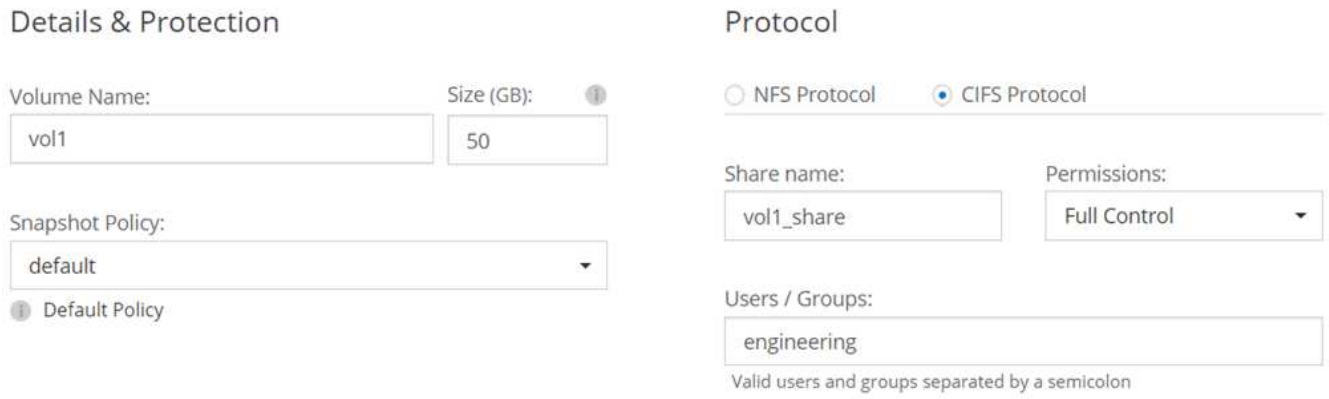
12. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

iSCSI を使用する場合は、この手順を省略してください。Cloud Manager では、 NFS および CIFS 専用のボリュームを作成できます。

このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



13. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。

フィールド	説明
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD ドメインサービスを Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=AADDC computers* 」または「 * OU=AADDC Users* 」と入力します。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

14. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にして階層化ポリシーを変更するかどうかを選択します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

15. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. 詳細情報 * をクリックして、 Cloud Manager で購入するサポートと Azure リソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

Cloud Manager は Cloud Volumes ONTAP システムを導入します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

GCP での Cloud Volumes ONTAP の起動

GCP では、作業環境を作成することで、シングルノードの Cloud Volumes ONTAP システムを起動できます。

作業を開始する前に

- 構成を選択し、管理者から GCP ネットワーキング情報を入手しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP 構成を計画"。
- BYOL システムを導入するには、ノードごとに 20 桁のシリアル番号（ライセンスキー）が必要です。

手順

1. [[subscribe]] 作業環境ページで、 * Cloud Volumes ONTAP の作成 * をクリックし、プロンプトに従います。
2. * 作業環境の定義 : [続行 *] をクリックします。
3. * Cloud Volumes ONTAP * を購読する：プロンプトが表示されたら、 GCP Marketplace で Cloud Volumes ONTAP に登録します。

   次のビデオは、サブスクリプションプロセスを示しています。

   ► https://docs.netapp.com/ja-jp/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. * 詳細とクレデンシャル * ：プロジェクトを選択し、クラスタ名を指定し、必要に応じてラベルを追加して、クレデンシャルを指定します。

   次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
Google Cloud プロジェクト	Cloud Volumes ONTAP を配置するプロジェクトを選択します。デフォルトプロジェクトは、 Cloud Manager が配置されているプロジェクトです。 ドロップダウンリストにプロジェクトが表示されない場合は、 Cloud Manager サービスアカウントを他のプロジェクトに関連付けていません。Google Cloud コンソールに移動し、 IAM サービスを開き、プロジェクトを選択します。Cloud Manager ロールが割り当てられたサービスアカウントをそのプロジェクトに追加します。プロジェクトごとにこの手順を繰り返す必要があります。 これは Cloud Manager 用に設定するサービスアカウントです。 "このページの手順 4b で説明しているように"。
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと GCP VM インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。

フィールド	説明
ラベルを追加します	ラベルは GCP リソースのメタデータです。Cloud Manager によって、システムに関連付けられた Cloud Volumes ONTAP システムと GCP リソースにラベルが追加されます。作業環境の作成時にユーザインターフェイスからラベルを 4 つまで追加し、その後追加することができます。API では、作業環境の作成時にラベルを 4 つに制限することはありません。ラベルの詳細については、を参照してください "Google Cloud のドキュメント：「 Labeling Resources"。
クレデンシャル	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。このクレデンシャルを使用して、 System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。

5. * 場所と接続性 * ：場所を選択し、ファイアウォールポリシーを選択して、データ階層化のための Google Cloud ストレージへのネットワーク接続を確認するチェックボックスを選択します。

   コールドデータを Google Cloud Storage バケットに階層化する場合は、 Cloud Volumes ONTAP が配置されているサブネットをプライベート Google アクセス用に構成する必要があります。手順については、を参照してください "Google Cloud のドキュメント：「 Configuring Private Google Access"。

6. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

   ライセンスの仕組みについては、を参照してください "ライセンス"。

   NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

7. * 構成済みパッケージ * ： Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、 * 独自の構成を作成 * をクリックします。

   いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

8. * ライセンス * ：必要に応じて Cloud Volumes ONTAP のバージョンを変更し、ライセンスを選択して、仮想マシンのタイプを選択します。

   システムの起動後に必要な変更があった場合は、後でライセンスまたは仮想マシンのタイプを変更できます。

   > 選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、 Cloud Volumes ONTAP 9.5 RC1 と 9.5 GA を選択した場合、更新が行われます。あるリリースから別のリリース（ 9.4 から 9.5 など）への更新は行われません。

9. * 基盤となるストレージリソース * ：初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、データの階層化を有効にするかどうかを指定します。

   ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。

   ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced

Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

ディスクの種類とサイズの選択については、を参照してください "GCP でシステムのサイジングを行う"。

10. * Write Speed & WORM * ：「 * Normal * 」または「 * High * write speed 」を選択し、必要に応じて Write Once 、 Read Many （ WORM ）ストレージをアクティブにします。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

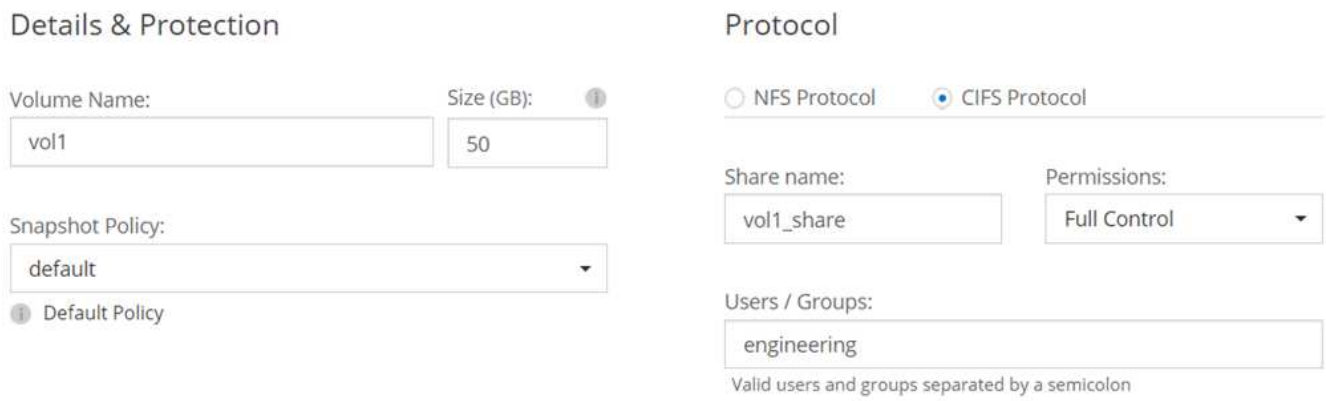
11. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

    iSCSI を使用する場合は、この手順を省略してください。Cloud Manager では、 NFS および CIFS 専用のボリュームを作成できます。

    このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

次の図は、 CIFS プロトコルの [Volume] ページの設定を示しています。



12. * CIFS セットアップ * ： CIFS プロトコルを選択した場合は、 CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

13. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ：必要に応じて、 Storage Efficiency 機能を有効にして階層化ポリシーを変更するかどうかを選択します。

    詳細については、を参照してください "ボリューム使用率プロファイルについて" および "データ階層化の概要"。

14. * データ階層化用 Google Cloud Platform アカウント * ： Google Cloud Platform アカウントに相互運用可能なストレージアクセスキーを提供して、データ階層化を設定します。データ階層化を無効にするには、 * Skip * をクリックします。

    これらのキーを使用して、 Cloud Manager でデータ階層化用の Cloud Storage バケットを設定できます。詳細については、を参照してください "GCP アカウントのセットアップと Cloud Manager への追加"。

15. * レビューと承認 *: 選択内容を確認して確認します。
    a. 設定の詳細を確認します。
    b. [詳細情報 * （ More information * ）] をクリックして、 Cloud Manager が購入するサポートと GCP リソースの詳細を確認します。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

結果

Cloud Manager は Cloud Volumes ONTAP システムを導入します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、 * 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください "NetApp Cloud Volumes ONTAP のサポート"。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、 System Manager または CLI を使用します。

  クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

従量課金制システムの登録

ネットアップによるサポートは Cloud Volumes ONTAP Explore 、 Standard 、および Premium システムに含まれていますが、先にシステムをネットアップに登録してサポートを有効にする必要があります。

手順

1. Cloud Manager にネットアップサポートサイトのアカウントをまだ追加していない場合は、「 * Account Settings * 」に移動して追加します。

   "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

2. [作業環境] ページで、登録するシステムの名前をダブルクリックします。
3. メニューアイコンをクリックし、 * Support registration registration * （サポート登録 * ）をクリックします。

4. ネットアップサポートサイトのアカウントを選択し、 * 登録 * をクリックします。

結果

Cloud Manager によってシステムがネットアップに登録されます。

Cloud Volumes ONTAP のセットアップ

Cloud Volumes ONTAP を導入したら、 NTP を使用してシステム時刻を同期し、 System Manager または CLI からオプションのタスクをいくつか実行してセットアップできます。

タスク	説明
NTP を使用してシステム時刻を同期します	NTP サーバを指定すると、ネットワーク内のシステム間で時刻が同期されるため、時刻の違いによる問題の回避に役立ちます。 Cloud Manager API を使用するか、 CIFS サーバのセットアップ時にユーザインターフェイスから NTP サーバを指定します。 • "CIFS サーバの変更" • "Cloud Manager API 開発者ガイド" たとえば、 AWS のシングルノードシステム用の API は次のようになります。 POST /vsa/working-environments/{workingEnvironmentId}/ntp Setup NTP server. Operation may only be performed on working environments whose status is: ON, DEGRADED. Parameters Parameter | Value | Description | Parameter Type | Data Type workingEnvironmentId | | Public Id of working environment | path | string body | (required) | NTP Configuration request | body | Model | Model Schema NTPConfigurationRequest { ntpServer (string): NTPS server } Parameter content type: application/json Try it out!

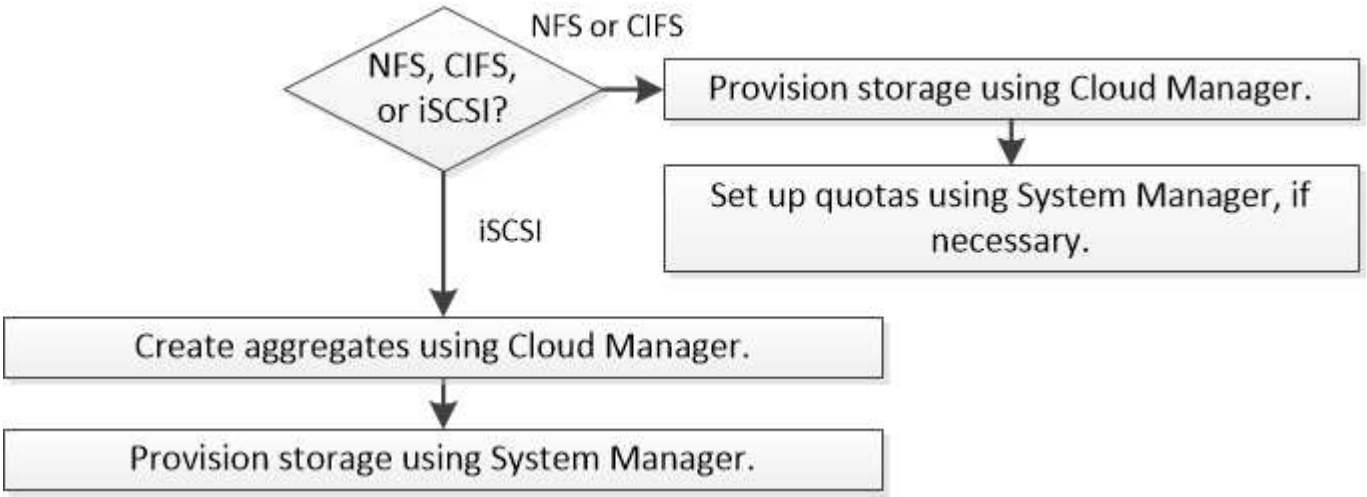
タスク	説明
オプション： AutoSupport を設定します	AutoSupport は、システムの状態をプロアクティブに監視し、デフォルトでメッセージをネットアップのテクニカルサポートに自動的に送信します。インスタンスを起動する前にアカウント管理者がプロキシサーバを Cloud Manager に追加していた場合、 Cloud Volumes ONTAP はそのプロキシサーバを AutoSupport メッセージに使用するように設定されます。AutoSupport をテストして、メッセージを送信できることを確認する必要があります。手順については、 System Manager のヘルプまたはを参照してください "ONTAP 9 システムアドミニストレーションリファレンス"。
オプション： EMS を設定します	イベント管理システム（ EMS ）は、 Cloud Volumes ONTAP システムで発生したイベントに関する情報を収集して表示します。イベント通知を受信するには、イベントの宛先（電子メールアドレス、 SNMP トラップホスト、または syslog サーバ）とイベントのルートを特定のイベントの重大度に設定します。EMS は CLI を使用して設定できます。手順については、を参照してください "ONTAP 9 EMS 構成エクスプレスガイド"。
オプション：複数の AWS アベイラビリティゾーンに HA システムの SVM 管理ネットワークインターフェイス（ LIF ）を作成する	SnapCenter または SnapDrive for Windows を HA ペアで使用する場合は、Storage Virtual Machine （ SVM ） Management Network Interface （ LIF ）が必要です。複数の AWS アベイラビリティゾーンで HA ペアを使用する場合は、 SVM 管理 LIF で _floating_ip アドレスを使用する必要があります。 HA ペアの起動時に、フローティング IP アドレスを指定するように求められます。IP アドレスを指定しなかった場合は、 System Manager または CLI から SVM 管理 LIF を自分で作成できます。次に、 CLI から LIF を作成する例を示します。 `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
オプション：設定ファイルのバックアップ場所を変更します	Cloud Volumes ONTAP は、適切に動作するために必要な設定可能なオプションに関する情報を含む構成バックアップファイルを自動的に作成します。デフォルトでは、 Cloud Volumes ONTAP は 8 時間ごとにファイルを Cloud Manager ホストにバックアップします。バックアップを別の場所に送信する場合は、データセンターまたは AWS 内の FTP または HTTP サーバにバックアップの場所を変更できます。たとえば、 FAS ストレージシステムのバックアップ場所がすでにあるとします。バックアップの場所は、CLI を使用して変更できます。を参照してください "ONTAP 9 システムアドミニストレーションリファレンス"。

ストレージのプロビジョニング

ストレージのプロビジョニング

ボリュームとアグリゲートを管理することで、 Cloud Volumes ONTAP システム用の追加の NFS ストレージと CIFS ストレージを Cloud Manager からプロビジョニングできます。iSCSI ストレージを作成する必要がある場合は、 System Manager から作成する必要があります。

> すべてのディスクとアグリゲートは、 Cloud Manager から直接作成および削除する必要があります。これらのアクションは、別の管理ツールから実行しないでください。これにより、システムの安定性が低下し、将来ディスクを追加できなくなる可能性があります。また、クラウドプロバイダの冗長料金が発生する可能性もあります。



FlexVol ボリュームの作成

Cloud Volumes ONTAP システムの起動後にストレージの追加が必要になった場合は、 Cloud Manager から NFS または CIFS 用の新しい FlexVol ボリュームを作成できます。

作業を開始する前に

AWS で CIFS を使用する場合は、 DNS と Active Directory を設定しておく必要があります。詳細については、を参照してください "Cloud Volumes ONTAP for AWS のネットワーク要件"。

手順

1. 作業環境のページで、 FlexVol ボリュームをプロビジョニングする Cloud Volumes ONTAP システムの名前をダブルクリックします。
2. アグリゲートまたは特定のアグリゲートに新しいボリュームを作成します。

アクション	手順
新しいボリュームを作成し、Cloud Manager に包含アグリゲートを選択させます	[新しいボリュームの追加] をクリックします。

アクション	手順
特定のアグリゲートに新しいボリュームを作成します	a. メニューアイコンをクリックし、 [* 詳細設定] 、 [詳細な割り当て *] の順にクリックします。 b. アグリゲートのメニューをクリックします。 c. [ボリュームの作成] をクリックします。

3. 新しいボリュームの詳細を入力し、 * Continue * をクリックします。

   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

4. CIFS プロトコルを選択し、 CIFS サーバがセットアップされていない場合は、 Create a CIFS Server （ CIFS サーバの作成）ダイアログボックスでサーバの詳細を指定し、 * Save and continue * をクリックします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

フィールド	説明
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。 • AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=computers 、 OU=corp * 」と入力します。 • Azure AD ドメインサービスを Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=AADDC computers* 」または「 * OU=AADDC Users* 」と入力します。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

5. Usage Profile 、 Disk Type 、および Tiering Policy ページで、 Storage Efficiency 機能を有効にするかどうかを選択し、ディスクタイプを選択し、必要に応じて階層化ポリシーを編集します。

   ヘルプについては、次のトピックを参照してください。

   - "ボリューム使用率プロファイルについて"
   - "AWS でのシステムのサイジング"
   - "Azure でのシステムのサイジング"
   - "データ階層化の概要"

6. [Go*] をクリックします。

結果

Cloud Volumes ONTAP がボリュームをプロビジョニングします。

完了後

CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。

ボリュームにクォータを適用する場合は、 System Manager または CLI を使用する必要があります。クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

HA の 2 つ目のノードでの FlexVol ボリュームの作成 設定

デフォルトでは、 Cloud Manager は HA 構成の最初のノードにボリュームを作成します。両方のノードがクライアントにデータを提供するアクティブ / アクティブ構成が必要な場合は、 2 番目のノードにアグリゲート

とボリュームを作成する必要があります。

手順

1. [作業環境（ Working Environments ）] ページで、アグリゲートを管理する Cloud Volumes ONTAP 作業環境の名前をダブルクリックします。
2. メニューアイコンをクリックし、 [* 詳細設定] > [高度な割り当て *] をクリックします。
3. Add Aggregate * をクリックして、アグリゲートを作成します。
4. Home Node には、 HA ペアの 2 番目のノードを選択します。
5. Cloud Manager でアグリゲートが作成されたら、そのアグリゲートを選択して * ボリュームの作成 * をクリックします。
6. 新しいボリュームの詳細を入力し、 * Create * をクリックします。

完了後

必要に応じて、このアグリゲートに追加のボリュームを作成できます。

> 複数の AWS アベイラビリティゾーンに HA ペアを導入する場合は、ボリュームが配置されているノードのフローティング IP アドレスを使用してボリュームをクライアントにマウントする必要があります。

アグリゲートの作成

アグリゲートは、自分で作成することも、 Cloud Manager でボリュームを作成するときに作成することもできます。アグリゲートを手動で作成することのメリットは、基盤となるディスクサイズを選択して、必要な容量またはパフォーマンスに合わせてアグリゲートをサイジングできることです。

手順

1. [Working Environments] ページで、アグリゲートを管理する Cloud Volumes ONTAP インスタンスの名前をダブルクリックします。
2. メニューアイコンをクリックし、 [* 詳細設定] 、 [詳細な割り当て *] の順にクリックします。
3. Add Aggregate * をクリックして、アグリゲートの詳細を指定します。

   ディスクタイプとディスクサイズについては、を参照してください "構成の計画"。

4. [* Go *] をクリックし、 [* 承認して購入 *] をクリックします。

iSCSI LUN のプロビジョニング

iSCSI LUN を作成する場合は、 System Manager から作成する必要があります。

作業を開始する前に

- ホストユーティリティは、 LUN に接続するホストにインストールしてセットアップする必要があります。
- ホストから iSCSI イニシエータ名を記録しておく必要があります。この名前は、 LUN の igroup を作成するときに指定する必要があります。
- System Manager でボリュームを作成する前に、十分なスペースを持つアグリゲートがあることを確認する必要があります。Cloud Manager でアグリゲートを作成する必要があります。詳細については、を参照

してください "アグリゲートの作成"。

このタスクについて

ここでは、 System Manager for Version 9.3 以降の使用方法について説明します。

手順

1. "System Manager にログインします。"。
2. [*Storage] > [LUNs] をクリックします。
3. 「 * Create * 」をクリックし、プロンプトに従って LUN を作成します。
4. ホストから LUN に接続します。

   手順については、を参照してください "Host Utilities のマニュアル" オペレーティングシステムに応じて提供されます。

FlexCache ボリュームを使用してデータアクセスを高速化する

FlexCache ボリュームは、元の（またはソース）ボリュームから NFS 読み取りデータをキャッシュするストレージボリュームです。その後キャッシュされたデータを読み取ることで、そのデータへのアクセスが高速になります。

FlexCache を使用すると、データアクセスを高速化したり、アクセス頻度の高いボリュームのトラフィック負荷を軽減したりできます。FlexCache ボリュームを使用すると、元のボリュームにアクセスせずに直接データを使用できるため、特にクライアントが同じデータに繰り返しアクセスする場合に、パフォーマンスの向上に役立ちます。FlexCache ボリュームは、読み取り処理が大量に発生するシステムワークロードに適しています。

現時点では、 Cloud Manager で FlexCache ボリュームを管理することはできませんが、 FlexCache CLI または ONTAP System Manager を使用して、 ONTAP ボリュームを作成および管理できます。

- "『 FlexCache Volumes for Faster Data Access Power Guide 』を参照してください"
- "System Manager での FlexCache ボリュームの作成"

3.7.2 リリース以降、 Cloud Manager はすべての新しい Cloud Volumes ONTAP システムに対して FlexCache ライセンスを生成します。ライセンスの使用量は 500GB に制限されています。

> ライセンスを生成するには、 Cloud Manager から https://ipa-signer.cloudmanager.netapp.com にアクセスする必要があります。この URL にファイアウォールからアクセスできることを確認してください。

使用頻度の低いデータを低コストのオブジェクトストレージに階層化

ホットデータ用の SSD または HDD のパフォーマンス階層と、アクセス頻度の低いデータ用のオブジェクトストレージの大容量階層を組み合わせることで、ストレージコストを削減できます。概要については、を参照してください "データ階層化の概要"。

データ階層化を設定するには、次の手順を実行するだけです。

1 サポートされている構成を選択します

ほとんどの構成がサポートされています。最新バージョンを実行している Cloud Volumes ONTAP Standard 、 Premium 、または BYOL システムがある場合は、この方法を推奨します。 "詳細はこちら。"。

2 **Cloud Volumes ONTAP** とオブジェクトストレージ間の接続を確認します

- AWS では、 S3 への VPC エンドポイントが必要です。 詳細はこちら。。
- Azure では、 Cloud Manager に必要な権限が付与されていれば何も実行する必要はありません。 詳細はこちら。。
- GCP の場合、 Cloud Manager に GCP アカウントを追加し、プライベート Google アクセス用のサブネットを設定する必要があります。 詳細はこちら。。

3 ボリュームを作成、変更、またはレプリケートするときに階層化ポリシーを選択します

ボリュームを作成、変更、またはレプリケートするときに、 Cloud Manager から階層化ポリシーを選択するよう求められます。

- "読み取り / 書き込みボリュームでのデータの階層化"
- "データ保護ボリューム上のデータの階層化"

> データ階層化に不要なもの
>
> - データの階層化を有効にするために機能ライセンスをインストールする必要はありません。
> - 大容量階層（ S3 バケット、 Azure BLOB コンテナ、 GCP バケット）を作成する必要はありません。クラウドマネージャーがそれを実現します。

データ階層化をサポートする構成

特定の構成と機能を使用する場合は、データ階層化を有効にできます。

- データ階層化は、次のバージョン以降、 Cloud Volumes ONTAP の Standard 、 Premium 、および BYOL でサポートされます。
  - AWS でバージョン 9.2 を実行します
  - Azure のシングルノードシステムの場合はバージョン 9.4
  - Azure バージョン 9.6 （ HA ペアを使用）
  - GCP のバージョン 9.6

    > データ階層化は、 DS3_v2 仮想マシンタイプの Azure ではサポートされていません。

- AWS では、パフォーマンス階層は汎用 SSD 、プロビジョニングされた IOPS SSD 、スループットに最適化された HDD のいずれかになります。
- Azure では、 Premium SSD Managed Disks 、 Standard SSD Managed Disks 、 Standard HDD Managed Disks のいずれかです。
- GCP では、 SSD または HDD （標準ディスク）のどちらかです。
- データ階層化は暗号化テクノロジでサポートされています。
- ボリュームでシンプロビジョニングを有効にする必要があります。

コールドデータを **AWS S3** に階層化するための要件

Cloud Volumes ONTAP が S3 に接続されていることを確認します。この接続を提供する最善の方法は、 S3 サービスへの vPC エンドポイントを作成することです。手順については、を参照してください "AWS のドキュメント：「 Creating a Gateway Endpoint"。

vPC エンドポイントを作成するときは、 Cloud Volumes ONTAP インスタンスに対応するリージョン、 vPC 、およびルートテーブルを必ず選択してください。S3 エンドポイントへのトラフィックを有効にする発信 HTTPS ルールを追加するには、セキュリティグループも変更する必要があります。そうしないと、 Cloud

Volumes ONTAP は S3 サービスに接続できません。

問題が発生した場合は、を参照してください "AWS のサポートナレッジセンター：ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか。"。

コールドデータを Azure BLOB ストレージに階層化するための要件

必要な権限が Cloud Manager に割り当てられていれば、パフォーマンス階層と大容量階層の間に接続を設定する必要はありません。Cloud Manager ポリシーに以下の権限が設定されている場合、 Cloud Manager は VNet サービスエンドポイントを有効にします。

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

権限は最新のに含まれています "Cloud Manager ポリシー"。

コールドデータを Google Cloud Storage に階層化するための要件 バケット

- サービスアカウントのストレージアクセスキーを入力して、 Cloud Manager に Google Cloud Platform アカウントを追加する必要があります。これらのキーを使用して、 Cloud Manager でデータ階層化用の Cloud Storage バケットを設定できます。手順については、を参照してください "GCP アカウントのセットアップと Cloud Manager への追加"。
- Cloud Volumes ONTAP が存在するサブネットは、プライベート Google アクセス用に設定する必要があります。手順については、を参照してください "Google Cloud のドキュメント：「 Configuring Private Google Access"。

読み取り / 書き込みボリュームのデータの階層化

Cloud Volumes ONTAP は、読み書き可能なボリューム上にあるアクセス頻度の低いデータを対費用効果の高いオブジェクトストレージに階層化して、ホットデータ用に高パフォーマンス階層を解放できます。

手順

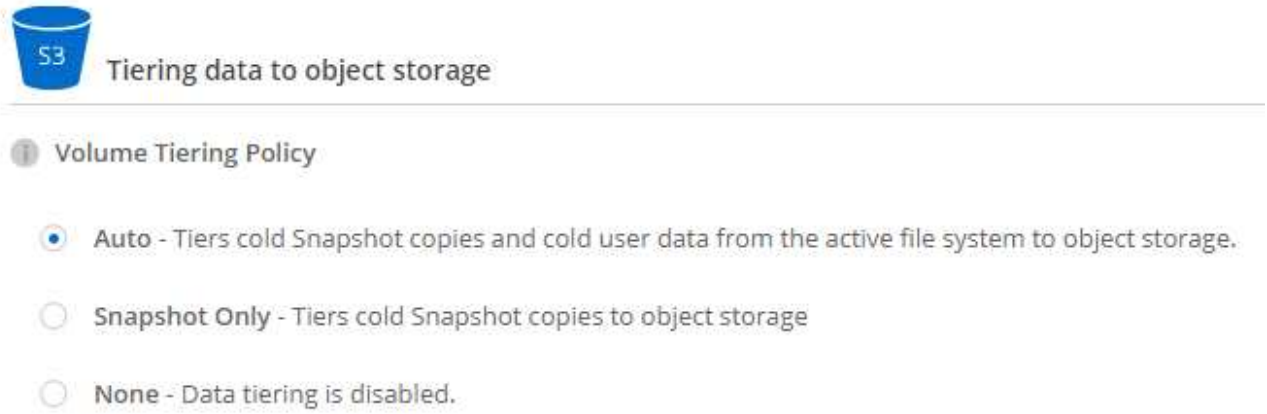
1. 作業環境で、新しいボリュームを作成するか、既存のボリュームの階層を変更します。

タスク	アクション
新しいボリュームを作成します	[新しいボリュームの追加] をクリックします。
既存のボリュームを変更します	ボリュームを選択し、 * ディスクタイプと階層化ポリシーの変更 * をクリックします。

2. スナップショットのみのポリシーまたは自動ポリシーを選択します。

   これらのポリシーの説明については、を参照してください "データ階層化の概要"。

   - 例 *



データ階層化対応のアグリゲートがまだ存在しない場合、 Cloud Manager はボリュームの新しいアグリゲートを作成します。

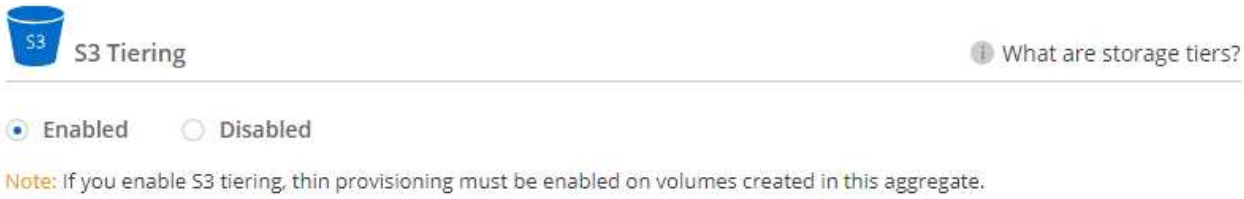
アグリゲートを自分で作成する場合は、アグリゲートを作成するときにアグリゲートでデータ階層化を有効にできます。

データ保護ボリュームのデータを階層化する

Cloud Volumes ONTAP では、データ保護ボリュームから容量階層にデータを階層化できます。デスティネーションボリュームをアクティブにすると、データは読み取られた時点でパフォーマンス階層に徐々に移動します。

手順

1. [作業環境] ページで、ソースボリュームを含む作業環境を選択し、ボリュームをレプリケートする作業環境にドラッグします。
2. 画面の指示に従って、階層化ページに移動し、オブジェクトストレージへのデータ階層化を有効にします。
    - 例 *



データの複製については、を参照してください "クラウドとの間でデータをレプリケートする"。

AWS または Azure で階層化レベルを変更する

データの階層化を有効にすると、 Cloud Volumes ONTAP は、アクセス頻度の低いデータを AWS の S3_Standard_storage クラスまたは Azure の _hot_storage 階層に階層化します。Cloud Volumes ONTAP を導入したら、アクセスされていないアクセス頻度の低いデータの階層化レベルを 30 日間変更することで、ストレージコストを削減できます。データにアクセスする場合はアクセスコストが高くなるため、階層化レベル

を変更する前に、アクセスコストを考慮する必要があります。

> 現在、 _Regional _storage クラスのみがサポートされているため、 GCP で階層化レベルを変更することはできません。

このタスクについて

階層化レベルはシステム全体で使用され、ボリュームごとではありません。

AWS では、非アクティブなデータが 30 日後に次のいずれかのストレージクラスに移動するように階層化レベルを変更できます。

- インテリジェントな階層化
- 標準的なアクセス頻度は低い
- 1 回のアクセスではほとんど発生しません

Azure では、非アクティブ期間が 30 日を経過したときにアクセス頻度の低いデータを _coal_storage 階層に移動するように階層化レベルを変更できます。

階層化レベルの仕組みの詳細については、を参照してください "データ階層化の概要"。

手順

1. 作業環境で、メニューアイコンをクリックし、 * S3 ストレージクラス * または * BLOB ストレージの階層化 * をクリックします。
2. 階層化レベルを選択し、 * Save * をクリックします。

Kubernetes 用の永続的ストレージとしての ONTAP の使用

Cloud Manager では、の導入を自動化できます "NetApp Trident" Kubernetes クラスタでは、コンテナ用の永続的ストレージとして ONTAP を使用できます。これは、 Cloud Volumes ONTAP クラスタとオンプレミスの ONTAP クラスタで機能します。

これらの手順を完了する前に、を実行する必要があります "Cloud Volumes ONTAP システムを作成します" または "オンプレミスの ONTAP クラスタを検出" をクリックします。

を使用して Kubernetes クラスタを導入する場合 "NetApp Kubernetes Service の略"を使用すると、 Cloud Manager は NetApp Cloud Central アカウントからクラスタを自動的に検出できます。その場合は、最初の 2 つの手順をスキップし、手順 3 から始めます。

1 ネットワーク接続を確認

1. Cloud Manager と Kubernetes クラスタの間、および Kubernetes クラスタから ONTAP システムへのネットワーク接続が確立されている必要があります。
2. Cloud Manager のインストール時に、アウトバウンドのインターネット接続で次のエンドポイントにアクセスできる必要があります。

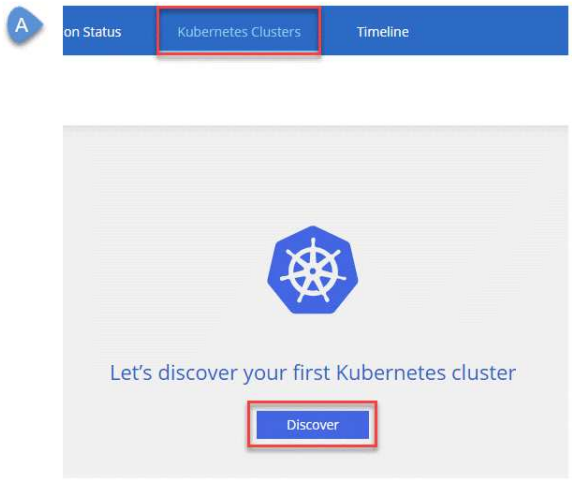
   ¥ https://packages.cloud.google.com/yum ¥ https://github.com/NetApp/trident/releases/download/

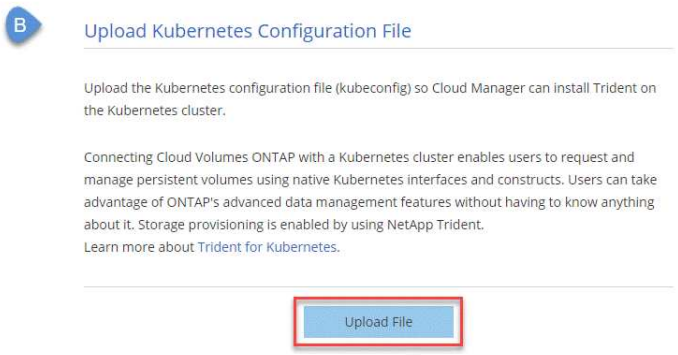
Cloud Manager は、作業環境をクラスタに接続すると Kubernetes クラスタに Trident をインストールします。

2 Kubernetes 構成ファイルを Cloud Manager にアップロード

Kubernetes クラスタごとに、アカウント管理者が YAML 形式の構成ファイル（ kubeconfig ）をアップロードする必要があります。ファイルをアップロードすると、 Cloud Manager はクラスタへの接続を検証し、暗号化された kubeconfig ファイルのコピーを保存します。

[* Kubernetes Clusters] > [Discover] > [Upload File] をクリックし、 kubeconfig ファイルを選択します。



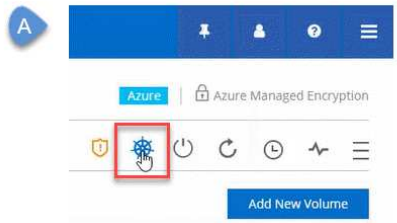


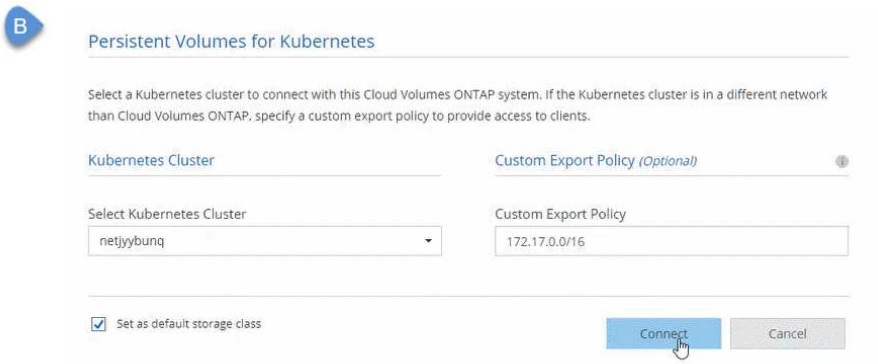
タブに [Discover] ボタンが表示されたスクリーンショットで、 [Upload File] をクリックして kubeconfig ファイルをアップロードします。"]

3 作業環境を Kubernetes クラスタに接続

作業環境で Kubernetes アイコンをクリックし、画面の指示に従います。異なるクラスタを異なる ONTAP システムに、複数のクラスタを同じ ONTAP システムに接続できます。

ネットアップストレージクラスを Kubernetes クラスタのデフォルトのストレージクラスとして設定することもできます。ユーザが永続ボリュームを作成すると、 Kubernetes クラスタは、接続された ONTAP システムをデフォルトでバックエンドストレージとして使用できます。





4 永続ボリュームのプロビジョニングを開始します

Kubernetes の標準のインターフェイスと構成要素を使用して、永続ボリュームを要求および管理できます。Cloud Manager では、永続的ボリュームのプロビジョニングに使用できる Kubernetes ストレージクラスが 4 つ作成されます。

- * NetApp-file* ：単一ノードの ONTAP システムにパーシステントボリュームをバインドする場合
- * NetApp-file-san* ： iSCSI パーシステントボリュームをシングルノードの ONTAP システムにバインドする場合
- * NetApp-fileredundant * ：永続的ボリュームを ONTAP HA ペアにバインドするため
- * NetApp-file-redundant-san * ： iSCSI 永続的ボリュームを ONTAP HA ペアにバインドする場合

Cloud Manager は、デフォルトで次のプロビジョニングオプションを使用するように Trident を設定します。

- シンボリューム
- デフォルトの Snapshot ポリシー
- アクセス可能な Snapshot ディレクトリ

"Trident で最初のボリュームをプロビジョニングする方法をご確認ください Kubernetes"

Trident ボリュームとは何ですか。

Cloud Manager は、 Kubernetes クラスタに接続する最初の ONTAP システム上にボリュームを作成します。ボリューム名に「 _trident_trident 」が追加されます。 ONTAP は、このボリュームを使用して Kubernetes クラスタに接続します。これらのボリュームは削除しないでください。

Kubernetes クラスタを切断または削除するとどうなりますか？

Cloud Manager を使用すると、個々の ONTAP システムを Kubernetes クラスタから切断できます。システムを切断すると、その ONTAP システムをコンテナ用の永続的ストレージとして使用できなくなります。既存の永続ボリュームは削除されません。

Kubernetes クラスタからすべてのシステムを切断したら、 Kubernetes 構成全体を Cloud Manager から削除することもできます。クラスタを削除しても、 Cloud Manager は Trident をアンインストールしないため、永続的ボリュームは削除されません。

どちらのアクションも API からのみ実行できます。今後のリリースでインターフェイスにアクションを追加する予定です。"API の詳細については、ここをクリックしてください"。

NetApp ボリューム暗号化によるボリュームの暗号化

NetApp Volume Encryption （ NVE ）は、一度に 1 ボリュームずつ保管データを暗号化するためのソフトウェアベースのテクノロジです。データ、 Snapshot コピー、およびメタデータが暗号化されます。データへのアクセスには、ボリュームごとに 1 つずつ、

一意の XTS-AES-256 キーを使用します。

このタスクについて

- Cloud Manager 3.7.1 以降では、ネットアップサポートに登録されている各 Cloud Volumes ONTAP システムに NetApp Volume Encryption ライセンスが自動的にインストールされます。
  - "Cloud Manager へのネットアップサポートサイトのアカウントの追加"
  - "従量課金制システムの登録"

  Cloud Manager は、中国地域のシステムに NVE ライセンスをインストールしません。

- 現時点で、 Cloud Volumes ONTAP は外部キー管理サーバを使用した NetApp Volume Encryption をサポートしています。オンボードキーマネージャはサポートされていません。
- ONTAP CLI から NetApp Volume Encryption をセットアップする必要があります。

  その後、 CLI または System Manager を使用して、特定のボリュームで暗号化を有効にできます。Cloud Manager のユーザインターフェイスと API では、 NetApp Volume Encryption がサポートされていません。

"サポートされている暗号化テクノロジの詳細を確認してください"。

手順

1. でサポートされているキー管理ツールのリストを確認します "NetApp Interoperability Matrix Tool で確認できます"。

   Key Managers * ソリューションを検索します。

2. "Cloud Volumes ONTAP CLI に接続します"。
3. SSL 証明書をインストールして、外部キー管理サーバに接続します。

   "ONTAP 9 ネットアップ暗号化パワーガイド：外部キー管理の設定"

4. CLI または System Manager を使用して、暗号化された新しいボリュームを作成するか、暗号化されていない既存のボリュームを変換します。
   - CLI の使用
     - 新しいボリュームの場合は、 -encrypt パラメータを指定して * volume create * コマンドを使用します。

       "ONTAP 9 ネットアップ暗号化パワーガイド：新しいボリュームでの暗号化の有効化"

     - 既存のボリュームについては、 * volume encryption conversion start * コマンドを使用します。

       "ONTAP 9 ネットアップ暗号化パワーガイド： volume encryption conversion start コマンドを使用した既存のボリュームでの暗号化の有効化"

   - System Manager の略
     - 新しいボリュームの場合は、 * Storage > Volumes > Create > Create FlexVol * の順にクリックし、 * Encrypted * を選択します。

"ONTAP 9 System Manager を使用したクラスタ管理： FlexVol ボリュームの作成"

- 既存のボリュームの場合は、ボリュームを選択し、 * 編集 * をクリックして、 * 暗号化 * を選択します。

  "ONTAP 9 System Manager を使用したクラスタ管理：ボリュームプロパティの編集"

既存のストレージの管理

Cloud Manager では、ボリューム、アグリゲート、 CIFS サーバを管理できます。また、容量の問題を回避するためにボリュームを移動するように求められます。

既存のボリュームの管理

既存のボリュームは、ストレージのニーズの変化に応じて管理できます。ボリュームの表示、編集、クローン作成、リストア、削除を実行できます。

手順

1. [作業環境] ページで、ボリュームを管理する Cloud Volumes ONTAP 作業環境をダブルクリックします。
2. ボリュームの管理：

タスク	アクション
ボリュームに関する情報を表示します	ボリュームを選択し、 * 情報 * をクリックします。
ボリュームの編集（読み取り / 書き込みボリュームのみ）	a. ボリュームを選択し、 * 編集 * をクリックします。 b. ボリュームの Snapshot ポリシー、 NFS アクセス制御リスト、または共有権限を変更し、 * Update * をクリックします。 ⓘ カスタムの Snapshot ポリシーが必要な場合は、 System Manager を使用して作成できます。
ボリュームのクローンを作成します	a. ボリュームを選択し、 * Clone * をクリックします。 b. 必要に応じてクローン名を変更し、 * Clone * をクリックします。 このプロセスにより、 FlexClone ボリュームが作成されます。FlexClone ボリュームは、書き込み可能なポイントインタイムコピーであり、メタデータ用に少量のスペースを使用するため、スペース効率に優れています。また、データの変更や追加に応じて追加のスペースを消費するだけです。 FlexClone ボリュームの詳細については、を参照してください "ONTAP 9 論理ストレージ管理ガイド"。

タスク	アクション
Snapshot コピーから新しいボリュームにデータをリストアします	a. ボリュームを選択し、 * Snapshot コピーからリストア * をクリックします。 b. Snapshot コピーを選択し、新しいボリュームの名前を入力して、 * Restore * をクリックします。
オンデマンドで Snapshot コピーを作成します	a. ボリュームを選択し、 * Snapshot コピーの作成 * をクリックします。 b. 必要に応じて名前を変更し、 * 作成 * をクリックします。
nfs mount コマンドを取得します	a. ボリュームを選択し、 * コマンドのマウント * をクリックします。 b. [* コピー（ Copy ）] をクリックします
基になるディスクタイプを変更します	a. ボリュームを選択し、 * ディスクタイプと階層化ポリシーの変更 * をクリックします。 b. ディスクタイプを選択し、 * Change * をクリックします。 Cloud Manager は、選択したディスクタイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。
階層化ポリシーを変更します	a. ボリュームを選択し、 * ディスクタイプと階層化ポリシーの変更 * をクリックします。 b. ［ * ポリシーの編集 * ］ をクリックします。 c. 別のポリシーを選択し、 * 変更 * をクリックします。 Cloud Manager は、選択したディスクタイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。
ボリュームの S3 への同期を有効または無効にします	ボリュームを選択し、 * S3 への同期 * または * 同期関係の削除 * をクリックします。 これらのオプションを使用するには、 S3 への同期機能を有効にする必要があります。手順については、を参照してください "AWS S3 へのデータの同期"
ボリュームを削除します	a. ボリュームを選択し、 * 削除 * をクリックします。 b. 再度 * Delete * をクリックして確定します。

既存のアグリゲートの管理

アグリゲートの管理を自分で行うには、ディスクの追加、アグリゲートに関する情報の表示、およびアグリゲートの削除を行います。

作業を開始する前に

アグリゲートを削除する場合は、まずアグリゲート内のボリュームを削除しておく必要があります。

このタスクについて

アグリゲートのスペースが不足している場合は、 OnCommand System Manager を使用してボリュームを別のアグリゲートに移動できます。

手順

1. [作業環境] ページで、アグリゲートを管理する Cloud Volumes ONTAP 作業環境をダブルクリックします。
2. メニューアイコンをクリックし、 [* 詳細設定] > [高度な割り当て *] をクリックします。
3. アグリゲートの管理：

タスク	アクション
アグリゲートに関する情報を表示します	アグリゲートを選択し、 * Info * をクリックします。
特定のアグリゲートにボリュームを作成します	アグリゲートを選択し、 * ボリュームの作成 * をクリックします。
アグリゲートにディスクを追加します	a. アグリゲートを選択し、 * AWS ディスクの追加 * または * Azure ディスクの追加 * をクリックします。 b. 追加するディスクの数を選択し、 * 追加 * をクリックします。 アグリゲート内のディスクはすべて同じサイズである必要があります。
アグリゲートを削除します	a. ボリュームを含まないアグリゲートを選択し、 * Delete * をクリックします。 b. 再度 * Delete * をクリックして確定します。

CIFS サーバの変更

DNS サーバまたは Active Directory ドメインを変更した場合は、クライアントへのストレージの提供を継続できるように、 Cloud Volumes ONTAP で CIFS サーバを変更する必要があります。

手順

1. 作業環境で、メニューアイコンをクリックし、 * Advanced > CIFS setup * をクリックします。
2. CIFS サーバの設定を指定します。

タスク	アクション
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「 * OU=computers 、 OU=corp * 」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

3. [保存（ Save ）] をクリックします。

結果

Cloud Volumes ONTAP は CIFS サーバを変更して更新します。

容量の問題を回避するためにボリュームを移動する

Cloud Manager では、容量の問題を回避するためにボリュームの移動が必要であることを示す Action Required メッセージが表示される場合がありますが、問題を修正するための推奨事項を提示することはできません。この場合は、問題の解決方法を特定してから、 1 つ以上のボリュームを移動する必要があります。

手順

1. 問題を解決する方法を認識する。。
2. 分析に基づいて、容量の問題を回避するためにボリュームを移動します。
   - ボリュームを別のシステムに移動します。。
   - ボリュームを同じシステム上の別のアグリゲートに移動します。。

容量の問題を解決する方法を特定する

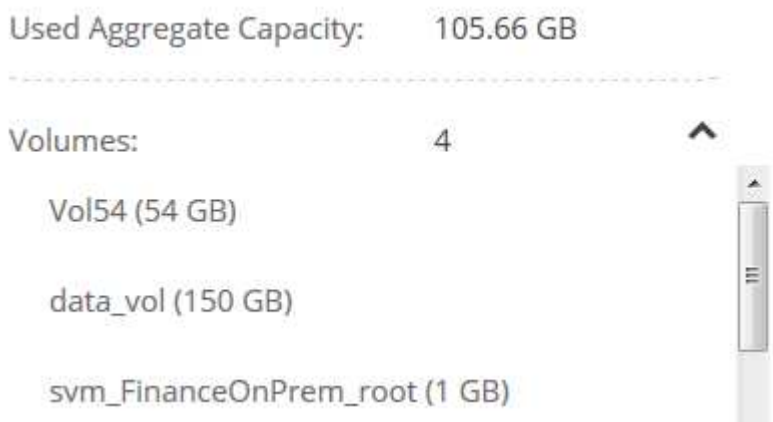
容量の問題を回避するために Cloud Manager がボリュームの移動に関する推奨事項を提供できない場合は、移動する必要があるボリュームを特定し、それらを同じシステム上の別のアグリゲートに移動するか、別のシステムに移動するかを決定する必要があります。

手順

1. Action Required メッセージの詳細情報を表示して、容量制限に達したアグリゲートを特定します。

たとえば、アグリゲート aggr1 の容量が上限に達したとします。

2. アグリゲートから移動する 1 つ以上のボリュームを指定します。
   a. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > 高度な割り当て * をクリックします。
   b. アグリゲートを選択し、 * Info * をクリックします。
   c. ボリュームのリストを展開します。



   d. 各ボリュームのサイズを確認し、アグリゲートから移動するボリュームを 1 つ以上選択します。

      将来的に容量の問題が発生しないように、アグリゲート内の空きスペースに十分な大きさのボリュームを選択する必要があります。

3. システムがディスク制限に達していない場合は、ボリュームを同じシステム上の既存のアグリゲートまたは新しいアグリゲートに移動する必要があります。

   詳細については、を参照してください "ボリュームを別のアグリゲートに移動して、容量の問題を回避します"。

4. システムがディスクの上限に達した場合は、次のいずれかを実行します。
   a. 未使用のボリュームを削除します。
   b. ボリュームを再配置して、アグリゲートの空きスペースを確保します。

      詳細については、を参照してください "ボリュームを別のアグリゲートに移動して、容量の問題を回避します"。

   c. スペースがある別のシステムに 2 つ以上のボリュームを移動します。

      詳細については、を参照してください "容量の問題を回避するためにボリュームを別のシステムに移動する"。

容量の問題を回避するためにボリュームを別のシステムに移動する

1 つ以上のボリュームを別の Cloud Volumes ONTAP システムに移動して、容量の問題を回避できます。システムがディスクの上限に達した場合は、この操作が必要になることがあります。

このタスクについて

このタスクの手順に従って、次のアクションが必要なメッセージを修正できます。

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.手順
. 使用可能な容量を持つ Cloud Volumes ONTAP
システムを特定するか、新しいシステムを導入します。
. ソースの作業環境をターゲットの作業環境にドラッグアンドドロップして、ボリュームの 1
回限りのデータレプリケーションを実行します。
```

+
詳細については、を参照してください "システム間でのデータのレプリケーション"。

1. [Replication Status] ページに移動し、 SnapMirror 関係を解除して、レプリケートされたボリュームをデータ保護ボリュームから読み取り / 書き込みボリュームに変換します。

   詳細については、を参照してください "データレプリケーションのスケジュールと関係の管理"。

2. データアクセス用にボリュームを設定します。

   データアクセス用のデスティネーションボリュームの設定については、を参照してください "ONTAP 9 ボリュームディザスタリカバリエクスプレスガイド"。

3. 元のボリュームを削除します。

   詳細については、を参照してください "既存のボリュームの管理"。

ボリュームを別のアグリゲートに移動して、容量の問題を回避します

1 つ以上のボリュームを別のアグリゲートに移動して、容量の問題を回避できます。

このタスクについて

このタスクの手順に従って、次のアクションが必要なメッセージを修正できます。

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.手順
.
既存のアグリゲートに、移動する必要があるボリュームの使用可能な容量があるかどうかを確認し
ます。
```

+
.. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > 高度な割り当て * をクリックします。
.. 各アグリゲートを選択し、 * Info * をクリックして、使用可能な容量（アグリゲート容量から使用済みアグリゲート容量を引いた容量）を確認します。

+

aggr1

Aggregate Capacity:	442.94 GB
Used Aggregate Capacity:	105.66 GB

1. 必要に応じて、既存のアグリゲートにディスクを追加します。
   a. アグリゲートを選択し、 * ディスクの追加 * をクリックします。
   b. 追加するディスクの数を選択し、 * 追加 * をクリックします。
2. 使用可能な容量を持つアグリゲートがない場合は、新しいアグリゲートを作成します。

   詳細については、を参照してください "アグリゲートの作成"。

3. System Manager または CLI を使用して、ボリュームをアグリゲートに移動します。
4. ほとんどの場合、 System Manager を使用してボリュームを移動できます。

   手順については、を参照してください "ONTAP 9 ボリューム移動エクスプレスガイド"。

データのレプリケートと保護

ONTAP クラスタの検出と管理

Cloud Manager では、オンプレミス環境、ネットアップのプライベートストレージ構成、 IBM クラウド内の ONTAP クラスタを検出できます。これらのクラスタを検出すると、 Cloud Manager から直接ハイブリッドクラウド環境全体にデータを簡単にレプリケートできます。

ONTAP クラスタの検出

Cloud Manager で ONTAP クラスタを検出すると、ハイブリッドクラウド全体でストレージのプロビジョニングとデータの複製が可能になります。

作業を開始する前に

クラスタを Cloud Manager に追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。

Cloud Manager は、 HTTPS を使用して ONTAP クラスタを検出します。カスタムファイアウォールポリシーを使用する場合は、次の要件を満たす必要があります。

- Cloud Manager ホストでは、ポート 443 経由の発信 HTTPS アクセスが許可されている必要があります。

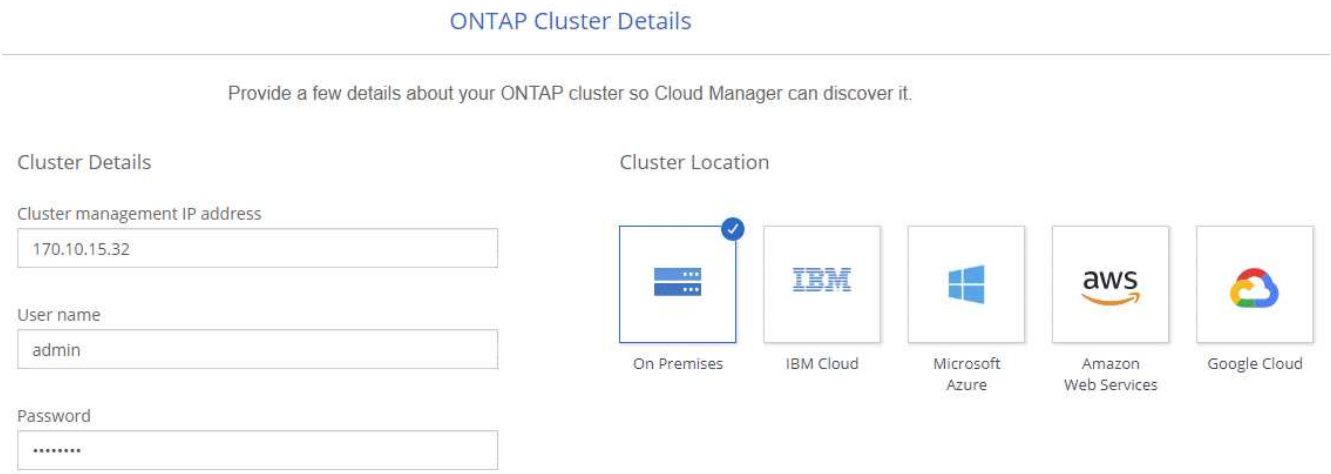
  Cloud Manager が AWS 内にある場合は、事前定義されたセキュリティグループによってすべての発信通信が許可されます。

- ONTAP クラスタでは、ポート 443 を介した着信 HTTPS アクセスが許可されている必要があります。

  デフォルトの「 mgmt 」ファイアウォールポリシーでは、すべての IP アドレスからの着信 HTTPS アクセスが許可されます。このデフォルトポリシーを変更した場合、または独自のファイアウォールポリシーを作成した場合は、 HTTPS プロトコルをそのポリシーに関連付け、 Cloud Manager ホストからのアクセスを有効にする必要があります。

手順

1. 作業環境ページで、 * 検出 * をクリックし、 * ONTAP クラスタ * を選択します。
2. ONTAP クラスタの詳細 * ページで、クラスタ管理 IP アドレス、 admin ユーザアカウントのパスワード、クラスタの場所を入力します。



3. [詳細] ページで、作業環境の名前と説明を入力し、 [* 移動] をクリックします。

結果

Cloud Manager はクラスタを検出します。ボリュームの作成、クラスタとの間でのデータの複製、OnCommand System Manager の起動を実行して高度なタスクを実行できるようになりました。

ONTAP クラスタでのボリュームのプロビジョニング

Cloud Manager を使用すると、 ONTAP クラスタで NFS ボリュームと CIFS ボリュームをプロビジョニングできます。

作業を開始する前に

クラスタに NFS または CIFS を設定する必要があります。System Manager または CLI を使用して、 NFS と CIFS を設定できます。

このタスクについて

既存のアグリゲートにボリュームを作成できます。Cloud Manager から新しいアグリゲートを作成することはできません。

手順

1. [Working Environments] ページで、ボリュームをプロビジョニングする ONTAP クラスタの名前をダブルクリックします。
2. [新しいボリュームの追加] をクリックします。
3. Create New Volume （新規ボリュームの作成）ページで、ボリュームの詳細を入力し、 * Create * （作成）をクリックします。

   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。

フィールド	説明
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
使用プロファイル	使用プロファイルは、ボリュームに対して有効になっている NetApp Storage Efficiency 機能を定義します。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。

システム間でのデータのレプリケーション

データ転送のための 1 回限りのデータレプリケーションを選択するか、ディザスタリカバリまたは長期保存のための定期的なスケジュールを選択することで、作業環境間でデータをレプリケートできます。たとえば、ディザスタリカバリ用にオンプレミスの ONTAP システムから Cloud Volumes ONTAP へのデータレプリケーションを設定できます。

Cloud Manager では、 SnapMirror と SnapVault テクノロジを使用して、別々のシステム上のボリューム間でのデータレプリケーションを簡素化します。ソースボリュームとデスティネーションボリュームを特定し、レプリケーションポリシーとスケジュールを選択するだけで済みます。Cloud Manager は、必要なディスクを購入し、関係を設定し、レプリケーションポリシーを適用してから、ボリューム間のベースライン転送を開始します。

> ベースライン転送には、ソースデータのフルコピーが含まれます。その後の転送には、ソースデータの差分コピーが含まれます。

データレプリケーションの要件

データを複製する前に、 Cloud Volumes ONTAP システムと ONTAP クラスタの両方で特定の要件が満たされていることを確認する必要があります。

バージョン要件

データを複製する前に、ソースボリュームとデスティネーションボリュームで互換性のある ONTAP バージョンが実行されていることを確認する必要があります。詳細については、を参照してください "データ保護パワーガイド"。

Cloud Volumes ONTAP 固有の要件

- インスタンスのセキュリティグループに、必要なインバウンドおよびアウトバウンドのルールが含まれている必要があります。具体的には、 ICMP とポート 10000 、 11104 、および 11105 のルールが必要です。

  これらのルールは、事前定義されたセキュリティグループに含まれています。

- 異なるサブネットにある 2 つの Cloud Volumes ONTAP システム間でデータをレプリケートするには、サブネットを一緒にルーティングする必要があります（これがデフォルト設定です）。
- AWS の Cloud Volumes ONTAP システムと Azure のシステムの間でデータをレプリケートするには、AWS VPC と Azure VNet の間に VPN 接続が必要です。

ONTAP クラスタ固有の要件

- アクティブな SnapMirror ライセンスがインストールされている必要があります。
- クラスタが社内にある場合は、企業ネットワークから AWS または Azure （通常は VPN 接続）に接続する必要があります。
- ONTAP クラスタは、サブネット、ポート、ファイアウォール、およびクラスタの追加要件を満たしている必要があります。

  詳細については、ご使用の ONTAP バージョンの『 Cluster and SVM Peering Express Guide 』を参照してください。

システム間のデータレプリケーションの設定

Cloud Volumes ONTAP システムと ONTAP クラスタ間でデータをレプリケートするには、ワンタイムデータレプリケーションを選択します。これにより、クラウドとの間でデータを移動したり、定期的にスケジュールを作成したりすることができ、ディザスタリカバリや長期保存に役立ちます。

このタスクについて

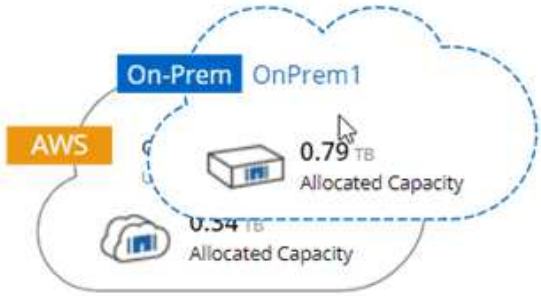
Cloud Manager は、シンプルなファンアウト / カスケードデータ保護構成をサポートしています。

- シンプルな構成では、ボリューム A からボリューム B へのレプリケーションが行われます
- ファンアウト構成では、ボリューム A から複数のデスティネーションへのレプリケーションが行われます。
- カスケード構成では、レプリケーションはボリューム A からボリューム B 、およびボリューム B からボリューム C に行われます

システム間で複数のデータレプリケーションを設定することにより、 Cloud Manager でファンアウトとカスケード構成を構成できます。たとえば、システム A からシステム B にボリュームを複製し、システム B からシステム C に同じボリュームを複製します

手順

1. [作業環境] ページで、ソースボリュームを含む作業環境を選択し、ボリュームをレプリケートする作業環境にドラッグします。



2. [Source and Destination Peering Setup] ページが表示されたら、クラスタピア関係のクラスタ間 LIF をすべて選択します。

   クラスタ間ネットワークは、クラスタピアどうしが *pair-wise full-mesh connectivity* を持つように設定する必要があります。具体的には、クラスタピア関係にある各クラスタペアの、すべてのインタークラスタ LIF の間に接続が確立されている必要があります。

   これらのページは、複数の LIF を持つ ONTAP クラスタがソースまたはデスティネーションである場合に表示されます。

3. ソースボリュームの選択ページで、レプリケートするボリュームを選択します。
4. デスティネーションボリュームの名前と階層化ページで、デスティネーションボリュームの名前を指定し、基盤となるディスクタイプを選択していずれかのアドバンストオプションを変更し、「 * Continue * 」をクリックします。

   デスティネーションが ONTAP クラスタの場合は、デスティネーション SVM とアグリゲートも指定する必要があります。

5. [最大転送レート（ Max Transfer Rate ）] ページで、データを転送できる最大転送レート（メガバイト / 秒）を指定します。
6. Replication Policy （レプリケーションポリシー）ページで、デフォルトポリシーのいずれかを選択するか、 * Additional Policies * （追加ポリシー）をクリックして、いずれかの詳細ポリシーを選択します。

   ヘルプについては、を参照してください "レプリケーションポリシーの選択"。

   カスタムバックアップ（ SnapVault ）ポリシーを選択した場合は、ポリシーに関連付けられたラベルがソースボリューム上の Snapshot コピーのラベルと一致する必要があります。詳細については、を参照してください "バックアップポリシーの仕組み"。

7. [スケジュール] ページで、ワンタイムコピーまたは定期的なスケジュールを選択します。

   いくつかのデフォルトスケジュールを使用できます。別のスケジュールを使用する場合は、 System Manager を使用して、 _destination_cluster に新しいスケジュールを作成する必要があります。

8. [レビュー] ページで、選択内容を確認し、 [* 移動] をクリックします。

結果

Cloud Manager がデータレプリケーションプロセスを開始します。レプリケーションの詳細は、 Replication Status ページで確認できます。

データレプリケーションのスケジュールと関係の管理

2 つのシステム間でデータレプリケーションをセットアップしたら、 Cloud Manager からデータレプリケーションスケジュールと関係を管理できます。

手順

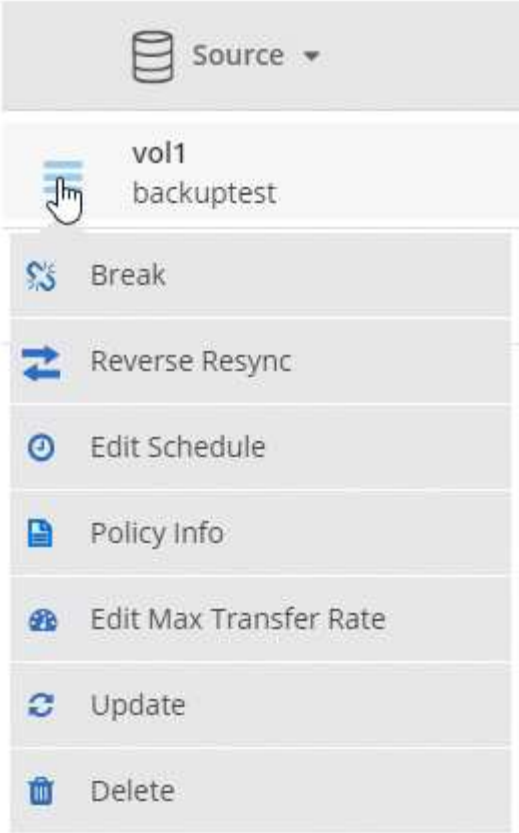
1. 作業環境ページで、ワークスペース内のすべての作業環境または特定の作業環境のレプリケーションステータスを確認します。

オプション	アクション
ワークスペース内のすべての作業環境	Cloud Manager の上部で、 * Replication Status * をクリックします。
特定の作業環境	作業環境を開き、 * Replications * をクリックします。

2. データレプリケーションリレーションシップのステータスを確認して、正常であることを確認します。

> 関係のステータスがアイドルで、ミラーの状態が初期化されていない場合は、定義されたスケジュールに従ってデータレプリケーションを実行するために、デスティネーションシステムから関係を初期化する必要があります。この関係は、 System Manager またはコマンドラインインターフェイス（ CLI ）を使用して初期化できます。これらの状態は、デスティネーションシステムに障害が発生してからオンラインに戻ると表示されます。

3. ソースボリュームの横にあるメニューアイコンを選択し、使用可能なアクションのいずれかを選択します。



次の表に、使用可能なアクションを示します。

アクション	説明
休憩	ソースボリュームとデスティネーションボリューム間の関係を解除し、データアクセスのためにデスティネーションボリュームをアクティブにします。このオプションは通常、データの破損、偶発的な削除、オフライン状態などのイベントが原因でソースボリュームがデータを処理できない場合に使用します。データアクセス用のデスティネーションボリュームの設定およびソースボリュームの再アクティブ化の詳細については、『ONTAP 9 Volume Disaster Recovery Express Guide』を参照してください。
再同期	ボリューム間の関係を再確立し、定義されたスケジュールに従ってデータレプリケーションを再開します。 ボリュームを再同期すると、デスティネーションボリュームの内容がソースボリュームの内容によって上書きされます。 デスティネーションボリュームからソースボリュームへデータを再同期化する逆再同期を実行するには、を参照してください "ONTAP 9 ボリュームディザスタリカバリエクスプレスガイド"。
リバース再同期	ソースボリュームとデスティネーションボリュームの役割を逆にします。元のソースボリュームの内容は、デスティネーションボリュームの内容によって上書きされます。これは、オフラインになったソースボリュームを再アクティブ化する場合に役立ちます。前回のデータレプリケーションからソースボリュームが無効になったまでの間に元のソースボリュームに書き込まれたデータは保持されません。

アクション	説明
スケジュールを編集します	データレプリケーションの別のスケジュールを選択できます。
ポリシー情報	データレプリケーションリレーションシップに割り当てられている保護ポリシーを表示します。
最大転送レートを編集します	データを転送できる最大レート（キロバイト / 秒）を編集できます。
更新	増分転送を開始してデスティネーションボリュームを更新します。
削除	ソースボリュームとデスティネーションボリューム間のデータ保護関係を削除します。つまり、ボリューム間でデータレプリケーションが行われなくなります。この操作では、データアクセスのデスティネーションボリュームはアクティブ化されません。また、システム間に他のデータ保護関係がない場合は、クラスタピア関係と Storage Virtual Machine （ SVM ）ピア関係も削除されます。

結果

アクションを選択すると、 Cloud Manager によって関係またはスケジュールが更新されます。

レプリケーションポリシーの選択

Cloud Manager でデータレプリケーションを設定するときに、レプリケーションポリシーの選択が必要になることがあります。レプリケーションポリシーは、ストレージシステムがソースボリュームからデスティネーションボリュームにデータをレプリケートする方法を定義します。

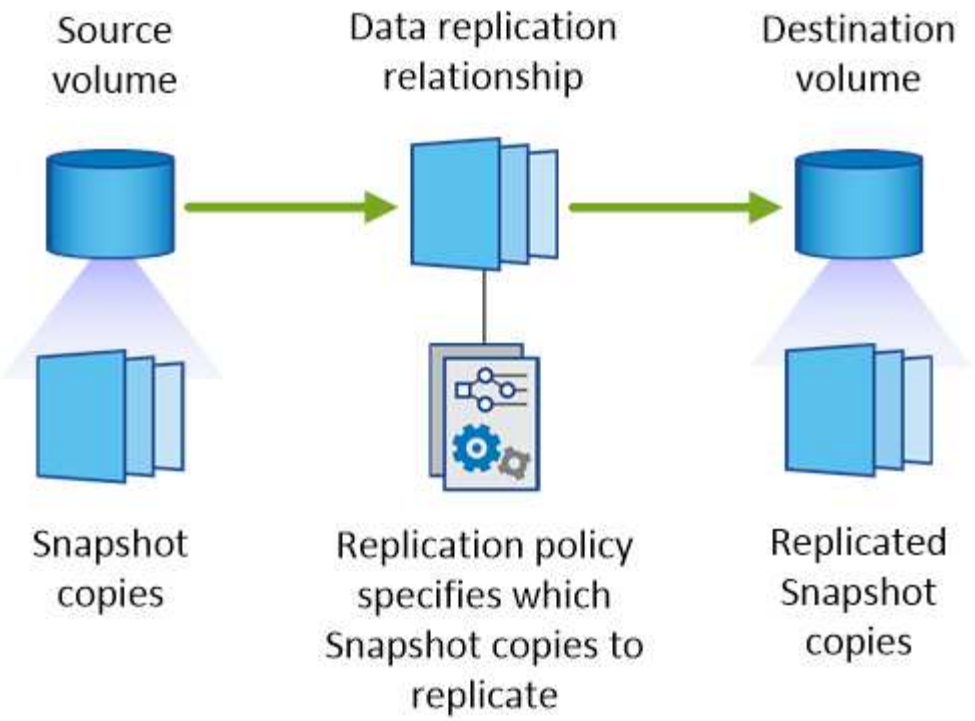
レプリケーションポリシーの機能

ONTAP オペレーティングシステムでは、 Snapshot コピーと呼ばれるバックアップが自動的に作成されます。Snapshot コピーは、ボリュームの読み取り専用イメージで、ある時点のファイルシステムの状態をキャプチャします。

システム間でデータをレプリケートする場合、ソースボリュームからデスティネーションボリュームに Snapshot コピーをレプリケートします。レプリケーションポリシーは、ソースボリュームからデスティネーションボリュームにレプリケートする Snapshot コピーを指定します。

> レプリケーションポリシーは、ディザスタリカバリ保護やディスクツーディスクのバックアップとリカバリを提供する SnapMirror テクノロジと SnapVault テクノロジを基盤としているため、 _protection_policies とも呼ばれます。

次の図は、 Snapshot コピーとレプリケーションポリシーの関係を示しています。



レプリケーションポリシーのタイプ

レプリケーションポリシーには、次の 3 種類があります。

- A_Mirror_policy は、新しく作成された Snapshot コピーをデスティネーションボリュームにレプリケートします。

  これらの Snapshot コピーを使用すると、災害復旧や 1 回限りのデータ複製に備えて、ソース・ボリュームを保護できます。データアクセス用のデスティネーションボリュームは、いつでもアクティブにできます。

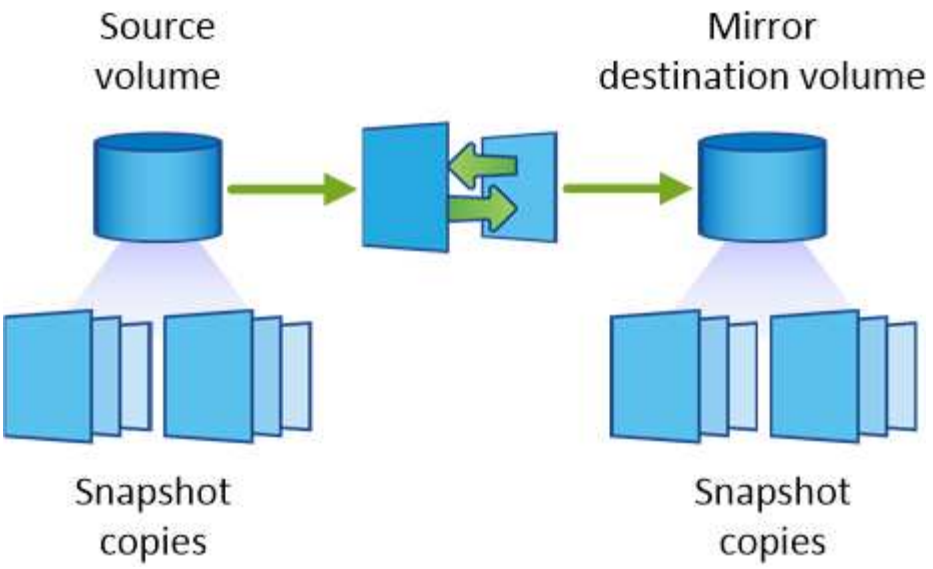
- a_Backup_policy は、特定の Snapshot コピーをデスティネーションボリュームにレプリケートし、通常、ソースボリューム上で保持するよりも長期間にわたって Snapshot コピーを保持します。

  データが破損または損失した場合に、これらの Snapshot コピーからデータをリストアし、標準準拠やその他のガバナンス関連の目的で保持できます。

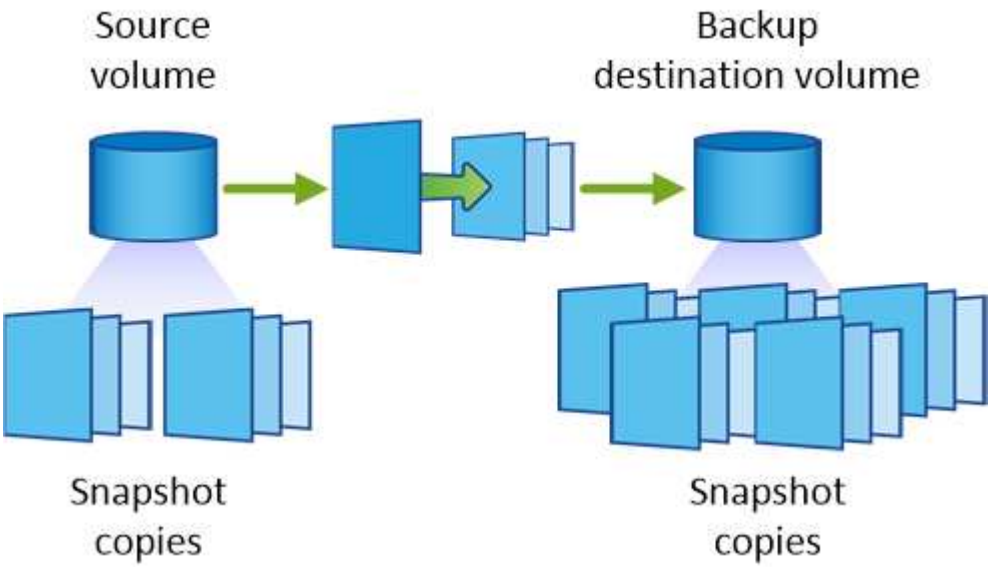
- A_Mirror と Backup_policy は、ディザスタリカバリと長期保持の両方を提供します。

  各システムには、デフォルトのミラーおよびバックアップポリシーが含まれており、多くの状況に適しています。カスタムポリシーが必要な場合は、 System Manager を使用して独自のポリシーを作成できます。

次の図は、ミラーポリシーとバックアップポリシーの違いを示しています。ミラーポリシーは、ソースボリュームで使用可能な Snapshot コピーをミラーリングします。



通常、バックアップポリシーでは、ソースボリュームに保持されている Snapshot コピーよりも長い期間 Snapshot コピーが保持されます。



バックアップポリシーの仕組み

ミラーポリシーとは異なり、バックアップ（ SnapVault ）ポリシーは、特定の Snapshot コピーをデスティネーションボリュームに複製します。デフォルトポリシーの代わりに独自のポリシーを使用する場合は、バックアップポリシーの仕組みを理解することが重要です。

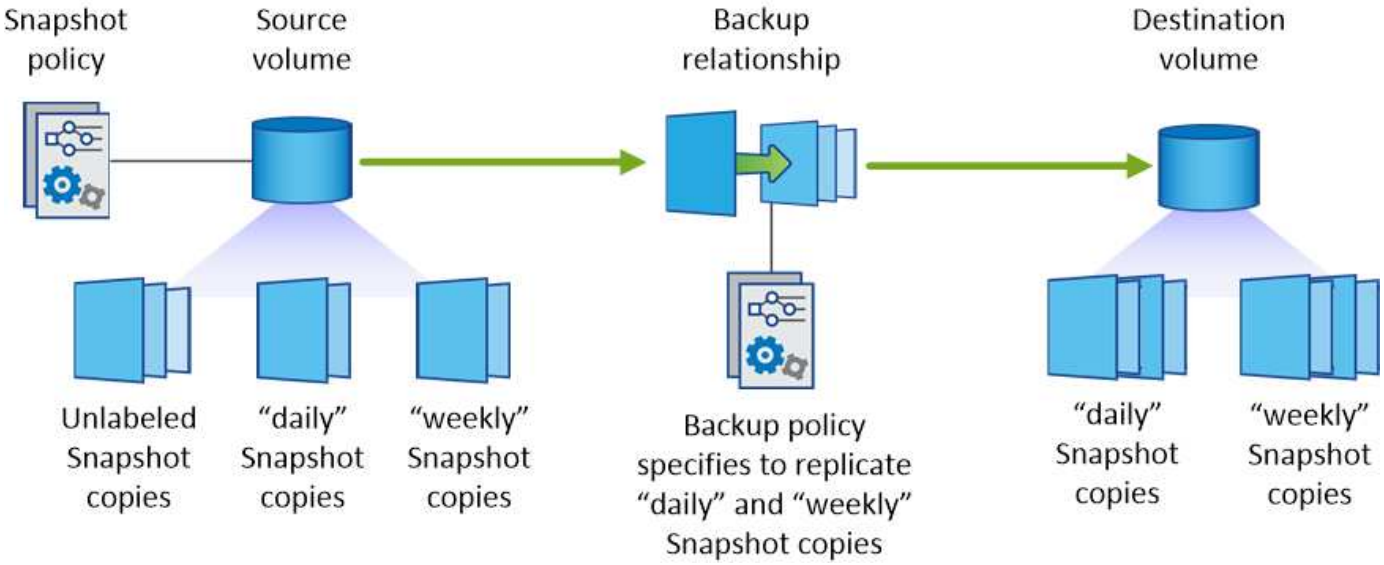
Snapshot コピーのラベルとバックアップ・ポリシーの関係を理解する

Snapshot ポリシーは、システムによるボリュームの Snapshot コピーの作成方法を定義します。このポリシーでは、 Snapshot コピーを作成するタイミング、保持するコピー数、ラベルの作成方法を指定します。たとえば、システムでは毎日午前 12 時 10 分に Snapshot コピーを 1 つ作成し、最新のコピーを 2 つ保持して、「 daily 」というラベルを付けることができます。

バックアップポリシーには、デスティネーションボリュームに複製するラベル付き Snapshot コピーと保持するコピー数を指定するルールが含まれています。バックアップポリシーで定義されたラベルは、スナップショ

ットポリシーで定義された 1 つ以上のラベルと一致する必要があります。そうしないと、システムは Snapshot コピーを複製できません。

たとえば、「 daily 」ラベルと「 weekly 」ラベルを含むバックアップポリシーでは、これらのラベルのみを含む Snapshot コピーのレプリケーションが行われます。次の図に示すように、他の Snapshot コピーはレプリケートされません。



デフォルトポリシーとカスタムポリシー

デフォルトの Snapshot ポリシーでは、毎時、毎日、および毎週の Snapshot コピーが作成されます。Snapshot コピーは 6 個の時間単位、 2 個の日単位、および 2 個の週単位 Snapshot コピーが保持されます。

デフォルトの Snapshot ポリシーでは、デフォルトのバックアップポリシーを簡単に使用できます。デフォルトのバックアップポリシーでは、毎日および毎週の Snapshot コピーが複製され、毎日 7 個、毎週 52 個の Snapshot コピーが保持されます。

カスタムポリシーを作成する場合は、これらのポリシーで定義されたラベルが一致している必要があります。System Manager を使用してカスタムポリシーを作成できます。

Amazon S3 へのデータのバックアップ

S3 へのバックアップは、クラウドデータを完全に管理して保護するバックアップとリストアの機能を提供する、 Cloud Volumes ONTAP のアドオン機能です。バックアップは、ほぼ長期のリカバリやクローニングに使用されるボリュームの Snapshot コピーとは無関係に S3 オブジェクトストレージに格納されます。

S3 へのバックアップを有効にすると、サービスはデータのフルバックアップを実行します。追加のバックアップはすべて増分バックアップです。つまり、変更されたブロックと新しいブロックのみがバックアップされます。

"価格の詳細については、 NetApp Cloud Central をご覧ください"。

すべてのバックアップ処理とリストア処理には Cloud Manager を使用する必要があります。ONTAP または Amazon S3 から直接操作を実行した場合、サポートされない構成になります。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 構成がサポートされていることを確認します

次の点を確認します。

- Cloud Volumes ONTAP 9.4 以降はサポート対象の AWS リージョンで実行されています： Nバージニア、オレゴン、アイルランド、フランクフルト、シドニー
- 新しいにサブスクライブしました "Cloud Manager Marketplace のサービス"
- TCP ポート 5010 は、 Cloud Volumes ONTAP のセキュリティグループのアウトバウンドトラフィックに対してオープン（デフォルトでオープン）
- TCP ポート 8088 は、 Cloud Manager のセキュリティグループ（デフォルトで開いている）のアウトバウンドトラフィック用に開かれています。
- 次のエンドポイントに Cloud Manager からアクセスできます。

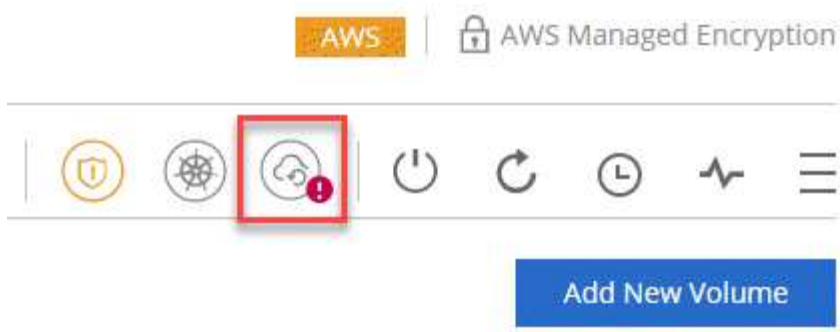
  \ https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Cloud Manager では、 VPC に最大 2 つのインターフェイス VPC エンドポイントを割り当てることができます（ VPC あたりの AWS の上限は 20 ）。
- Cloud Manager に、最新のでリストされている VPC エンドポイントの権限を使用する権限があります "Cloud Manager ポリシー"：

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

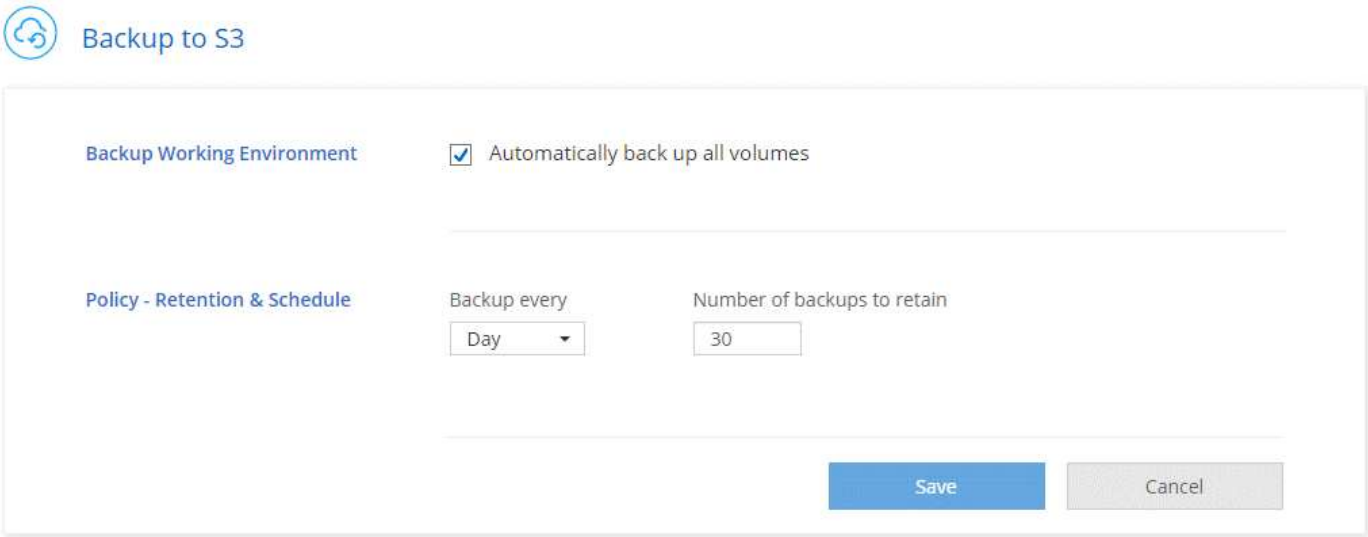
2 新規または既存のシステムで **S3** へのバックアップを有効にします

- 新しいシステム： S3 へのバックアップ機能は、作業環境ウィザードではデフォルトで有効になっています。このオプションは必ず有効にしておいてください。
- 既存システム：作業環境を開き、バックアップ設定アイコンをクリックしてバックアップを有効にします。



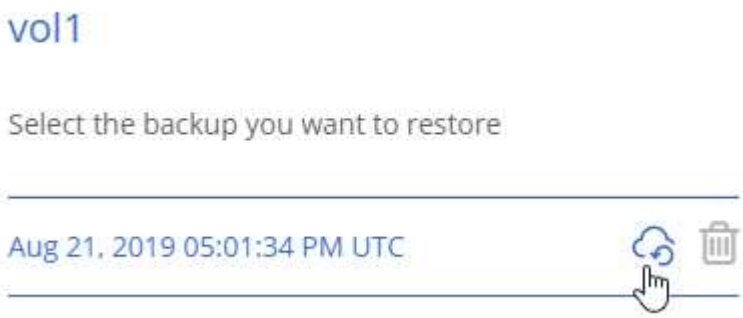
3 必要に応じて、バックアップポリシーを変更します

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームのバックアップコピーが 30 個保持されます。必要に応じて、保持するバックアップコピーの数を変更できます。



4 必要に応じて、データをリストアします

Cloud Manager の上部で、 * Backup & Restore * をクリックし、ボリュームを選択してバックアップを選択し、バックアップから新しいボリュームにデータをリストアします。



要件

S3 へのボリュームのバックアップを開始する前に、次の要件を読み、サポートされている構成になっていることを確認してください。

サポートされている **ONTAP** のバージョン

S3 へのバックアップは、 Cloud Volume ONTAP 9.4 以降でサポートされます。

サポートされている **AWS** リージョン

次の AWS リージョンでは、 Cloud Volumes ONTAP で S3 へのバックアップがサポートされます。

- 米国東部（ N（バージニア州）
- US West （オレゴン州）
- EU （アイルランド）
- 欧州（フランクフルト）
- アジア太平洋地域（シドニー）

AWS 権限が必要です

Cloud Manager に権限を提供する IAM ロールには次の権限が必要です。

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

AWS サブスクリプションの要件

3.7.3 リリースから、 AWS Marketplace で新しい Cloud Manager サブスクリプションが提供されるようになりました。このサブスクリプションでは、 Cloud Volumes ONTAP 9.6 以降の PAYGO システムと Backup to S3 機能の導入が可能です。必要です "この新しい Cloud Manager サブスクリプションに登録してください" S3 へのバックアップを有効にする前に、S3 へのバックアップ機能に対する請求は、このサブスクリプションを通じて行われます。

ポート要件

- TCP ポート 5010 は、 Cloud Volumes ONTAP からバックアップサービスへの発信トラフィックに対してオープンである必要があります。
- Cloud Manager のセキュリティグループ上のアウトバウンドトラフィックには、 TCP ポート 8088 が開いている必要があります。

  これらのポートは、事前定義されたセキュリティグループを使用した場合はすでに開いています。ただし、独自のポートを使用している場合は、これらのポートを開く必要があります。

アウトバウンドインターネットアクセス

次のエンドポイントに Cloud Manager からアクセスできることを確認してください：
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager がこのエンドポイントにアクセスし、 S3 へのバックアップで許可するユーザのリストに

AWS アカウント ID を追加します。

インターフェイス **VPC** エンドポイント

Backup to S3 機能を有効にすると、 Cloud Volumes ONTAP が実行されている VPC にインターフェイス VPC エンドポイントが Cloud Manager によって作成されます。この _ バックアップエンドポイント _ は、 S3 へのバックアップが実行されている NetApp VPC に接続します。ボリュームをリストアすると、 Cloud Manager によって追加のインターフェイス VPC エンドポイント - - The _ restore endpoint_ が作成されます。

VPC 内の他の Cloud Volumes ONTAP システムでは、これらの 2 つの VPC エンドポイントを使用します。

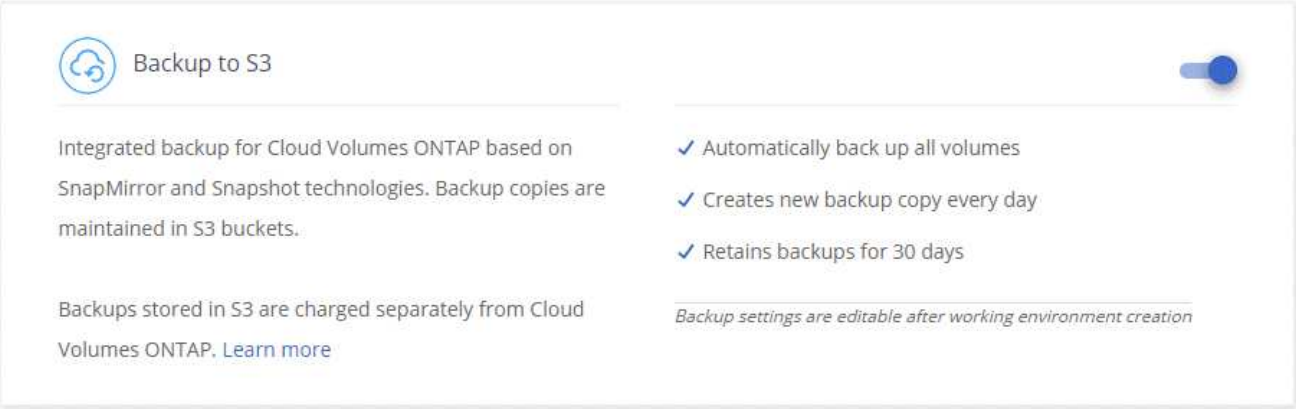
"インターフェイス VPC エンドポイントのデフォルトの制限は、 VPC ごとに 20 です"。この機能を有効にする前に、 VPC が制限に達していないことを確認してください。

新しいシステムでの **S3** へのバックアップの有効化

S3 へのバックアップ機能は、作業環境ウィザードではデフォルトで有効になっています。このオプションは必ず有効にしておいてください。

手順

1. [Cloud Volumes ONTAP の作成 *] をクリックします。
2. クラウドプロバイダとして Amazon Web Services を選択し、シングルノードまたは HA システムを選択します。
3. [詳細と資格情報] ページに入力します。
4. S3 へのバックアップページで、機能を有効なままにして続行をクリックします。



5. ウィザードの各ページを設定し、システムを導入します。

結果

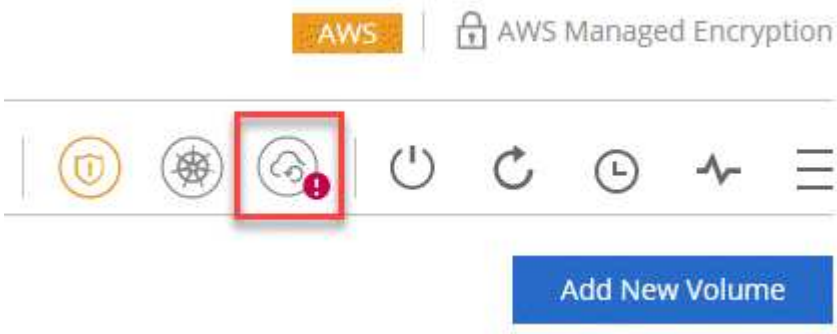
S3 へのバックアップ機能はシステムで有効になっており、ボリュームを毎日バックアップし、 30 個のバックアップコピーを保持します。 バックアップ保持の変更方法について説明します。

既存のシステムでの **S3** へのバックアップの有効化

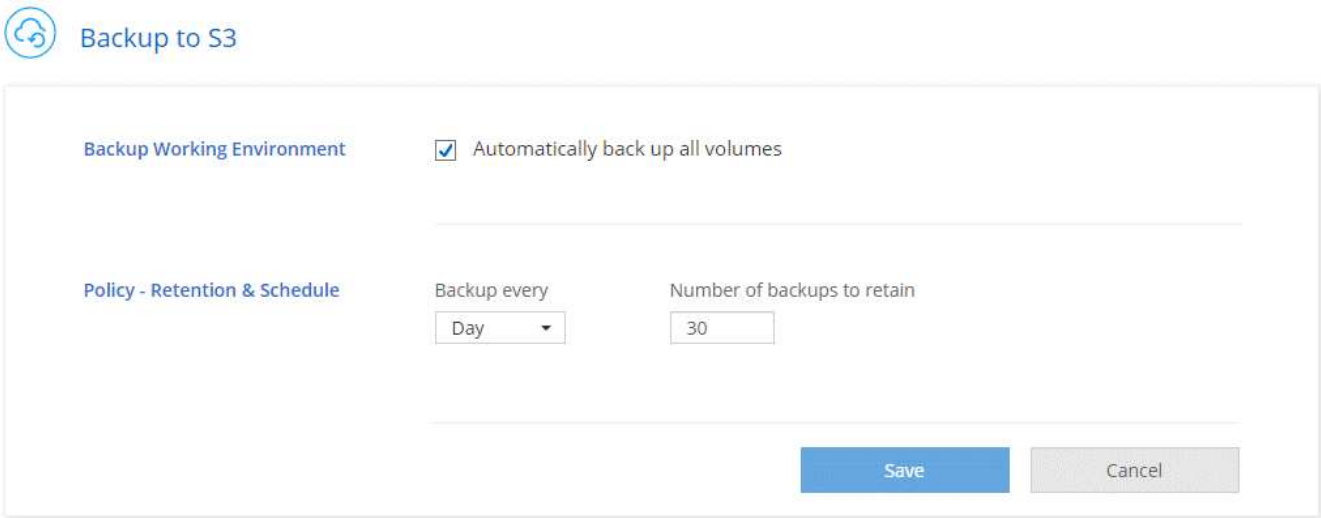
サポートされている構成を実行していれば、既存の Cloud Volumes ONTAP システムで S3 へのバックアップを有効にすることができます。詳細については、を参照してください [要件]。

手順

1. 作業環境を開きます。
2. バックアップ設定アイコンをクリックします。



3. [すべてのボリュームを自動的にバックアップする *] を選択します。
4. バックアップの保持を選択し、 * Save * をクリックします。



結果

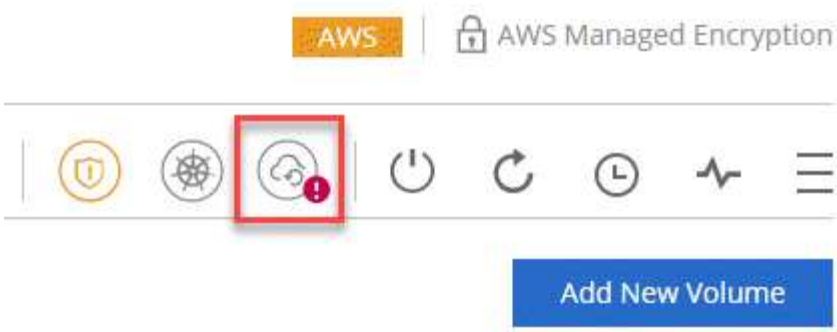
S3 へのバックアップ機能は、各ボリュームの初期バックアップの作成時に開始されます。

バックアップ保持期間を変更しています

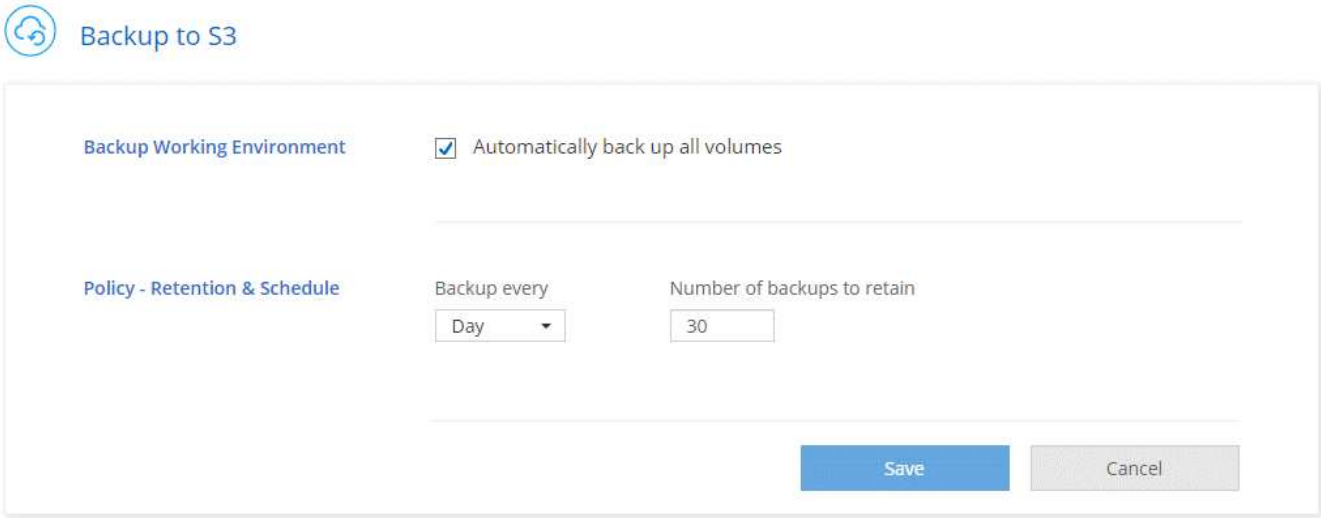
デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームのバックアップコピーが 30 個保持されます。保持するバックアップコピーの数は変更できます。

手順

1. 作業環境を開きます。
2. バックアップ設定アイコンをクリックします。



3. バックアップの保持期間を変更し、 * Save * をクリックします。



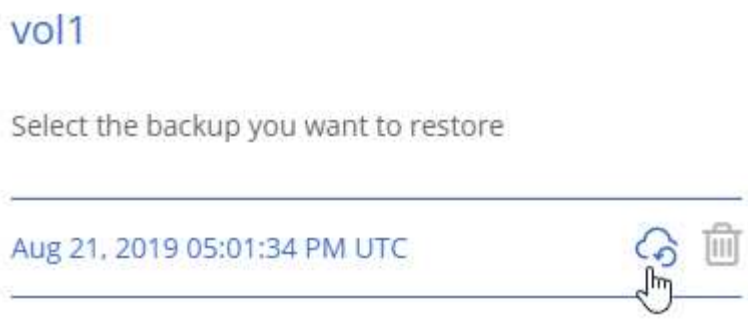
ボリュームをリストアする

バックアップからデータをリストアすると、 Cloud Manager は _new_volume へのフルボリュームリストアを実行します。データは同じ作業環境または別の作業環境にリストアできます。

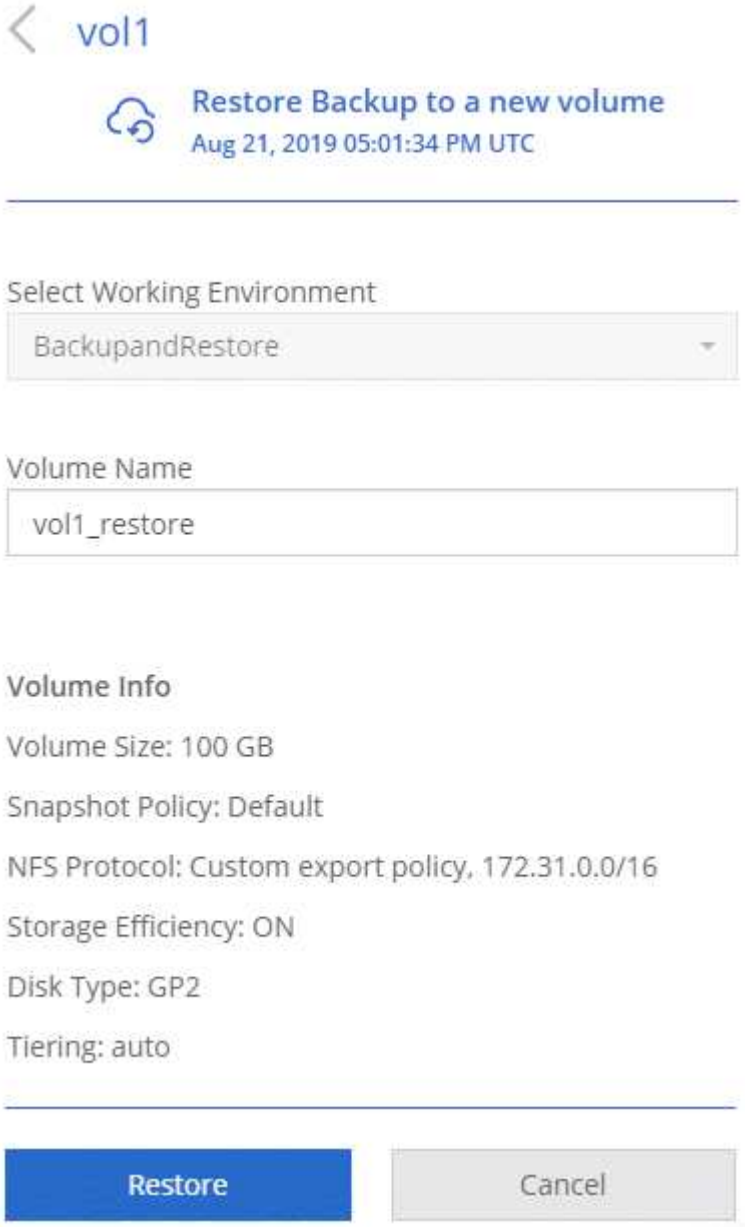
手順

1. Cloud Manager の上部で、 * Backup & Restore * をクリックします。
2. リストアするボリュームを選択します。

3. リストアするバックアップを見つけ、リストアアイコンをクリックします。



4. ボリュームのリストア先となる作業環境を選択します。
5. ボリュームの名前を入力します。
6. [* リストア] をクリックします。

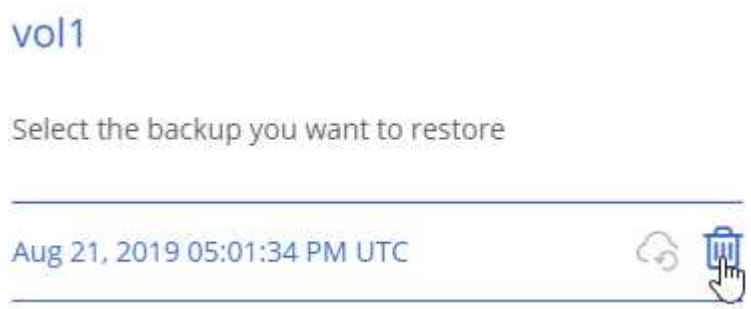


バックアップを削除する

バックアップは、 Cloud Manager から削除するまで S3 に保持されます。ボリュームを削除しても、 Cloud Volumes ONTAP システムを削除しても、バックアップは削除されません。

手順

1. Cloud Manager の上部で、 * Backup & Restore * をクリックします。
2. ボリュームを選択します。
3. 削除するバックアップを見つけ、削除アイコンをクリックします。



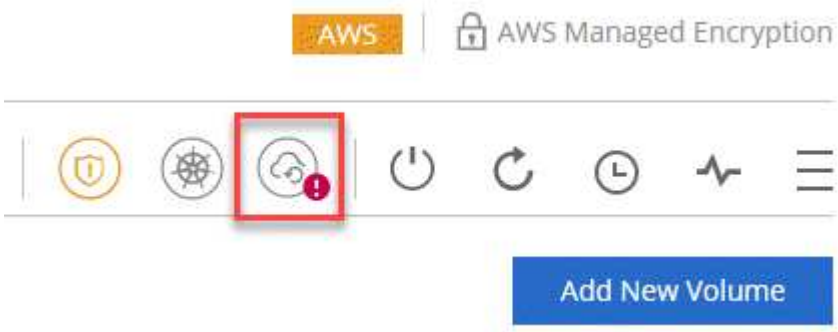
4. バックアップの削除を確定します。

S3 へのバックアップの無効化

S3 へのバックアップを無効にすると、システムの各ボリュームのバックアップが無効になります。既存のバックアップは削除されません。

手順

1. 作業環境を開きます。
2. バックアップ設定アイコンをクリックします。



3. すべてのボリュームを自動的にバックアップする * を無効にし、 * 保存 * をクリックします。

S3 へのバックアップの仕組み

次のセクションでは、 S3 へのバックアップ機能について詳しく説明します。

バックアップの保管場所バックアップノバショ

バックアップコピーは、 Cloud Volumes ONTAP システムが配置されているリージョンのネットアップ所有の S3 バケットに格納されます。

増分バックアップです

データの初回のフルバックアップ以降は、追加のバックアップはすべて増分されるため、変更されたブロックと新しいブロックのみがバックアップされます。

バックアップは午前 **0** 時に作成されます

日次バックアップは、毎日午前 0 時を過ぎた直後に開始されます。現時点では、ユーザが指定した時間にバックアップ処理をスケジュールすることはできません。

バックアップコピーは **Cloud Central** アカウントに関連付けられます

バックアップコピーはに関連付けられます "Cloud Central アカウント" Cloud Manager が配置されます。

同じ Cloud Central アカウントに複数の Cloud Manager システムがある場合、各 Cloud Manager システムには同じバックアップのリストが表示されます。これには、他の Cloud Manager システムの Cloud Volumes ONTAP インスタンスに関連付けられたバックアップが含まれます。

バックアップポリシーはシステム全体に適用されます

保持するバックアップの数はシステムレベルで定義されます。システム上のボリュームごとに異なるポリシーを設定することはできません。

セキュリティ

バックアップデータは、転送中の AES-256 ビット暗号化と TLS 1.2 HTTPS 接続によって保護されます。

データは、セキュアな Direct Connect リンクを経由してサービスに送信され、 AES 256 ビット暗号化によって保管データが保護されます。その後、暗号化されたデータが HTTPS TLS 1.2 接続を使用してクラウドに書き込まれます。データは、セキュアな VPC エンドポイント接続を介してのみ Amazon S3 に転送されるため、インターネット経由ではトラフィックが送信されません。

各ユーザには、サービスが所有する全体的な暗号化キーに加えて、テナントキーが割り当てられます。この要件は、銀行で顧客の安全を確保するために、 1 組のキーを必要とする場合と同様です。クラウドクレデンシャルとしてのすべてのキーは、サービスによって安全に保管され、サービスの保守を担当する特定のネットアップ担当者にのみ制限されます。

制限

- 次のいずれかのタイプのインスタンスを使用する場合、 Cloud Volumes ONTAP システムは最大 20 個のボリュームを S3 にバックアップできます。
  - m4.xlarge
  - m5.xlarge のように指定します
  - R4.xlarge （ R4.xlarge ）
  - R5.xlarge （ R5.xlarge ）

- Cloud Manager 以外で作成したボリュームは、自動的に S3 にバックアップされません。

  たとえば、 ONTAP CLI 、 ONTAP API 、または System Manager からボリュームを作成した場合、そのボリュームは自動的にはバックアップされません。

  これらのボリュームをバックアップする場合は、 S3 へのバックアップを無効にしてから再度有効にする必要があります。

- バックアップからデータをリストアすると、 Cloud Manager は _new_volume へのフルボリュームリストアを実行します。この新しいボリュームは S3 に自動的にバックアップされません。

  リストア処理で作成されたボリュームをバックアップする場合は、 S3 へのバックアップを無効にしてから再度有効にする必要があります。

- バックアップできるボリュームのサイズは 50TB 以下です。
- S3 へのバックアップでは、ボリュームのバックアップを合計 245 個まで保持できます。
- S3 へのバックアップが有効になっている場合は、 Cloud Volumes ONTAP システムで WORM ストレージはサポートされません。

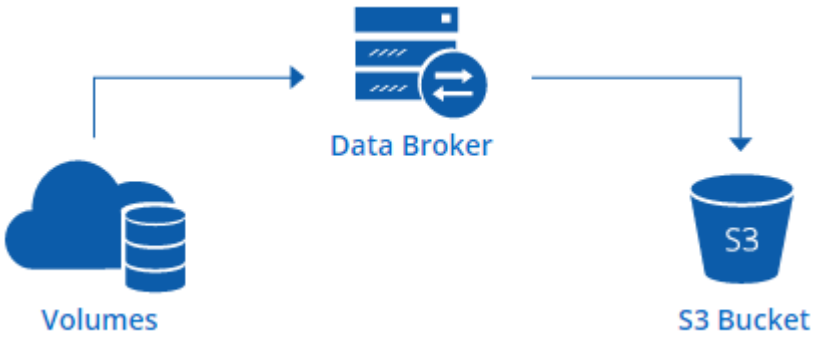
Amazon S3 にデータを同期しています

作業環境をと統合することで、 ONTAP ボリュームのデータを Amazon S3 バケットに同期できます "NetApp Cloud Sync の略"。その後、同期されたデータをセカンダリコピーとして使用したり、 EMR や RedShift などの AWS サービスを使用してデータを処理したりできます。

S3 への同期機能の仕組み

作業環境を Cloud Sync サービスといつでも統合できます。作業環境を統合すると、クラウド同期サービスは、選択したボリュームのデータを単一の S3 バケットに同期します。この統合は、オンプレミスまたは NetApp Private Storage （ NPS ）構成の一部である ONTAP クラスタだけでなく、 Cloud Volumes ONTAP の作業環境でも機能します。

データを同期するために、サービスは VPC でデータブローカーインスタンスを起動します。クラウド同期では、作業環境ごとに 1 つのデータブローカーを使用して、ボリュームから S3 バケットにデータを同期します。最初の同期の後、変更されたデータは毎日午前 0 時に同期されます。



高度なクラウド同期アクションを実行する場合は、 Cloud Sync サービスに直接移動します。ここから、 S3

から NFS サーバへの同期、ボリューム用の異なる S3 バケットの選択、スケジュールの変更などのアクションを実行できます。

14 日間の無料トライアル

新しい Cloud Sync ユーザの場合、最初の 14 日間は無料です。無償トライアルの終了後は、 _sync Relationship _ ごとに 1 時間あたりの料金を支払うか、ライセンスを購入する必要があります。S3 バケットに同期する各ボリュームは、同期関係とみなされます。両方の支払いオプションを Cloud Sync から直接設定するには、ライセンス設定ページを使用します。

ヘルプの入手方法

Cloud Manager の S3 への同期機能または一般的なクラウド同期に関するサポートには、次のオプションを使用します。

- 製品に関する一般的なフィードバック： ng-cloudsync-contact@netapp.com
- テクニカルサポートオプション：
  - ネットアップのクラウド同期コミュニティ
  - 製品内チャット（ Cloud Manager の右下隅）

作業環境と **Cloud Sync** サービスの統合

Cloud Manager から Amazon S3 へボリュームを直接同期する場合は、作業環境と Cloud Sync サービスを統合する必要があります。

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

手順

1. 作業環境を開き、 * S3 への同期 * をクリックします。
2. 「 * Sync * 」をクリックし、画面の指示に従ってデータを S3 に同期します。

> データ保護ボリュームを S3 に同期することはできません。ボリュームは書き込み可能である必要があります。

ボリュームの同期関係の管理

運用環境を Cloud Sync サービスと統合した後は、追加のボリュームを同期したり、ボリュームの同期を停止したり、 Cloud Sync との統合を削除したりできます。

手順

1. [作業環境] ページで、同期関係を管理する作業環境をダブルクリックします。
2. ボリュームの S3 への同期を有効または無効にする場合は、ボリュームを選択し、 * S3 への同期 * または * 同期関係の削除 * をクリックします。
3. 作業環境のすべての同期関係を削除するには、 * S3 への同期 * タブをクリックし、 * 同期の削除 * をクリックします。

   この操作では、同期されたデータは S3 バケットから削除されません。データブローカーが他の同期関係で使用されていない場合、クラウド同期サービスはデータブローカーを削除します。

データプライバシーに関する分析情報を入手できます

Cloud Compliance の詳細をご確認ください

Cloud Compliance は、 AWS と Azure での Cloud Volumes ONTAP 向けのデータプライバシーとコンプライアンスのサービスです。人工知能（ AI ）ベースのテクノロジを使用したクラウドコンプライアンスは、データコンテキストを把握し、 Cloud Volumes ONTAP システム全体で機密データを特定するのに役立ちます。

Cloud Compliance は現在、限定リリースとして提供されています。

"Cloud Compliance のユースケースを紹介します"。

の機能

Cloud Compliance には、コンプライアンスの取り組みに役立つツールがいくつか用意されています。Cloud Compliance を使用すると、次のことができます。

- 個人識別情報（ PII ）の識別
- GDPR 、 CCPA 、 PCI 、 HIPAA の各プライバシー規制の要件に応じて、さまざまな機密情報の範囲を特定します
- データサブジェクトアクセス要求への応答（ dsar ）

コスト

Cloud Compliance は、ネットアップが無償で提供する Cloud Volumes ONTAP 向けのアドオンサービスです。Cloud Compliance をアクティブ化するにはクラウドインスタンスを導入する必要があり、そのインスタンスをクラウドプロバイダが課金します。データがネットワークの外部に流れないため、データの入力または出力に料金は発生しません。

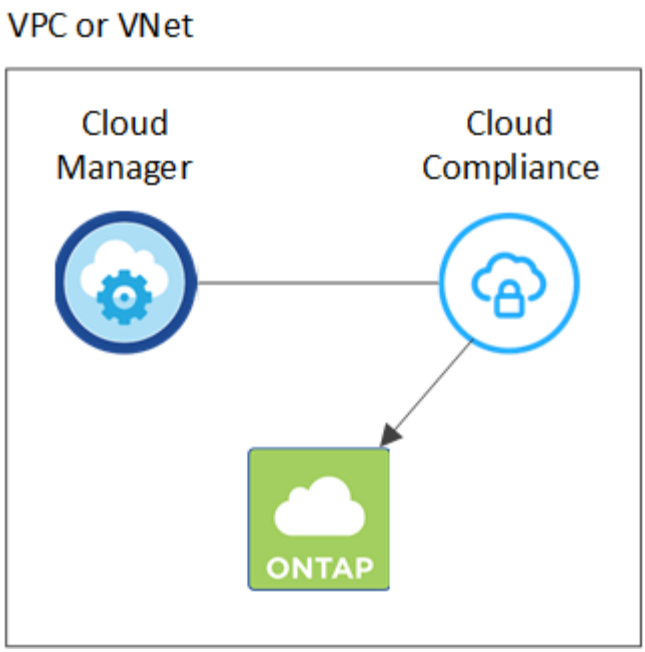
Cloud Compliance の仕組み

Cloud Compliance の仕組みは次のとおりです。

1. 1 つ以上の Cloud Volumes ONTAP システムでクラウドコンプライアンスを有効にします。
2. Cloud Compliance は、 AI のラーニングプロセスを使用してデータをスキャンします。
3. Cloud Manager では、 [* コンプライアンス] をクリックし、提供されているダッシュボードおよびレポートツールを使用して、コンプライアンスの取り組みを支援します。

Cloud Compliance インスタンス

1 つ以上の Cloud Volumes ONTAP システムで Cloud Compliance を有効にすると、 Cloud Manager は要求内の最初の Cloud Volumes ONTAP システムと同じ VPC または VNet に Cloud Compliance インスタンスを導入します。



インスタンスについては、次の点に注意してください。

- Azure では、 Cloud Compliance は 512 GB ディスクの Standard_D16s_v3 VM で実行されます。
- AWS では、クラウドコンプライアンスは m5.mcd インスタンスと 500GB io1 ディスクで実行します。

  m5.mcd を使用できない地域では、代わりに m4.mcd インスタンスに対して Cloud Compliance を実行します。

- インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例：*_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*
- Cloud Manager システムごとに導入される Cloud Compliance インスタンスは 1 つだけです。
- Cloud Compliance ソフトウェアのアップグレードは自動化されているため、心配する必要はありません。

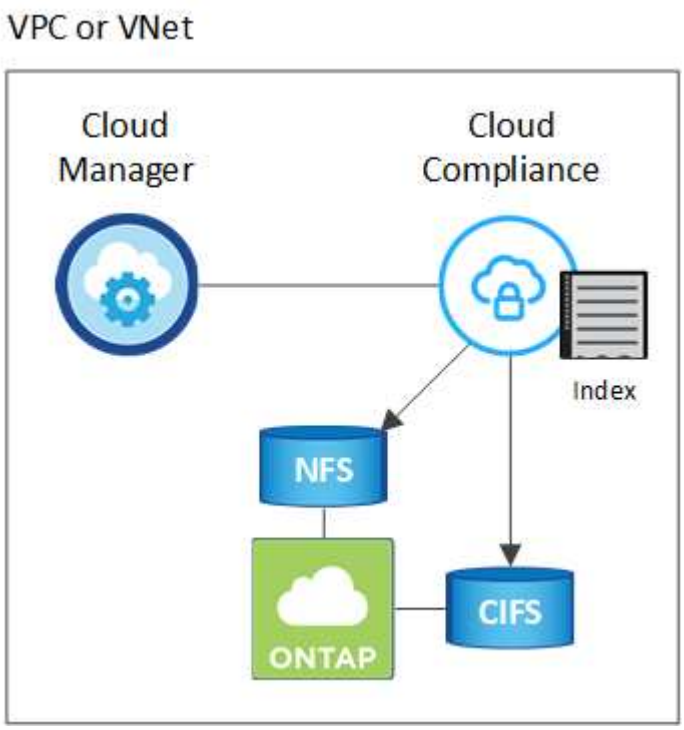
Cloud Compliance は Cloud Volumes ONTAP システム上のデータを継続的にスキャンするため、インスタンスは常時実行している必要があります。

スキャンの動作

Cloud Compliance を有効にすると、データのスキャンがただちに開始され、個人データや機密データが識別されます。

Cloud Compliance は、 NFS ボリュームと CIFS ボリュームをマウントすることで、他のクライアントと同様に Cloud Volumes ONTAP に接続します。NFS ボリュームには読み取り専用で自動的にアクセスされますが、 CIFS ボリュームをスキャンするためには Active Directory のクレデンシャルを指定する必要があります。

Cloud Compliance は、各ボリュームの非構造化データをスキャンして、さまざまな個人情報を取得します。組織のデータをマッピングし、各ファイルを分類して、データ内のエンティティと定義済みパターンを特定して抽出します。スキャンの結果は、個人情報、機密性の高い個人情報、およびデータカテゴリのインデックスです。



初回スキャン後、 Cloud Compliance は各ボリュームを継続的にスキャンして差分変更を検出し、インスタンスの実行を維持することが重要な理由です。

スキャンのオンとオフは作業環境レベルで切り替えることができますが、ボリュームレベルではできません。 "詳細をご確認ください"。

Cloud Compliance がインデックス化する情報

Cloud Compliance は、非構造化データ（ファイル）を収集してインデックスを作成し、カテゴリを割り当てます。Cloud Compliance インデックスに含まれるデータは次のとおりです。

標準メタデータ

Cloud Compliance は、ファイルタイプ、サイズ、作成日、変更日など、ファイルに関する標準のメタデータを収集します。

個人データ

メールアドレス、識別番号、クレジットカード番号など、個人を特定できる情報。 "個人データの詳細については、こちらをご覧ください"。

機密性の高い個人データ

GDPR やその他のプライバシー規制で定義されている、健康データ、民族的起源、政治的見解などの機密情報の特殊な種類。 "機密性の高い個人データの詳細をご覧ください"。

カテゴリ

Cloud Compliance は、スキャンしたデータをさまざまなタイプのカテゴリに分類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 "カテゴリの詳細については、こちらをご覧ください"。

名前エンティティ認識

Cloud Compliance は、 AI を使用して、ドキュメントから自然な人物の名前を抽出します。 "データ主体のアクセスリクエストへの対応について説明します"。

ネットワークの概要

Cloud Manager は、プライベート IP アドレスとセキュリティグループを使用して Cloud Compliance インスタンスを導入し、 Cloud Manager からのインバウンド HTTP 接続を有効にします。この接続を使用すると、Cloud Manager インターフェイスから Cloud Compliance ダッシュボードにアクセスできます。

アウトバウンドルールは完全にオープンです。インスタンスは、 Cloud Manager のプロキシを使用して Cloud Volumes ONTAP システムおよびインターネットに接続します。Cloud Compliance ソフトウェアのアップグレードと使用状況の指標の送信には、インターネットアクセスが必要です。

ネットワーク要件が厳しい場合は、 "Cloud Compliance が連絡するエンドポイントについて説明します"。

> インデックス付けされたデータが Cloud Compliance インスタンスから離れることはありません。データは仮想ネットワークの外部にはリレーされず、 Cloud Manager には送信されません。

コンプライアンス情報へのユーザアクセス

Cloud Manager Admin は、すべての作業環境のコンプライアンス情報を表示できます。

ワークスペース管理者は、アクセス権限を持つシステムのコンプライアンス情報のみを表示できます。ワークスペース管理者が Cloud Manager の作業環境にアクセスできない場合、作業環境のコンプライアンス情報は [コンプライアンス] タブに表示されません。

"Cloud Manager のロールに関する詳細情報"。

『 Getting started with Cloud Compliance for Cloud Volumes ONTAP 』

AWS または Azure で Cloud Compliance for Cloud Volumes ONTAP を使用するには、いくつかの手順を実行します。

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

1 構成が要件を満たしていることを確認します

- Cloud Compliance インスタンスにアウトバウンドのインターネットアクセスが設定されていることを確認します。

  Cloud Manager は、要求に応じて最初の Cloud Volumes ONTAP システムと同じ VPC または VNet にインスタンスを導入します。

- ユーザが、 AWS または Azure に直接接続されているホスト、または Cloud Compliance インスタンスと同じネットワーク内のホストから Cloud Manager のインターフェイスにアクセスできることを確認します（インスタンスにはプライベート IP アドレスが割り当てられます）。
- Cloud Compliance インスタンスの実行を継続できることを確認します。

2 **Cloud Volumes ONTAP** でクラウドへのコンプライアンスを有効化

- 新しい作業環境：作業環境の作成時に必ずクラウドへのコンプライアンスを有効にしてください（デフォルトで有効になっています）。
- 既存の作業環境： * コンプライアンス * をクリックし、必要に応じて作業環境のリストを編集し、 * コンプライアンスダッシュボードを表示 * をクリックします。

3 ボリュームへのアクセスを確認

Cloud Compliance が有効になったので、ボリュームにアクセスできることを確認します。

- クラウドコンプライアンスインスタンスには、各 Cloud Volumes ONTAP サブネットへのネットワーク接続が必要です。
- Cloud Volumes ONTAP のセキュリティグループは、クラウドコンプライアンスインスタンスからのインバウンド接続を許可する必要があります。
- NFS ボリュームのエクスポートポリシーで、 Cloud Compliance インスタンスからのアクセスを許可する必要があります。
- CIFS ボリュームをスキャンするには、 Cloud Compliance で Active Directory のクレデンシャルが必要です。

  コンプライアンス * > * CIFS スキャンステータス * > * CIFS クレデンシャルの編集 * をクリックし、クレデンシャルを入力します。クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、 Cloud Compliance は昇格された権限が必要なデータを確実に読み取ることができます。

4 **Cloud Manager** と **Cloud Compliance** の間の接続を確認

- Cloud Manager のセキュリティグループは、 Cloud Compliance インスタンスとの間のポート 80 経由のインバウンドおよびアウトバウンドのトラフィックを許可する必要があります。
- AWS ネットワークでインターネットアクセスに NAT やプロキシを使用しない場合、 Cloud Manager のセキュリティグループは、 Cloud Compliance インスタンスからの TCP ポート 3128 経由のインバウンドトラフィックを許可する必要があります。

前提条件の確認

Cloud Compliance を有効にする前に、次の前提条件を確認し、サポートされている構成であることを確認してください。Cloud Compliance を有効にしたあとは、コンポーネント間の接続を確認する必要があります。これについては以下で説明します。

アウトバウンドインターネットアクセスを有効にします

Cloud Compliance にはアウトバウンドのインターネットアクセスが必要です。仮想ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、 Cloud Compliance インスタンスがアウトバウンドのインターネットアクセスを使用して次のエンドポイントに接続していることを確認します。

エンドポイント	目的
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
¥ https://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com ¥ https://hub.docker.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com	Cloud Compliance でマニフェストとテンプレートにアクセスしてダウンロードしたり、ログと指標を送信したりできます。

Web ブラウザから **Cloud Compliance** への接続を確認

Cloud Compliance インスタンスは、プライベート IP アドレスを使用して、インデックス付きデータがインターネットにアクセスできないようにします。そのため、 Cloud Manager へのアクセスに使用する Web ブラウザは、そのプライベート IP アドレスに接続する必要があります。この接続は、 AWS または Azure への直接接続（ VPN など）、または Cloud Compliance インスタンスと同じネットワーク内にあるホストから確立できます。

パブリック IP アドレスを使用して Cloud Manager にアクセスしている場合は、ネットワーク内のホストで Web ブラウザが実行されていない可能性があります。

クラウドコンプライアンスを継続的に実現

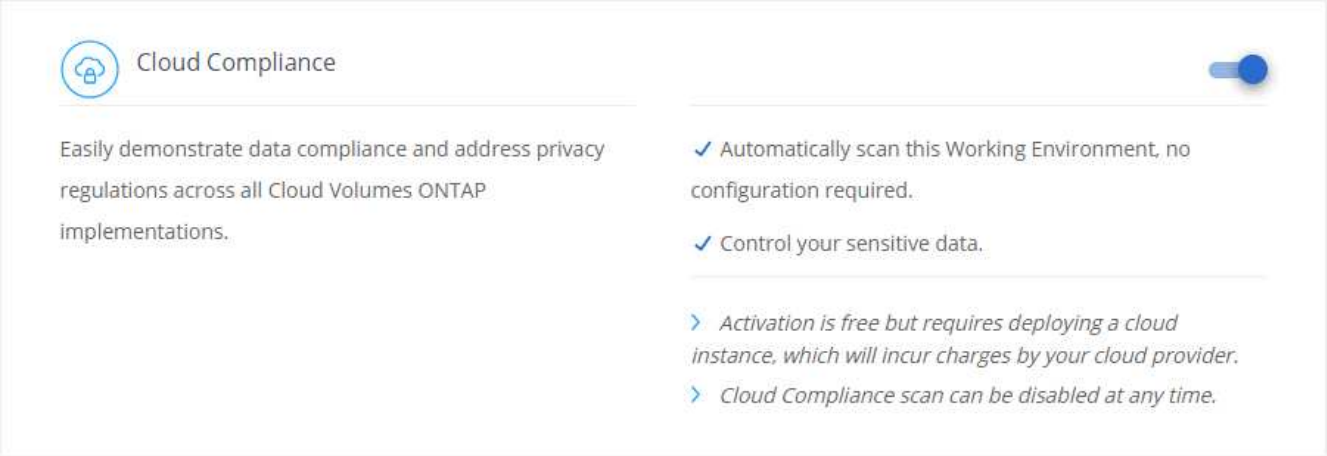
データを継続的にスキャンするには、 Cloud Compliance インスタンスをオンのままにする必要があります。

新しい作業環境での **Cloud Compliance** の有効化

Cloud Compliance は、作業環境ウィザードではデフォルトで有効になります。このオプションは必ず有効にしておいてください。

手順

1. [Cloud Volumes ONTAP の作成 *] をクリックします。
2. クラウドプロバイダとして Amazon Web Services または Microsoft Azure を選択し、シングルノードまたは HA システムを選択します。
3. [詳細と資格情報] ページに入力します。
4. [サービス] ページで、 Cloud Compliance を有効のままにして、 [* 続行] をクリックします。



5. ウィザードの各ページを設定し、システムを導入します。

   ヘルプについては、を参照してください "AWS での Cloud Volumes ONTAP の起動" および "Azure で Cloud Volumes ONTAP を起動します"。

結果

Cloud Volumes ONTAP システムでクラウドコンプライアンスが有効になっています。Cloud Compliance を初めて有効にした場合は、 Cloud Manager によってクラウドプロバイダに Cloud Compliance インスタンスが導入されます。インスタンスが使用可能になると、作成した各ボリュームにインスタンスが書き込まれた時点でデータのスキャンが開始されます。

既存の作業環境で **Cloud Compliance** を有効化

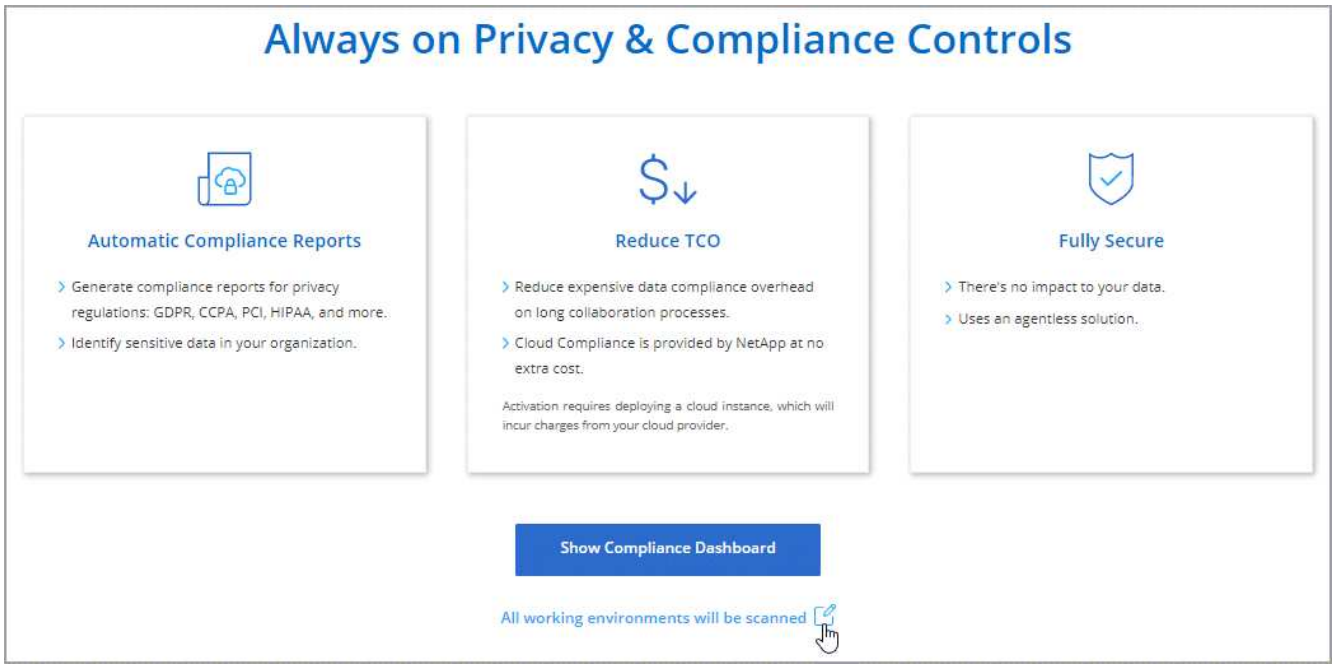
既存の Cloud Volumes ONTAP システムで Cloud Compliance を有効にするには、 Cloud Manager の * Compliance * タブを使用します。

また、作業環境を個別に選択して、 * 作業環境 * タブからクラウドへのコンプライアンスを有効にすることもできます。システムが 1 つしかない場合を除き、完了するまでに時間がかかります。

複数の作業環境での手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. 特定の作業環境で Cloud Compliance を有効にする場合は、編集アイコンをクリックします。

   それ以外の場合は、アクセス可能なすべての作業環境で Cloud Compliance が有効になります。

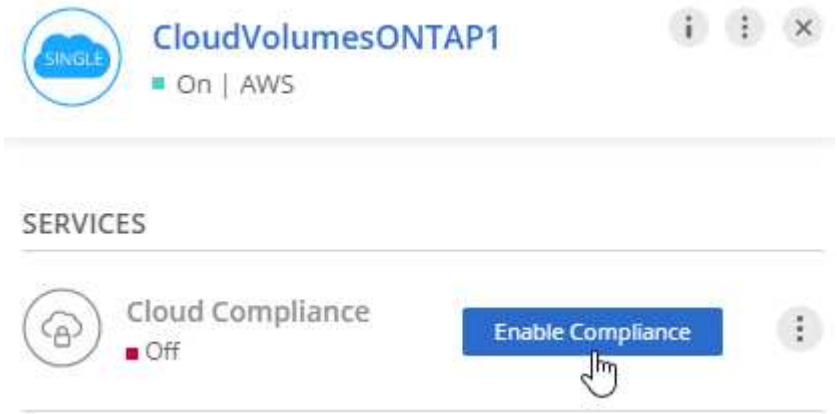


タブのスクリーンショット。"]

3. ［ * 遵守ダッシュボードを表示 * ］ をクリックします。

単一の作業環境での手順

1. Cloud Manager の上部で、 * 作業環境 * をクリックします。
2. 作業環境を選択します。
3. 右側のペインで、 * コンプライアンスを有効にする * をクリックします。



結果

Cloud Compliance を初めて有効にした場合は、 Cloud Manager によってクラウドプロバイダに Cloud Compliance インスタンスが導入されます。

Cloud Compliance は、それぞれの作業環境でデータのスキャンを開始します。データは、 Cloud Compliance の初期スキャンが完了するとすぐに Compliance ダッシュボードに表示されます。所要時間はデータ量によって異なります。数分から数時間かかる場合もあります。

Cloud Compliance がボリュームにアクセスできることの確認

ネットワーク、セキュリティグループ、およびエクスポートポリシーを確認して、 Cloud Compliance が Cloud Volumes ONTAP 上のボリュームにアクセスできることを確認します。CIFS ボリュームにアクセスできるようにするには、 Cloud Compliance に CIFS クレデンシャルを指定する必要があります。

手順

1. クラウドコンプライアンスインスタンスと各 Cloud Volumes ONTAP サブネットの間にネットワーク接続が確立されていることを確認します。

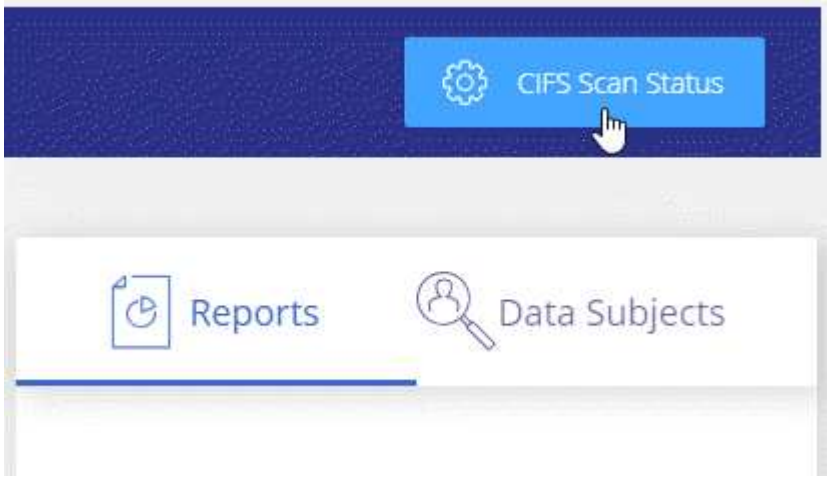
   Cloud Manager は、要求に応じて最初の Cloud Volumes ONTAP システムと同じ VPC または VNet に Cloud Compliance インスタンスを導入します。そのため、一部の Cloud Volumes ONTAP システムが異なるサブネットまたは仮想ネットワークにある場合は、この手順が重要になります。

2. Cloud Volumes ONTAP のセキュリティグループがクラウドコンプライアンスインスタンスからのインバウンドトラフィックを許可していることを確認してください。

   Cloud Compliance インスタンスの IP アドレスからのトラフィックのセキュリティグループを開くか、仮想ネットワーク内からのすべてのトラフィックのセキュリティグループを開くことができます。

3. NFS ボリュームのエクスポートポリシーに Cloud Compliance インスタンスの IP アドレスが含まれていて、各ボリュームのデータにアクセスできることを確認します。
4. CIFS を使用する場合は、 Active Directory クレデンシャルを使用して Cloud Compliance を提供し、 CIFS ボリュームをスキャンできるようにします。

   a. Cloud Manager の上部で、 * Compliance * をクリックします。
   b. 右上の * CIFS Scan Status をクリックします。

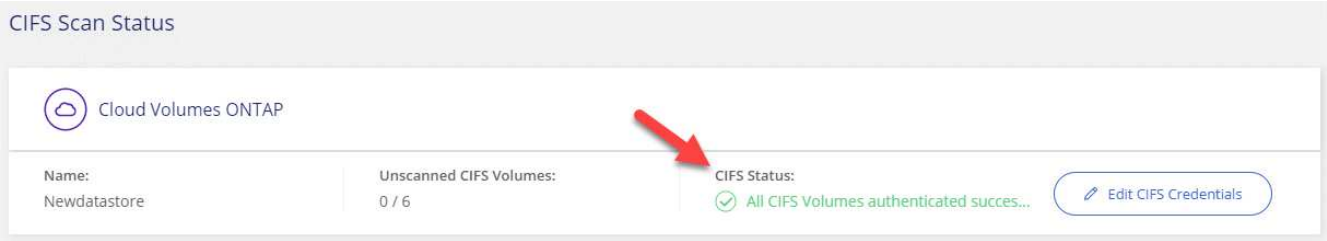


ボタンを示す [Compliance] タブのスクリーンショット。"]

   c. 各 Cloud Volumes ONTAP システムについて、 * CIFS クレデンシャルの編集 * をクリックし、クラウド・コンプライアンスがシステム上の CIFS ボリュームにアクセスするために必要なユーザ名とパスワードを入力します。

      クレデンシャルは読み取り専用ですが、管理者のクレデンシャルを指定することで、 Cloud Compliance は昇格された権限が必要なデータを読み取ることができます。クレデンシャルは Cloud Compliance インスタンスに保存されます。

クレデンシャルを入力すると、すべての CIFS ボリュームが認証されたことを示すメッセージが表示されます。



Cloud Manager から Cloud Compliance にアクセスできることの確認

Cloud Manager と Cloud Compliance の間の接続を確認し、 Cloud Compliance が検出したコンプライアンスの分析情報を確認します。

手順

1. Cloud Manager のセキュリティグループで、 Cloud Compliance インスタンスとの間のポート 80 経由のインバウンドおよびアウトバウンドのトラフィックが許可されていることを確認してください。

   この接続により、 [コンプライアンス] タブに情報を表示できます。

2. AWS ネットワークがインターネットアクセスに NAT やプロキシを使用しない場合は、 Cloud Manager のセキュリティグループを変更して、 Cloud Compliance インスタンスからの TCP ポート 3128 経由のインバウンドトラフィックを許可します。

   これは、 Cloud Compliance インスタンスが、インターネットへのアクセスにプロキシとして Cloud Manager を使用するためです。

   このポートは、すべての新しい Cloud Manager インスタンスで、バージョン 3.7.5 以降でデフォルトで開きます。それより前のバージョンで作成された Cloud Manager インスタンスでは開きません。

プライベートデータの可視化と管理を実現

組織内の個人データと機密性の高い個人データに関する詳細を表示することで、個人データを管理できます。また、データに含まれる Cloud Compliance のカテゴリとファイルタイプを確認して、情報を可視化することもできます。

個人データ

Cloud Compliance は、データ内の特定の単語、文字列、パターン（ Regex ）を自動的に識別します。たとえば、個人識別情報（ PII ）、クレジットカード番号、社会保障番号、銀行口座番号などです。 すべてのリストを参照してください。

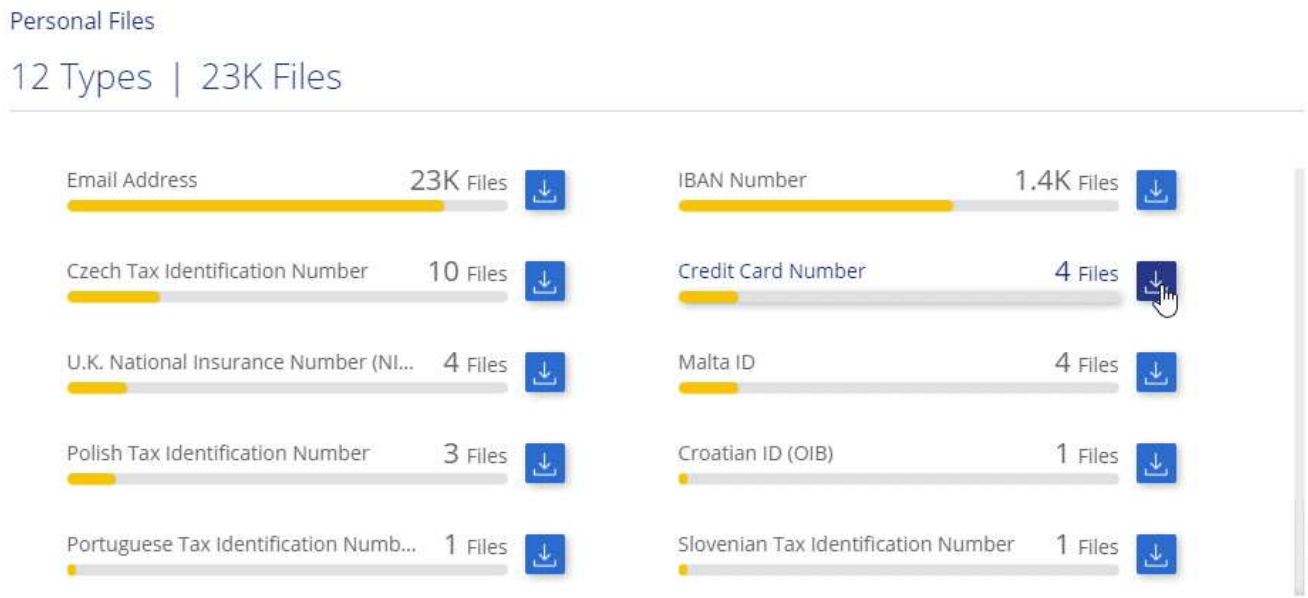
一部のタイプの個人データについては、 Cloud Compliance は _ 近接性検証 _ を使用してその結果を検証します。検証は、見つかった個人データに近接した 1 つまたは複数の定義済みキーワードを検索することによって行われます。たとえば、 Cloud Compliance は米国を識別しますソーシャルセキュリティ番号（ SSN ）は、 IT の横に近接語（ *SSN_or_social security* など）が表示されている場合、 SSN として表示されます。

以下のリストを参照してください Cloud Compliance がプロキシミティ検証を使用する状況を示します。

個人データを含むファイルを表示する

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. メイン画面から上位 2 つのファイルタイプのいずれかの詳細を直接ダウンロードするか、「 * すべて表示 * 」をクリックして、見つかった個人データタイプのリストをダウンロードします。



ダイアログボックスのスクリーンショット。結果は、ファイルの詳細を含む CSV ファイルになります。"]

個人データの種類

ファイルに含まれる個人データは、一般的な個人データまたは国 ID です。3 番目の列は、 Cloud Compliance で使用されているかどうかを示します 近接性検証 識別子の調査結果を検証します。

を入力します	識別子	近接性検証：
全般	E メールアドレス	いいえ
	クレジットカード番号	いいえ
	IBAN 番号（国際銀行口座番号）	いいえ
	IP アドレス	はい。

を入力します	識別子	近接性検証：
国家識別番号	ベルギー ID （ Numero National ）	はい。
	ブルガリア語 ID （統一市民番号）	はい。
	キプロス税識別番号（ TIC ）	はい。
	デンマーク税識別番号（ CPR ）	はい。
	エストニア ID （イスクウッド）	はい。
	フィンランド ID （ henkilrotunnus ）	はい。
	フランス税識別番号（ SPI ）	はい。
	ドイツの納税者番号（ Steuerliche Identifyikationsnummer ）	はい。
	ハンガリー語税識別番号（ Adó azonosí tó Jel ）	はい。
	アイルランド ID （ PPS ）	はい。
	イスラエルの身分証明書	はい。
	イタリア ID （コディス・フスセール）	はい。
	ラトビア税識別番号	はい。
	リトアニア語 ID （ Asmens kodas ）	はい。
	ルクセンブルク iD	はい。
	マルタの身分証明書	はい。
	オランダ ID （ BSN ）	はい。
	ポーランド税識別番号	はい。
	ポルトガル語税識別番号（ NIF ）	はい。
	ルーマニア語税識別番号	はい。
	スロバキア語税識別番号	はい。
	スロベニアの税識別番号	はい。
	南アフリカ ID	はい。
	スペイン語税識別番号	はい。
	スウェーデン税識別番号	はい。
	英国国民保険番号（日野）	はい。
	米国社会保障番号（ SSN ）	はい。

機密性の高い個人データ

Cloud Compliance は、などのプライバシー規制に従って、機密性の高い特別な個人情報を自動的に識別します "GDPR の第 9 、 10 記事"。たとえば、人の健康、民族の起源、性的指向に関する情報などです。 すべてのリストを参照してください。

Cloud Compliance は、人工知能（ AI ）、自然言語処理（ NLP ）、機械学習（ ML ）、コグニティブコンピューティング（ CC ）を使用して、スキャンするコンテンツの意味を理解し、エンティティを抽出してそれに

応じて分類します。

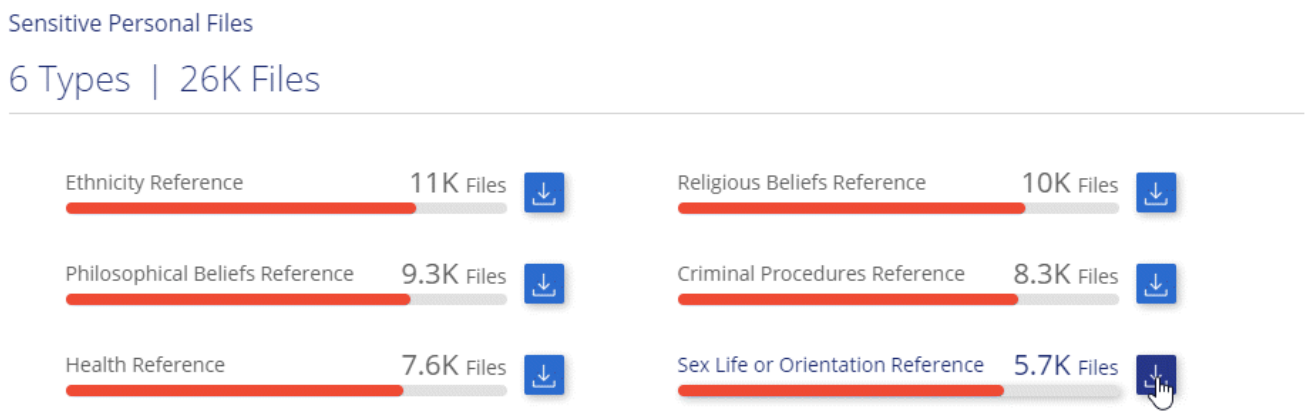
たとえば、機密性の高い GDPR データカテゴリの 1 つは民族起源です。クラウドコンプライアンスは、 NLP の能力を備えているため、「ジョージ・メキシカン」（ GDPR の第 9 条で規定されている機密データを示す）と「ジョージ・イメキシカン・フード」を読み取る文との違いを区別できます。

> 機密性の高い個人データをスキャンする場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

機密性の高い個人データを含むファイルを表示する

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. メイン画面から上位 2 つのファイルタイプのいずれかの詳細を直接ダウンロードするか、「 * すべて表示 * 」をクリックして、見つかった機密性の高い個人データタイプのリストをダウンロードします。



機密性の高い個人データのタイプ

Cloud Compliance がファイルに保存できる機密性の高い個人データには、次のものがあります。

刑事手続きの参照
: 天然人の犯罪に関するデータ。

『民族リファレンス』を参照してください
: 自然な人の人種または民族の起源に関するデータ。

健全性リファレンス
: 自然な人の健康に関するデータ。

哲学の信仰の参照
: 自然な人の哲学的信念に関するデータ。

宗教的信条参照
: 自然な人の宗教的信条に関するデータ。

性別生命または方向の参照

自然人の性生活や性的指向に関するデータ。

カテゴリ

Cloud Compliance は、スキャンしたデータをさまざまなタイプのカテゴリに分類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 カテゴリのリストを参照してください。

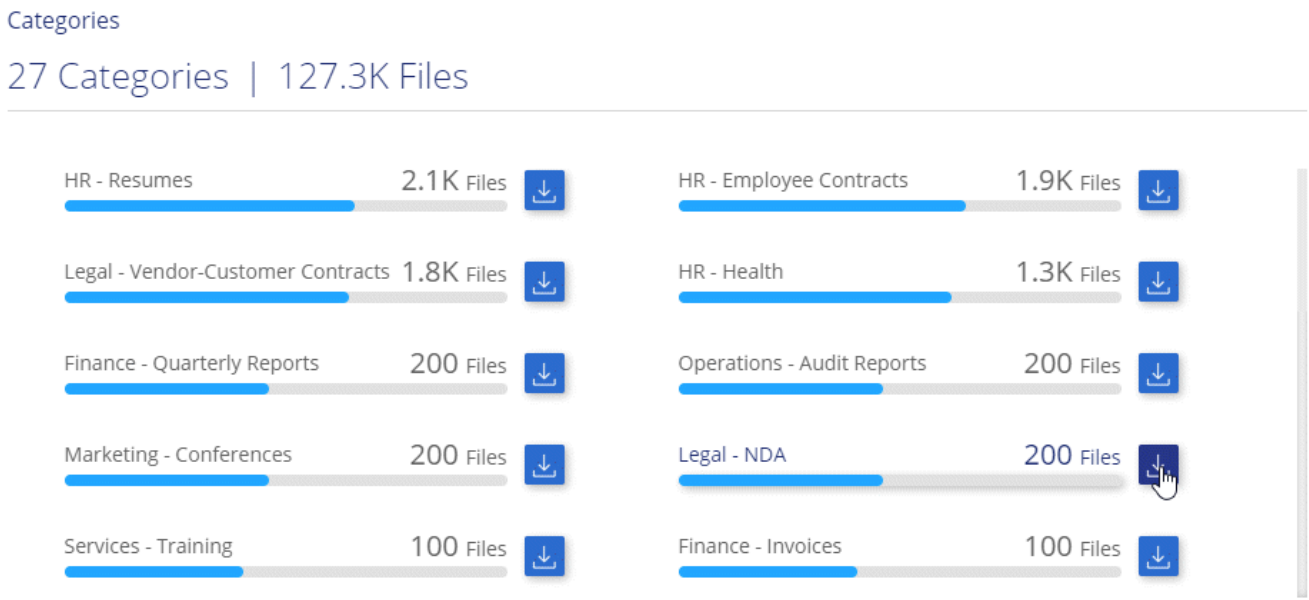
カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、履歴書や従業員契約などのカテゴリには機密データを含めることができます。CSV レポートをダウンロードすると、従業員契約が安全でない場所に保存される場合があります。その後、その問題を修正できます。

カテゴリでは英語のみがサポートされています。言語のサポートは、あとで追加されます。

カテゴリ別にファイルを表示します

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. メイン画面から上位 4 つのファイルタイプのいずれかの詳細を直接ダウンロードするか、「 * すべて表示 * 」をクリックして、任意のカテゴリのリストをダウンロードします。



カテゴリのタイプ

Cloud Compliance では、次のようにデータが分類されます。

財務

- 貸借対照表
- 注文書
- 請求書

- 四半期ごとのレポート

時間

- バックグラウンドチェック
- 報酬プラン
- 従業員の契約
- 従業員レビュー
- 健常性
- 再開します

法律

- NDA
- ベンダー - お客様との契約

マーケティング

- キャンペーン
- 会議

処理

- 監査レポート

営業

- SO 番号

サービス

- RFI （ RFI ）
- RFP
- トレーニング

サポート

- 苦情やチケット

その他

- アーカイブファイル
- 音声
- CAD ファイル
- コード
- 実行可能ファイル
- イメージ

ファイルの種類

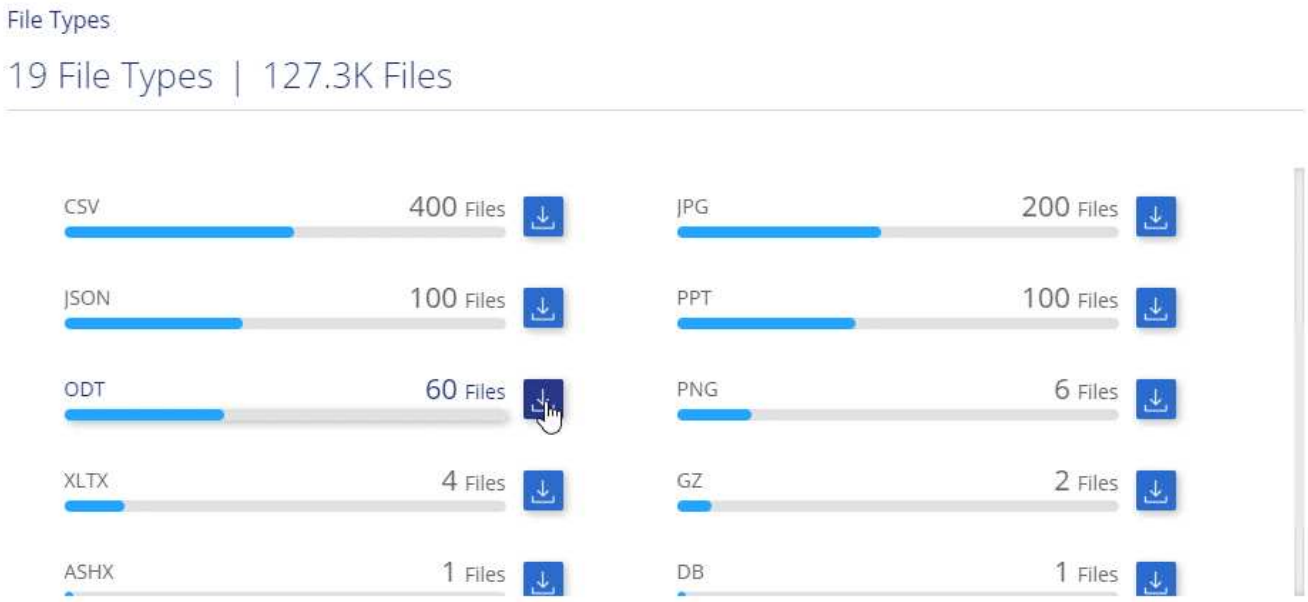
Cloud Compliance は、スキャンしたデータをファイルタイプ別に分類し、Cloud Compliance では、スキャンで見つかったすべてのファイルタイプを表示できます。

ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。たとえば ' 組織に関する非常に機密性の高い情報を含む CAD ファイルを保存する場合がありますセキュリティで保護されていない場合は、権限を制限するか、ファイルを別の場所に移動することで、機密データを制御できます。

ファイルタイプを表示しています

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. メイン画面から上位 4 つのファイルタイプのいずれかの詳細を直接ダウンロードするか、 * すべて表示 * をクリックして、任意のファイルタイプのリストをダウンロードします。



見つかった情報の正確性

ネットアップでは、 Cloud Compliance によって識別される個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

以下の表は、ネットアップのテストに基づく、 Cloud Compliance が検出した情報の正確さを示しています。精度 _ と _ リコール _ で分解します。

精度（ **Precision** ）

どのようなクラウドコンプライアンスが見つかったかが正しく特定された可能性。たとえば、個人データの正確な割合が 90% の場合、個人情報を含むと識別された 10 個中 9 個のファイルに個人情報が実際に含まれていることを意味します。10 個のファイルのうち 1 個はフォールスポジティブです。

取り消し

クラウドコンプライアンスが何をすべきかを判断する確率。たとえば、個人データのリコール率が 70% の場合、 Cloud Compliance では、実際に個人情報が含まれている 10 個中 7 個のファイルを識別できます。Cloud Compliance は、データの 30% を見逃すことになり、ダッシュボードには表示されません。

Cloud Compliance は可用性が限定的にリリースされており、常に結果の正確さが向上しています。これらの改善点は、今後の Cloud Compliance リリースで自動的に提供される予定です。

を入力します	精度（ **Precision** ）	取り消し
個人データ - 一般	90% ~ 95%	60% 〜 80%
個人データ - 国 ID	30% ~ 60%	40% ~ 60%
機密性の高い個人データ	80% ~ 95%	20% ~ 30%
カテゴリ	90% ~ 97%	60% 〜 80%

各ファイルリストレポート（ **CSV** ファイル）に含まれる内容

ダッシュボードでは、特定されたファイルの詳細を含むファイルリスト（ CSV 形式）をダウンロードできます。10 、 000 件を超える結果がある場合は、上位 10 、 000 件のみがリストに表示されます（サポートはあとで追加されます）。

各ファイルリストには、次の情報が含まれています。

- ファイル名
- 場所のタイプ
- 場所
- ファイルパス
- ファイルタイプ
- カテゴリ
- 個人情報
- 機密性の高い個人情報
- 削除の検出日

  削除の検出日は、ファイルが削除または移動された日付を示します。これにより、機密ファイルがいつ移動されたかを識別できます。削除されたファイルは、ダッシュボードに表示されるファイル番号の一部ではありません。ファイルは CSV レポートにのみ表示されます。

プライバシーリスク評価レポートの表示

プライバシーリスクアセスメントレポートには、 GDPR や CCPA などのプライバシー規制に必要な、組織のプライバシーリスクステータスの概要が記載されています。

ネットアップでは、 Cloud Compliance によって識別される個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

このレポートには次の情報が含まれます。

準拠ステータス
: 重要度スコア（詳細については以下を参照）と、機密性の低い個人または機密性の高い個人のデータの分布。

評価の概要
: 検出された個人データの種類とデータのカテゴリの内訳。

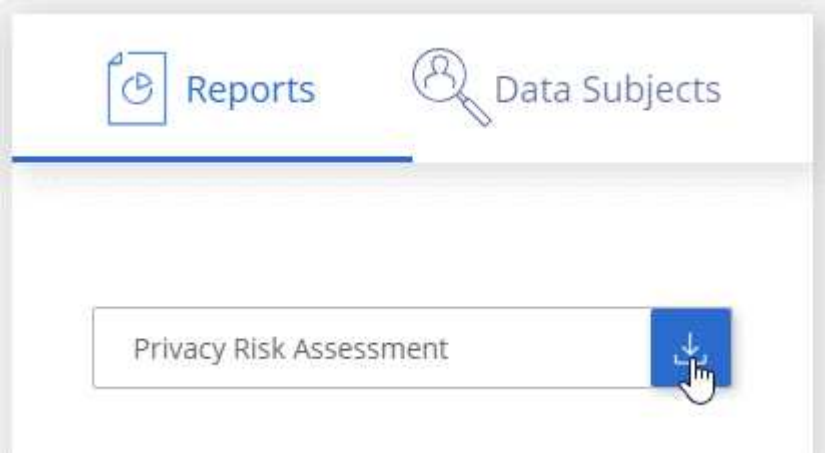
この評価のデータ主体
: 国 ID が見つかった場所別の人の数。

プライバシーリスク評価レポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. [**Reports**] の下にある [* Privacy Risk Assessment*] の横にあるダウンロードアイコンをクリックします。



結果

Cloud Compliance によって PDF レポートが生成され、必要に応じて他のグループに送信して確認できます。

重要度スコア

Cloud Compliance は、次の 3 つの変数に基づいて、プライバシーリスク評価レポートの重大度スコアを計算します。

- すべてのデータの個人データの割合。
- すべてのデータの機密性の高い個人データの割合。

- データ主体を含むファイルの割合。国 ID 、社会保障番号、税務 ID 番号などの国 ID によって決定されます。

スコアの決定に使用されるロジックは次のとおりです。

重要度スコア	ロジック
0	3 つの変数はすべて 0% です
1.	変数の 1 つが 0% を超えています
2.	変数の 1 つが 3% を超えています
3.	2 つの変数が 3% を超えています
4.	3 つの変数が 3% を超えています
5.	変数の 1 つが 6% より大きい
6.	2 つの変数が 6% より大きくなっています
7.	3 つの変数が 6% より大きい
8.	変数の 1 つが 15% より大きくなっています
9.	変数のうちの 2 つが 15% より大きくなっています
10.	変数のうちの 3 つが 15% より大きくなっています

データ主体アクセス要求に応答します

データ主体アクセス要求（ dsar ）に応答するには、件名のフルネームまたは既知の識別子（電子メールアドレスなど）を検索し、レポートをダウンロードします。このレポートは、企業が GDPR や同様のデータプライバシー法を遵守する必要がある場合に役立つように作成されています。

> ネットアップでは、 Cloud Compliance によって識別される個人データと機密性の高い個人データの正確性を 100% 保証することはできません。必ずデータを確認して情報を検証してください。

データ主体アクセス要求とは

欧州 GDPR などのプライバシー規制により、データ主体（お客様や従業員など）は個人データにアクセスする権利が付与されます。データ主体がこの情報を要求すると ' これは dsar (データ主体アクセス要求) と呼ばれます組織は、これらの要求に「期日前に」、受領後 1 か月以内に対応する必要があります。

クラウドコンプライアンスは、どのようにして顧客のニーズに対応するのに役立ちますか？

データ主体検索を実行すると、そのユーザーの名前または ID を持つすべてのファイルが Cloud Compliance によって検索されます。Cloud Compliance は、名前または識別子に関する最新のインデックス付け済みデータをチェックします。新しいスキャンは開始されません。

検索が完了したら、ファイルのリストまたはデータサブジェクトアクセス要求レポートをダウンロードできます。このレポートでは、データから得た情報を集約して、利用者に返すことができる法的条件にします。

データ主体の検索とレポートのダウンロード

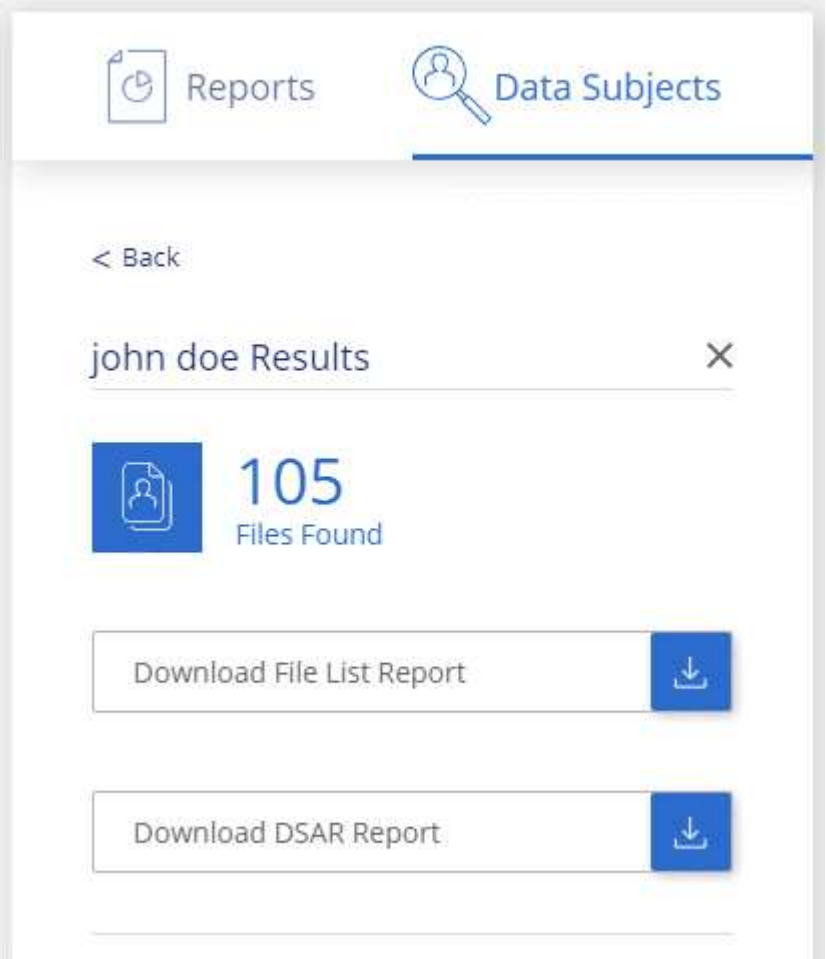
データ主体のフルネームまたは既知の識別子を検索し、ファイルリストレポートまたは dsar レポートをダウンロードします。で検索できます "個人情報の種類"。

> データ主体の名前を検索する場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

手順

1. Cloud Manager の上部で、 * Compliance * をクリックします。
2. [* データ主体 *] をクリックします。
3. データ主体のフルネームまたは既知の識別子を検索します

   次の例では、 name *John doe*: を検索しています。



4. 次のいずれかのオプションを選択します。
   - * ファイルリストレポートのダウンロード *: データ主体に関する情報を含むファイルのリスト。

> 10 、 000 件を超える結果がある場合、レポートに表示されるのはトップ 10 、 000 件だけです（サポートはあとで追加されます）。

- **Download dsar Report**: アクセス要求に対する正式な応答で、データ主体に送信できます。このレポートには、データ主体に基づいて Cloud Compliance によって検出されたデータに基づいて自動的に生成された情報が含まれます。この情報は、テンプレートとして使用するように設計されています。データ主体に送信する前に、フォームに必要事項を記入して内部で確認してください。

Cloud Compliance の無効化

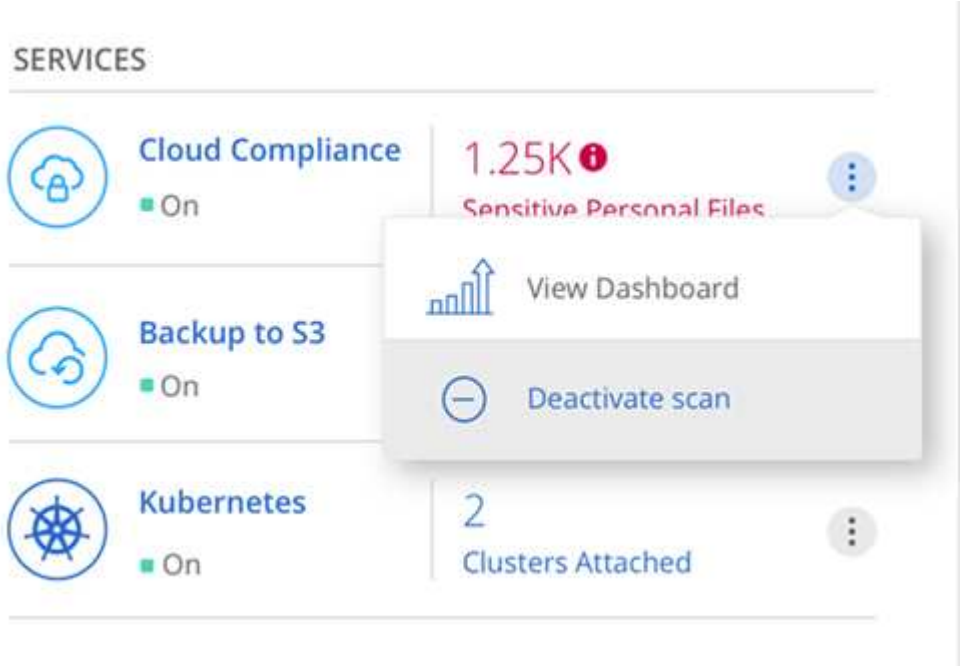
必要に応じて、 Cloud Compliance のスキャンを停止して、 1 つ以上の作業環境をスキャンすることができます。また、 Cloud Volumes ONTAP システムでクラウドコンプライアンスを使用する必要がなくなった場合は、クラウドコンプライアンスインスタンスを削除することもできます。

作業環境のコンプライアンススキャンを非アクティブにします

スキャンを非アクティブ化すると、 Cloud Compliance はシステム上のデータをスキャンしなくなり、インデックス付けされたコンプライアンス分析情報を Cloud Compliance インスタンスから削除します（作業環境自体のデータは削除されません）。

手順

1. Cloud Manager の上部で、 * 作業環境 * をクリックします。
2. 作業環境を選択します。
3. 右側のパネルで、 Cloud Compliance サービスのアクションアイコンをクリックし、 * スキャンを非アクティブ化 * を選択します。



Cloud Compliance インスタンスを削除しています

Cloud Volumes ONTAP でクラウドコンプライアンスを使用する必要がなくなった場合は、クラウドコンプライアンスインスタンスを削除できます。インスタンスを削除すると、インデックス付きデータが存在する関連ディスクも削除されます。

ステップ

1. クラウドプロバイダのコンソールに移動して、 Cloud Compliance インスタンスを削除します。

   インスタンスの名前は *CloudCompliancy_with* で、生成されたハッシュ（ *UUID* ）を連結しています。例：*_CloudCompliion-16bb6564-38ad-40802-9a92-36f5fd2f71c7*

Cloud Compliance についての FAQ です

この FAQ は、質問に対する簡単な回答を探している場合に役立ちます。

クラウドコンプライアンスとは

Cloud Compliance は、ネットアップの新しいクラウドソリューションです。人工知能（ AI ）ベースのテクノロジを使用したクラウドコンプライアンスにより、組織はデータコンテキストを把握し、 AWS または Azure でホストされている Cloud Volumes ONTAP システム全体で機密データを特定できます。

Cloud Compliance では、データプライバシーや機密性に関する新しいデータコンプライアンス規制（ GDPR 、 CCPA など）に対応するための事前定義されたパラメータ（機密情報の種類やカテゴリなど）が提供されます。

Cloud Compliance を使用すべき理由

Cloud Compliance では、データを通じて次のことを支援できます。

- データコンプライアンスやプライバシーの規制に準拠
- データ保持ポリシーに準拠
- GDPR 、 CCPA 、その他のデータプライバシー規制の要件に応じて、特定のデータを簡単に検索し、レポートを作成できます。

Cloud Compliance の一般的なユースケースを教えてください。

- 個人識別情報（ PII ）を識別します。
- GDPR および CCPA のプライバシー規制の要件に応じて、さまざまな機密情報の範囲を特定します。
- データプライバシーに関する新しい規制や今後の規制に対応できます。

"Cloud Compliance のユースケースについて詳しくは、こちらをご覧ください"。

Cloud Compliance でスキャンできるデータの種類を教えてください。

Cloud Compliance では、 NFS および CIFS プロトコル経由の非構造化データのスキャンがサポートされます。現在、 Cloud Compliance は、 Cloud Volumes ONTAP で管理されているデータをスキャンします。

"スキャンの仕組みを説明します"。

サポートされているクラウドプロバイダを教えてください。

Cloud Compliance は、 Cloud Manager の一部として機能し、現在は AWS と Azure をサポートしています。

これにより、異なるクラウドプロバイダ間で統一されたプライバシー可視性を実現できます。Google Cloud Platform （ GCP ）のサポートがまもなく追加されます。

Cloud Compliance へのアクセス方法

Cloud Compliance の運用と管理には Cloud Manager を使用します。Cloud Compliance 機能には、 Cloud Manager の * Compliance * タブからアクセスできます。

Cloud Compliance の仕組み

Cloud Compliance では、 Cloud Manager システムと Cloud Volumes ONTAP インスタンスのほかに、もう 1 つの人工知能レイヤを導入します。次に、 Cloud Volumes ONTAP 上のデータをスキャンし、見つかったデータのインデックスを作成します。

"Cloud Compliance の仕組みをご覧ください"。

クラウドのコンプライアンスコストはいくらですか？

クラウドコンプライアンスは Cloud Volumes ONTAP の一部として提供され、追加コストは不要です。機能をカスタマイズするには、将来的に追加のコストが必要になる可能性があります。

> Cloud Compliance では、クラウドプロバイダにインスタンスを導入する必要があり、そのインスタンスをクラウドプロバイダが課金します。

Cloud Compliance はどのくらいの頻度でデータをスキャンしますか？

データが頻繁に変更されるため、 Cloud Compliance はデータに影響を与えることなくデータを継続的にスキャンします。データの初回スキャンには時間がかかる場合がありますが、その後のスキャンでは差分変更のみがスキャンされるため、システムのスキャン時間が短縮されます。

"スキャンの仕組みを説明します"。

Cloud Compliance はレポートを提供しますか。

はい。Cloud Compliance から提供される情報は、組織内の他の関係者にも関係があるため、レポートを作成して分析情報を共有することができます。

Cloud Compliance で使用できるレポートは次のとおりです。

プライバシーリスクアセスメントレポート

データからプライバシーに関する情報を収集し、プライバシーリスクスコアを取得します。 "詳細はこちら。"。

Data Subject Access Request レポート

データサブジェクトの特定の名前または個人 ID に関する情報を含むすべてのファイルのレポートを抽出できます。 "詳細はこちら。"。

特定の情報タイプに関するレポート

個人データや機密性の高い個人データを含む、特定されたファイルの詳細を含むレポートを利用できます。カテゴリおよびファイルタイプ別に分類されたファイルを表示することもできます。 "詳細はこち

ら。"。

クラウドコンプライアンスに必要なインスタンスまたは VM のタイプはどれですか？

- Azure では、 Cloud Compliance は 512 GB ディスクの Standard_D16s_v3 VM で実行されます。
- AWS では、クラウドコンプライアンスは m5.mcd インスタンスと 500GB io1 ディスクで実行します。

  m5.mcd を使用できない地域では、代わりに m4.mcd インスタンスに対して Cloud Compliance を実行します。

"Cloud Compliance の仕組みをご覧ください"。

スキャンのパフォーマンスは変化しますか？

スキャンパフォーマンスは、クラウド環境のネットワーク帯域幅と平均ファイルサイズによって異なります。

Cloud Compliance を有効にする方法

Cloud Compliance は、新しい作業環境の作成時に有効にすることができます。既存の作業環境で有効にするには、 * コンプライアンス * タブ（最初の活動化のみ）を使用するか、特定の作業環境を選択します。

"開始方法をご確認ください"。

> Cloud Compliance をアクティブにすると、最初のスキャンがすぐに開始されます。コンプライアンスの結果はすぐ後に表示されます。

Cloud Compliance を無効にする方法

個々の作業環境を選択したら、作業環境のページで Cloud Compliance を無効にすることができます。

"詳細はこちら。"。

> Cloud Compliance インスタンスを完全に削除するには、クラウドプロバイダのポータルから Cloud Compliance インスタンスを手動で削除します。

Cloud Volumes ONTAP でデータ階層化が有効になっている場合はどうなりますか。

コールドデータをオブジェクトストレージに階層化する Cloud Volumes ONTAP システムでは、クラウド準拠を有効にすることができます。データの階層化が有効になっている場合、 Cloud Compliance は、ディスクに格納されているすべてのデータと、オブジェクトストレージに階層化されたコールドデータをスキャンします。

コンプライアンススキャンはコールドデータを加熱しません — コールドデータを保存し ' オブジェクトストレージに階層化します

クラウドコンプライアンスを使用してオンプレミスの ONTAP ストレージをスキャンできますか。

いいえCloud Compliance は、現在 Cloud Manager の一部として提供されており、 Cloud Volumes ONTAP を

サポートしています。Cloud Volumes Service や Azure NetApp Files などのクラウドサービスを追加して、クラウドコンプライアンスをサポートすることを計画しています。

Cloud Compliance から組織に通知を送信できますか？

いいえ。ただし、組織内で共有できるステータスレポートはダウンロードできます。

組織のニーズに合わせてサービスをカスタマイズできますか。

Cloud Compliance は、設定不要でデータを分析します。これらの分析情報を抽出して、組織のニーズに活用できます。

クラウドコンプライアンス情報を特定のユーザに制限できますか。

はい。 Cloud Compliance は Cloud Manager に完全に統合されています。Cloud Manager ユーザは、ワークスペースの権限に基づいて表示可能な作業環境の情報のみを表示できます。

"詳細はこちら。"。

Cloud Volumes ONTAP の管理

Cloud Volumes ONTAP に接続しています

Cloud Volumes ONTAP の高度な管理を実行する必要がある場合は、 OnCommand System Manager またはコマンドラインインターフェイスを使用します。

OnCommand System Manager に接続しています

Cloud Volumes ONTAP システム上で実行されるブラウザベースの管理ツールである OnCommand System Manager から Cloud Volumes ONTAP タスクを実行する必要がある場合があります。たとえば、 LUN を作成する場合は、 System Manager を使用する必要があります。

作業を開始する前に

Cloud Manager にアクセスするコンピュータは、 Cloud Volumes ONTAP にネットワーク接続している必要があります。たとえば、 AWS または Azure の Jump ホストから Cloud Manager にログインする必要がある場合があります。

> 複数の AWS 可用性ゾーンに導入されている場合、 Cloud Volumes ONTAP HA 構成では、クラスタ管理インターフェイスにフローティング IP アドレスが使用されます。つまり、外部ルーティングは使用できません。同じルーティングドメインの一部であるホストから接続する必要があります。

手順

1. [作業環境] ページで、 System Manager で管理する Cloud Volumes ONTAP システムをダブルクリックします。
2. メニューアイコンをクリックし、 * Advanced > System Manager * をクリックします。
3. [* 起動 *] をクリックします。

   System Manager が新しいブラウザタブにロードされます。

4. ログイン画面で、 [ユーザー名] フィールドに「 * admin * 」と入力し、作業環境の作成時に指定したパスワードを入力して、 [* サインイン *] をクリックします。

結果

System Manager コンソールがロードされます。これで、 Cloud Volumes ONTAP の管理に使用できるようになりました。

Cloud Volumes ONTAP CLI に接続しています

Cloud Volumes ONTAP CLI を使用すると、すべての管理コマンドを実行できます。高度なタスクを実行する場合や、 CLI を使用する場合に適しています。Secure Shell （ SSH ）を使用して CLI に接続できます。

作業を開始する前に

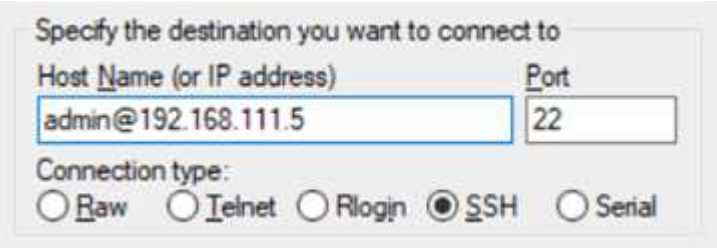
SSH を使用して Cloud Volumes に接続するホスト ONTAP は、 Cloud Volumes ONTAP にネットワーク接続している必要があります。たとえば、 AWS または Azure の Jump ホストから SSH を使用する必要がある場合があります。

複数の AZS に導入されている場合、 Cloud Volumes ONTAP HA 構成では、クラスタ管理インターフェイスにフローティング IP アドレスが使用されます。これは、外部ルーティングが使用できないことを意味します。同じルーティングドメインの一部であるホストから接続する必要があります。

手順

1. Cloud Manager で、クラスタ管理インターフェイスの IP アドレスを特定します。
   a. [作業環境] ページで、 Cloud Volumes ONTAP システムを選択します。
   b. 右側のペインに表示されるクラスタ管理 IP アドレスをコピーします。
2. SSH を使用して、 admin アカウントを使用してクラスタ管理インターフェイスの IP アドレスに接続します。
   - 例 *

     次の図は、 PuTTY を使用した例を示しています。



3. ログインプロンプトで、 admin アカウントのパスワードを入力します。
   - 例 *

```
Password: ********
COT2::>
```

Cloud Volumes ONTAP ソフトウェアを更新しています

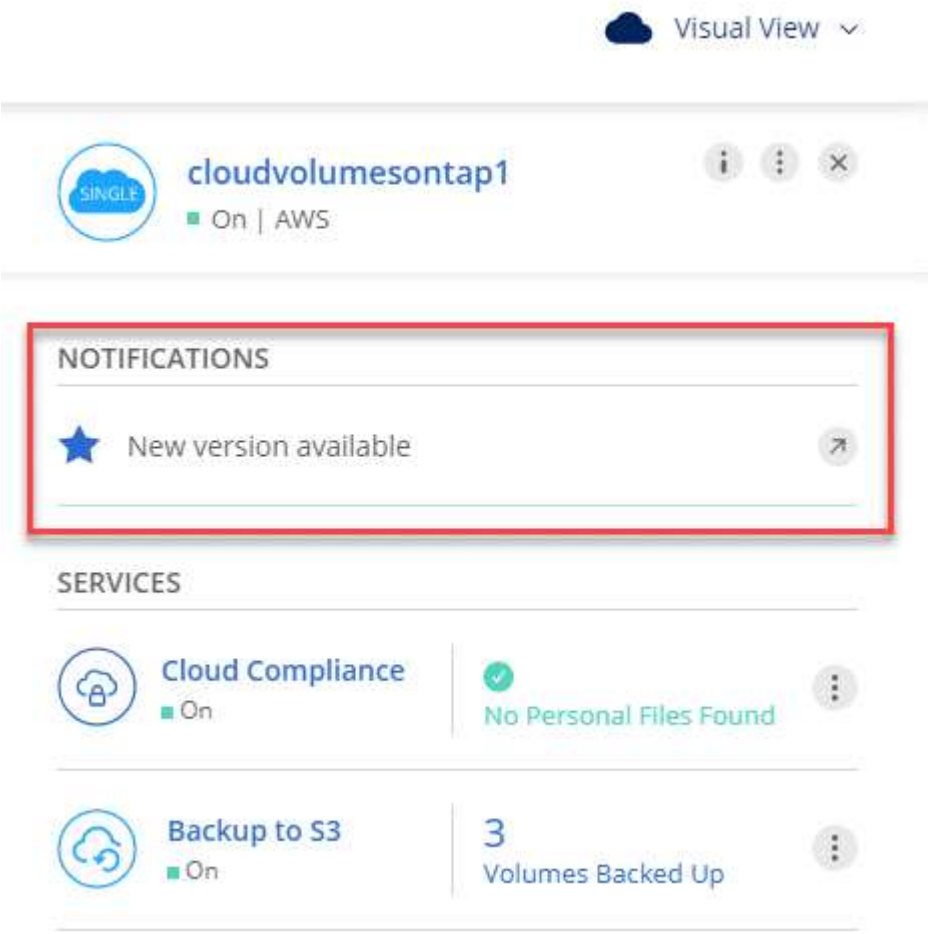
Cloud Manager には、現在の Cloud Volumes ONTAP リリースへのアップグレード、または Cloud Volumes ONTAP を以前のリリースにダウングレードするために使用できるいくつかのオプションがあります。ソフトウェアをアップグレードまたはダウングレードする前に、 Cloud Volumes ONTAP システムを準備する必要があります。

ソフトウェアの更新を **Cloud Manager** で完了しておく必要があります

Cloud Volumes ONTAP のアップグレードが Cloud Manager から完了している必要があります。System Manager または CLI を使用して Cloud Volumes ONTAP をアップグレードしないでください。これを行うと、システムの安定性に影響を与える可能性

Cloud Volumes ONTAP の更新方法

Cloud Manager は、 Cloud Volumes ONTAP の新しいバージョンが利用可能になると、 Cloud Volumes ONTAP の作業環境に次の通知を表示します。



ページに表示される新しいバージョンの通知を示します。"]

この通知からアップグレードプロセスを開始できます。アップグレードプロセスを自動化するには、 S3 バケットからソフトウェアイメージを取得し、イメージをインストールしてから、システムを再起動します。詳細については、を参照してください Cloud Manager 通知からの Cloud Volumes ONTAP のアップグレード。

> AWS の HA システムの場合、 Cloud Manager のアップグレードプロセスの一環として HA メディエーターがアップグレードされることがあります。

ソフトウェアアップデートの詳細オプション

Cloud Manager には、 Cloud Volumes ONTAP ソフトウェアを更新するための次の高度なオプションも用意されています。

- 外部 URL のイメージを使用してソフトウェアを更新します

  このオプションは、 Cloud Manager が S3 バケットにアクセスしてソフトウェアをアップグレードできない場合、パッチが提供されている場合、またはソフトウェアを特定のバージョンにダウングレードする場

合に役立ちます。

詳細については、を参照してください HTTP または FTP サーバを使用した Cloud Volumes ONTAP のアップグレードまたはダウングレード。

- システムの代替イメージを使用してソフトウェアを更新します

  このオプションを使用すると、代替ソフトウェアイメージをデフォルトイメージにすることで、以前のバージョンにダウングレードできます。このオプションは HA ペアでは使用できません。

  詳細については、を参照してください ローカルイメージを使用した Cloud Volumes ONTAP のダウングレード。

Cloud Volumes ONTAP ソフトウェアの更新の準備

アップグレードまたはダウングレードを実行する前に、システムの準備ができていることを確認し、必要な設定変更を行う必要があります。

- [ダウンタイムの計画]
- [バージョン要件の確認]
- [自動ギブバックが有効になっていることの確認]
- SnapMirror 転送の一時停止
- [アグリゲートがオンラインであることの確認]

ダウンタイムの計画

シングルノードシステムをアップグレードする場合は、アップグレードプロセスによって、 I/O が中断される最長 25 分間システムがオフラインになります。

HA ペアのアップグレードは無停止で、 I/O が中断されません。無停止アップグレードでは、各ノードが連携してアップグレードされ、クライアントへの I/O の提供が継続されます。

バージョン要件の確認

アップグレードまたはダウングレード可能な ONTAP のバージョンは、システムで現在実行している ONTAP のバージョンによって異なります。

バージョン要件については、を参照してください "ONTAP 9 ドキュメント：「 Cluster update requirements"。

自動ギブバックが有効になっていることの確認

Cloud Volumes ONTAP HA ペア（デフォルト設定）で自動ギブバックを有効にする必要があります。サポートされていない場合、処理は失敗します。

"ONTAP 9 ドキュメント：「 Commands for configuring automatic giveback"

SnapMirror 転送の一時停止

Cloud Volumes ONTAP システムにアクティブな SnapMirror 関係がある場合は、 Cloud Volumes ONTAP ソフトウェアを更新する前に転送を一時停止することを推奨します。転送を一時停止すると、 SnapMirror の障害を防ぐことができます。デスティネーションシステムからの転送を一時停止する必要があります。

このタスクについて

ここでは、 System Manager for Version 9.3 以降の使用方法について説明します。

手順

1. "System Manager にログインします。" デスティネーションシステムから作成します。
2. ［ * 保護 ］ > ［ 関係 * ］ の順にクリックします。
3. 関係を選択し、 * Operations > Quiesce * をクリックします。

アグリゲートがオンラインであることの確認

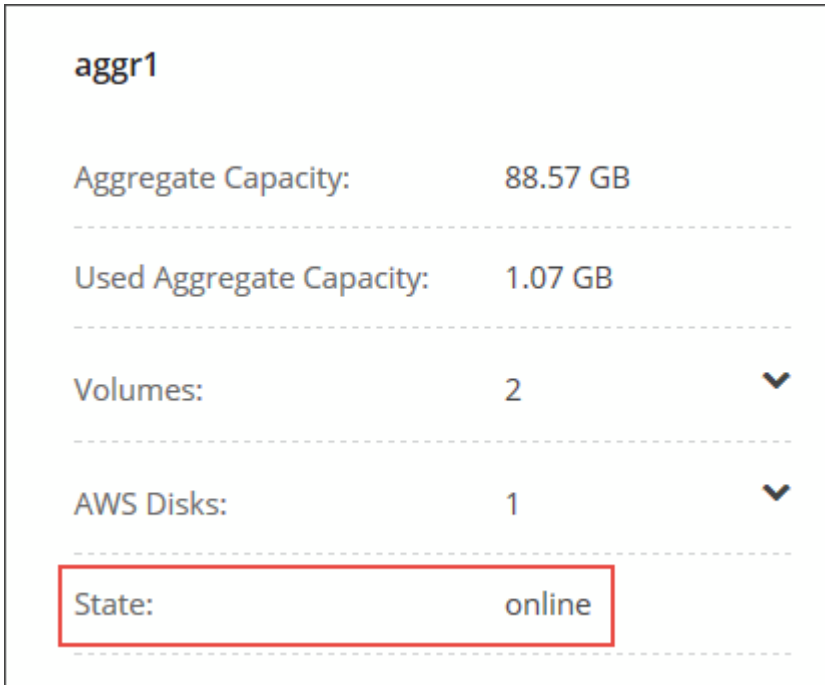
ソフトウェアを更新する前に、 Cloud Volumes ONTAP のアグリゲートがオンラインである必要があります。アグリゲートはほとんどの構成でオンラインになっている必要がありますが、オンラインになっていない場合はオンラインにしてください。

このタスクについて

ここでは、 System Manager for Version 9.3 以降の使用方法について説明します。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > 高度な割り当て * をクリックします。
2. アグリゲートを選択し、 * Info * をクリックして、状態がオンラインであることを確認します。



3. アグリゲートがオフラインの場合は、 System Manager を使用してアグリゲートをオンラインにします。
   a. "System Manager にログインします。"。

b. ストレージ > アグリゲートとディスク > アグリゲート * をクリックします。

c. アグリゲートを選択し、 * その他の操作 > ステータス > オンライン * をクリックします。

Cloud Manager 通知からの Cloud Volumes ONTAP のアップグレード

新しいバージョンの Cloud Volumes ONTAP が利用可能になると、 Cloud Manager から通知が表示されます。通知をクリックしてアップグレードプロセスを開始します。

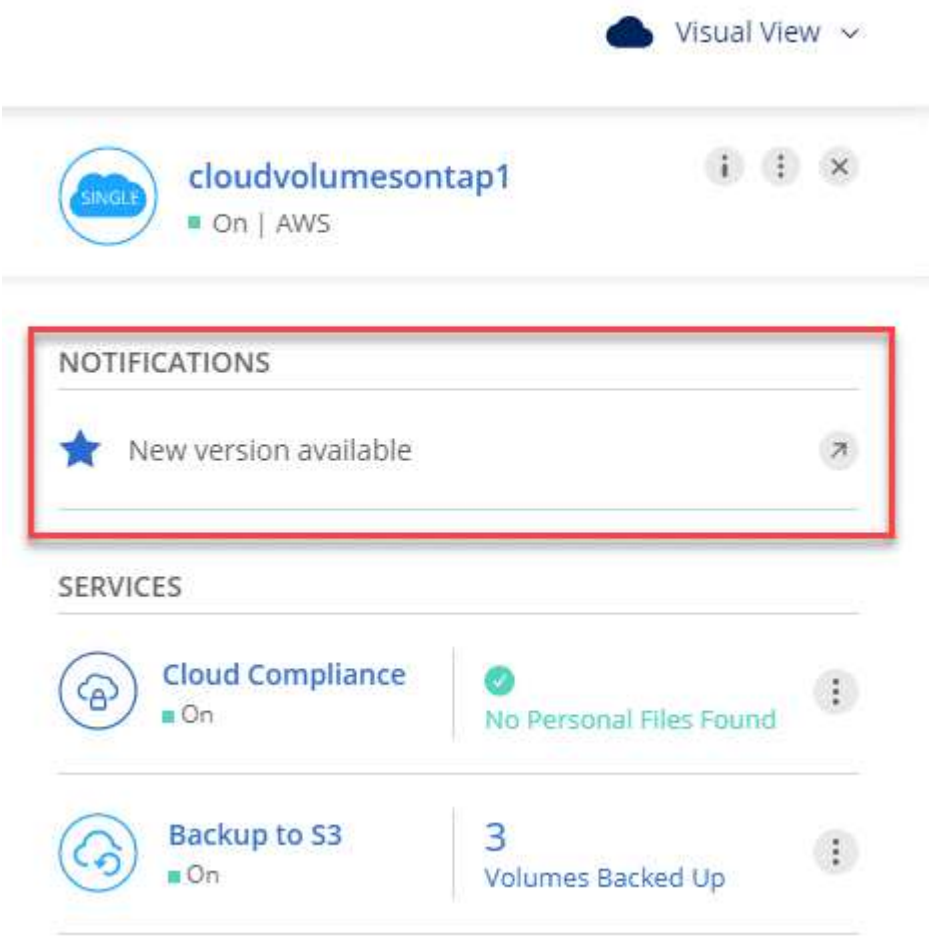
作業を開始する前に

Cloud Volumes ONTAP システムでは、ボリュームやアグリゲートの作成などの Cloud Manager 操作を実行してはいけません。

手順

1. [作業環境（ Working Environments ）] をクリックします。
2. 作業環境を選択します。

   新しいバージョンが使用可能になると、右側のペインに通知が表示されます。



ページに表示される新しいバージョンの通知を示します。"]

3. 新しいバージョンが利用可能な場合は、 * アップグレード * をクリックします。

4. [リリース情報] ページで、リンクをクリックして、指定したバージョンのリリースノートを読み、 [* 読み … *] チェックボックスをオンにします。
5. エンドユーザライセンス契約（ EULA ）ページで EULA を読んでから、「 * I read and approve the EULA * 」を選択します。
6. [レビューと承認] ページで、重要なメモを読み、 [* I understand … *] を選択して、 [* Go *] をクリックします。

結果

Cloud Manager がソフトウェアのアップグレードを開始します。ソフトウェアの更新が完了したら、作業環境に対してアクションを実行できます。

完了後

SnapMirror 転送を一時停止した場合は、 System Manager を使用して転送を再開します。

HTTP または FTP サーバを使用した Cloud Volumes ONTAP のアップグレードまたはダウングレード

Cloud Volumes ONTAP ソフトウェアイメージを HTTP サーバまたは FTP サーバに配置し、 Cloud Manager からソフトウェアの更新を開始できます。このオプションは、 Cloud Manager が S3 バケットにアクセスしてソフトウェアをアップグレードできない場合、またはソフトウェアをダウングレードする場合に使用できます。

手順

1. Cloud Volumes ONTAP ソフトウェアイメージをホストできる HTTP サーバまたは FTP サーバを設定します。
2. 仮想ネットワークへの VPN 接続がある場合は、 Cloud Volumes ONTAP ソフトウェアイメージを自社のネットワーク内の HTTP サーバまたは FTP サーバに配置できます。それ以外の場合は、クラウド内の HTTP サーバまたは FTP サーバにファイルを配置する必要があります。
3. Cloud Volumes ONTAP 用に独自のセキュリティグループを使用する場合は、送信ルールで HTTP または FTP 接続が許可されていることを確認し、 Cloud Volumes ONTAP がソフトウェアイメージにアクセスできるようにします。

   事前定義された Cloud Volumes ONTAP セキュリティグループでは、デフォルトで発信 HTTP 接続と FTP 接続が許可されます。

4. からソフトウェアイメージを取得します "ネットアップサポートサイト"。
5. ソフトウェアイメージを、ファイルの提供元の HTTP サーバまたは FTP サーバ上のディレクトリにコピーします。
6. Cloud Manager の作業環境で、メニューアイコンをクリックし、 * Advanced > Update Cloud Volumes ONTAP * をクリックします。
7. アップデートソフトウェアページで、「 URL から利用可能なイメージを選択」を選択し、 URL を入力して「 * イメージの変更 * 」をクリックします。
8. [* Proceed](続行) をクリックして確定します

結果

Cloud Manager がソフトウェアの更新を開始します。ソフトウェアの更新が完了したら、作業環境に対してアクションを実行できます。

完了後

SnapMirror 転送を一時停止した場合は、 System Manager を使用して転送を再開します。

ローカルイメージを使用した **Cloud Volumes ONTAP** のダウングレード

同一リリースファミリの以前のリリース（ 9.5 から 9.4 など）への Cloud Volumes ONTAP の移行は、ダウングレードと呼ばれます。新規クラスタまたはテストクラスタをダウングレードする場合は、サポートなしでダウングレードできますが、本番クラスタをダウングレードする場合は、テクニカルサポートにお問い合わせください。

各 Cloud Volumes ONTAP システムには、実行中の現在のイメージとブート可能な代替イメージの 2 つのソフトウェアイメージを格納できます。Cloud Manager では、代替イメージをデフォルトイメージに変更できます。現在のイメージに問題が発生している場合は、このオプションを使用して以前のバージョンの Cloud Volumes ONTAP にダウングレードできます。

このタスクについて

このダウングレードプロセスは、シングルクラウドボリューム ONTAP システムでのみ使用できます。HA ペアでは使用できません。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > Cloud Volumes ONTAP の更新 * をクリックします。
2. ソフトウェアの更新ページで、代替イメージを選択し、 * イメージの変更 * をクリックします。
3. [* Proceed](続行) をクリックして確定します

結果

Cloud Manager がソフトウェアの更新を開始します。ソフトウェアの更新が完了したら、作業環境に対してアクションを実行できます。

完了後

SnapMirror 転送を一時停止した場合は、 System Manager を使用して転送を再開します。

Cloud Volumes ONTAP システムの変更

ストレージのニーズの変化に応じて、 Cloud Volumes ONTAP インスタンスの構成を変更する必要がある場合があります。たとえば、従量課金制の設定を変更したり、インスタンスや VM のタイプを変更したり、別のサブスクリプションに移動したりできます。

Cloud Volumes ONTAP BYOL システムへのライセンスファイルのインストール

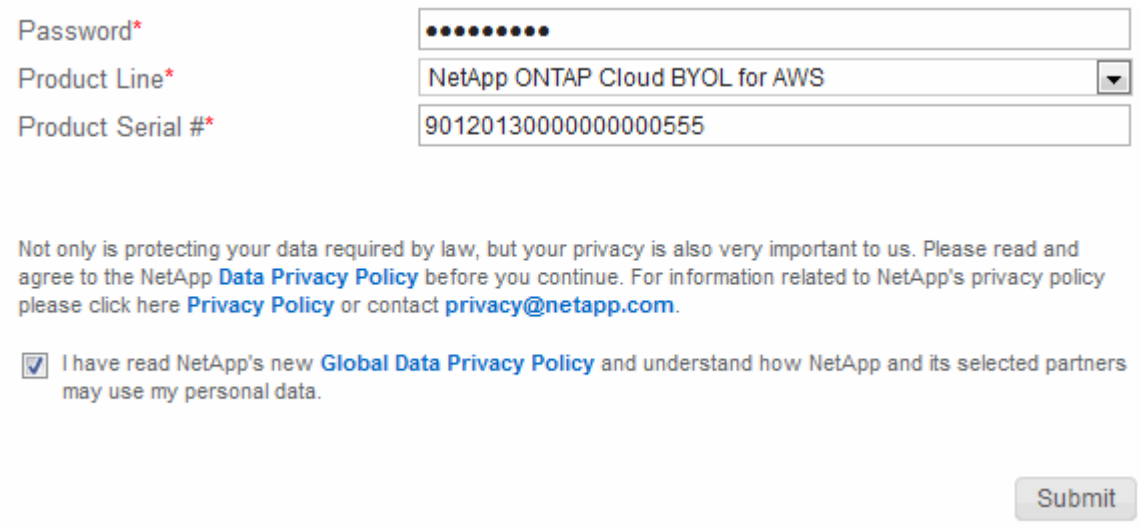
Cloud Manager がネットアップから BYOL ライセンスファイルを取得できない場合は、ご自身でファイルを取得し、 Cloud Manager に手動でアップロードして、 Cloud Volumes ONTAP システムにライセンスをインストールできるようにします。

手順

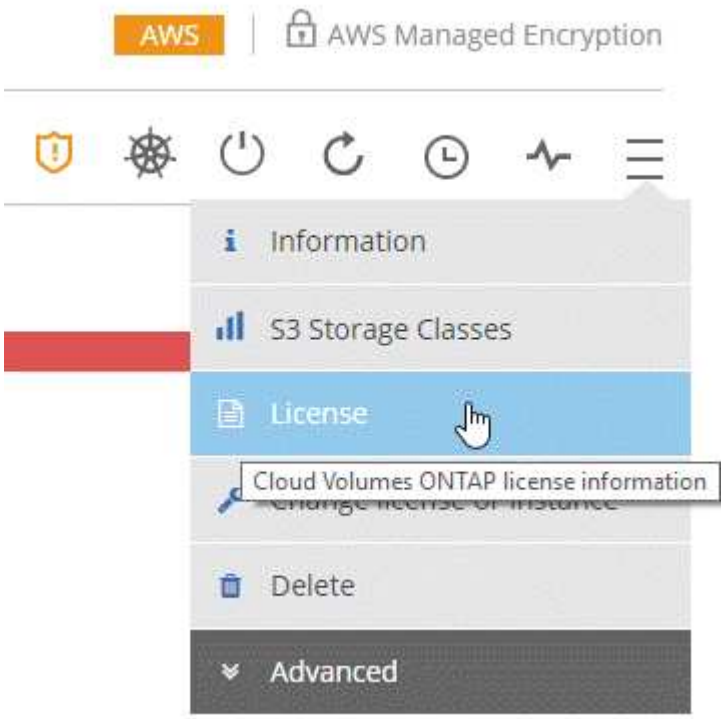
1. にアクセスします "ネットアップライセンスファイルジェネレータ" をクリックし、ネットアップサポートサイトのクレデンシャルでログインします。

2. パスワードを入力し、製品を選択してシリアル番号を入力し、プライバシーポリシーを読み、同意したことを確認してから、 * Submit * をクリックします。

    - 例 *



3. 電子メールまたは直接ダウンロードで serialnumber.nlf JSON ファイルを受信するかどうかを選択します。
4. Cloud Manager で、 Cloud Volumes ONTAP BYOL 作業環境を開きます。
5. メニューアイコンをクリックし、 * ライセンス * をクリックします。



6. [ライセンスファイルのアップロード *] をクリックします。
7. [* Upload] をクリックし、ファイルを選択します。

結果

Cloud Manager は、 Cloud Volumes ONTAP システムに新しいライセンスファイルをインストールします。

Cloud Volumes ONTAP のインスタンスまたはマシンタイプを変更する

AWS 、 Azure 、 GCP で Cloud Volumes ONTAP を起動する際には、いくつかのインスタンスまたはマシンのタイプから選択できます。必要に応じてサイズが小さすぎる、または大きすぎると判断した場合は、いつでもインスタンスまたはマシンタイプを変更できます。

このタスクについて

- Cloud Volumes ONTAP HA ペア（デフォルト設定）で自動ギブバックを有効にする必要があります。サポートされていない場合、処理は失敗します。

  "ONTAP 9 ドキュメント：「 Commands for configuring automatic giveback"

- Cloud Volumes ONTAP が再起動されます。

  シングルノードシステムの場合、 I/O は中断されます。

  HA ペアの場合、変更は中断されません。HA ペアは引き続きデータを提供します。

- インスタンスまたはマシンタイプを変更すると、クラウドプロバイダのサービス料金に影響します。

手順

1. 作業環境で、メニューアイコンをクリックし、 * ライセンスまたはインスタンスの変更 * for AWS 、 * ライセンスまたは VM * for Azure 、 * ライセンスまたはマシンの変更 * for GCP をクリックします。
2. 従量課金制の構成を使用している場合は、オプションで別のライセンスを選択できます。
3. インスタンスまたはマシンタイプを選択し、チェックボックスを選択して、変更の影響を理解したことを確認し、 * OK * をクリックします。

結果

Cloud Volumes ONTAP が新しい設定でリブートします。

従量課金制の構成を切り替える

従量課金制の Cloud Volumes ONTAP システムを起動した後は、ライセンスを変更することで、いつでも Explore 、 Standard 、 Premium の構成を変更できます。ライセンスを変更すると、未フォーマット時の容量制限が増減し、別の AWS インスタンスタイプまたは Azure 仮想マシンタイプから選択できます。

> GCP では、従量課金制構成ごとに 1 つのマシンタイプを使用できます。異なるマシンタイプの中から選択することはできません。

このタスクについて

従量課金制ライセンスの切り替えについては、次の点に注意してください。

- Cloud Volumes ONTAP が再起動されます。

  シングルノードシステムの場合、 I/O は中断されます。

HA ペアの場合、変更は中断されません。HA ペアは引き続きデータを提供します。

- インスタンスまたはマシンタイプを変更すると、クラウドプロバイダのサービス料金に影響します。

手順

1. 作業環境で、メニューアイコンをクリックし、 * ライセンスまたはインスタンスの変更 * for AWS 、 * ライセンスまたは VM * for Azure 、 * ライセンスまたはマシンの変更 * for GCP をクリックします。
2. ライセンスタイプとインスタンスタイプまたはマシンタイプを選択し、チェックボックスを選択して、変更の影響を理解していることを確認し、 * OK * をクリックします。

結果

Cloud Volumes ONTAP が新しいライセンス、インスタンスタイプまたはマシンタイプ、またはその両方でリブートします。

代替クラウドボリューム **ONTAP** 構成への移行

従量課金制サブスクリプションと BYOL サブスクリプションの間、または単一の Cloud Volumes ONTAP システムと HA ペアの間で移行する場合は、新しいシステムを導入してから、既存のシステムから新しいシステムにデータを複製できます。

手順

1. 新しい Cloud Volumes ONTAP の作業環境を作成します。

   "AWS での Cloud Volumes ONTAP の起動"
   "Azure で Cloud Volumes ONTAP を起動します"
   "GCP での Cloud Volumes ONTAP の起動"

2. "1 回限りのデータレプリケーションを設定します" レプリケートする必要がある各ボリュームのシステム間。
3. 終了した Cloud Volumes ONTAP システムを終了します ニーズ "元の作業環境を削除します"。

AWS Marketplace へのサブスクリプションの変更

料金を請求する AWS アカウントを変更する場合は、 Cloud Volumes ONTAP システムの AWS Marketplace サブスクリプションを変更します。

手順

1. まだサブスクリプションを作成していない場合は、から新しいサブスクリプションを追加します "AWS Marketplace で提供される Cloud Manager"。
2. Cloud Manager の作業環境で、メニューアイコンをクリックし、 * Marketplace Subscription * をクリックします。
3. ドロップダウンリストからサブスクリプションを選択します。
4. [保存（ Save ）] をクリックします。

書き込み速度を通常または高速に変更しています

Cloud Volumes ONTAP のデフォルトの書き込み速度は normal です。ワークロードで高速書き込みパフォーマンスが必要な場合は、高速書き込み速度に変更できます。書き込み速度を変更する前に、次のことを確認し

てください "通常の設定と高い設定の違いを理解する"。

このタスクについて

- ボリュームやアグリゲートの作成などの処理が実行中でないことを確認してください。
- この変更によって Cloud Volumes ONTAP が再起動することに注意してください。

  シングルノードシステムの場合、 I/O は中断されます。

  HA ペアの場合、変更は中断されません。HA ペアは引き続きデータを提供します。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > 書き込み速度 * をクリックします。
2. 「 * Normal * 」または「 * High * 」を選択します。

   「高」を選択した場合は、「 I understand … 」文を読んで、チェックボックスをオンにして確認する必要があります。

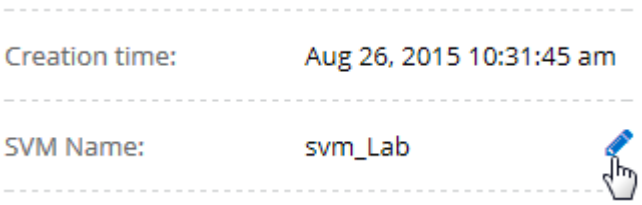
3. [保存] をクリックし、確認メッセージを確認して、 [続行] をクリックします。

ストレージ仮想マシン名の変更

Cloud Manager は、 Cloud Volumes ONTAP 用の Storage Virtual Machine （ SVM ）に自動的に名前を付けます。厳密な命名規則がある場合は、 SVM の名前を変更できます。たとえば、 ONTAP クラスタの SVM の名前を一致させることができます。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 情報 * をクリックします。
2. SVM 名の右側にある Edit アイコンをクリックします。



3. SVM 名の変更ダイアログボックスで、 SVM 名を変更し、 * 保存 * をクリックします。

Cloud Volumes ONTAP のパスワードの変更

Cloud Volumes ONTAP にはクラスタ管理者アカウントが含まれています。必要に応じて、 Cloud Manager からこのアカウントのパスワードを変更できます。

> System Manager または CLI を使用して admin アカウントのパスワードを変更しないでください。パスワードは Cloud Manager に反映されません。その結果、 Cloud Manager はインスタンスを適切に監視できません。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > パスワードの設定 * をクリックします。
2. 新しいパスワードを 2 回入力し、 [保存] をクリックします。

   新しいパスワードは、最後に使用した 6 つのパスワードのうちの 1 つと異なるものにする必要があります。

C4.4XLarge および C4.8XLarge インスタンスのネットワーク MTU の変更

デフォルトでは、 Cloud Volumes ONTAP は、 CS4.4XLarge インスタンスまたは AWS の C4.8XLarge インスタンスを選択した場合に、 9,000 MTU （ジャンボフレームとも呼ばれます）を使用するように設定されています。ネットワーク設定に適している場合は、ネットワーク MTU を 1,500 バイトに変更できます。

このタスクについて

9,000 バイトのネットワーク最大伝送ユニット（ MTU ）は、特定の構成で可能な最大ネットワークスループットを提供できます。

同じ vPC 内のクライアントが Cloud Volumes ONTAP システムと通信し、それらのクライアントの一部またはすべてが 9,000 MTU をサポートしている場合は、 9,000 MTU を選択することを推奨します。トラフィックが vPC から発信されると、パケットの断片化が発生し、パフォーマンスが低下する可能性があります。

VPC 外のクライアントまたはシステムが Cloud Volumes ONTAP システムと通信する場合は、ネットワーク MTU を 1,500 バイトにすることをお勧めします。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 詳細設定 > ネットワーク利用率 * をクリックします。
2. [* 標準 *] または [* ジャンボフレーム *] を選択します。
3. [変更（ Change ）] をクリックします。

複数の AWS の HA ペアに関連付けられているルーティングテーブルの変更 AZS

HA ペアのフローティング IP アドレスへのルートを含む AWS ルーティングテーブルを変更できます。この処理は、新しい NFS または CIFS クライアントが AWS の HA ペアにアクセスする必要がある場合に実行できます。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 情報 * をクリックします。
2. * ルートテーブル * をクリックします。
3. 選択したルーティングテーブルのリストを変更し、 * 保存 * をクリックします。

結果

Cloud Manager は AWS 要求を送信してルートテーブルを変更します。

Cloud Volumes ONTAP の状態の管理

Cloud Manager から Cloud Volumes ONTAP を停止して起動し、クラウドコンピューティングコストを管理できます。

Cloud Volumes ONTAP の自動シャットダウンのスケジュール設定

特定の時間間隔で Cloud Volumes ONTAP をシャットダウンして、コンピューティングコストを削減できます。これを手動で行う代わりに、 Cloud Manager を設定して、システムを自動的にシャットダウンし、特定の時間に再起動することができます。

このタスクについて

Cloud Volumes ONTAP システムの自動シャットダウンをスケジュールする際、アクティブなデータ転送が実行中の場合のシャットダウンは延期されます。転送が完了すると、 Cloud Manager によってシステムがシャットダウンされます。

このタスクでは、 HA ペアの両方のノードの自動シャットダウンをスケジューリングします。

手順

1. 作業環境で、時計アイコンをクリックします。

2. シャットダウンスケジュールを指定します。

   a. システムを毎日、平日、週末、またはこれら 3 つのオプションの組み合わせでシャットダウンするかどうかを選択します。

   b. システムをオフにするタイミングと、オフにする期間を指定します。

      - 例 *

      次の図は、毎週土曜日の午前 0 時にシステムをシャットダウンするように Cloud Manager に指示するスケジュールを示しています48 時間。Cloud Manager は、毎週月曜日の午前 0 時にシステムを再起動します

3. [保存（ Save ）] をクリックします。

結果

Cloud Manager はスケジュールを保存します。時計アイコンが変化して、スケジュールが設定されたことを示します。 

Cloud Volumes ONTAP を停止しています

Cloud Volumes ONTAP を停止すると、計算コストの発生を抑えることができ、ルートディスクとブートディ

スクの Snapshot が作成されます。これはトラブルシューティングに役立ちます。

このタスクについて

HA ペアを停止すると、 Cloud Manager は両方のノードをシャットダウンします。

手順

1. 作業環境で、 * 電源オフ * アイコンをクリックします。

2. Snapshot を作成するオプションを有効にしておくと、システムのリカバリが可能になります。
3. [オフにする *] をクリックします。

   システムの停止には、最大数分かかる場合があります。システムは、後で [作業環境] ページから再起動できます。

AWS のリソースコストを監視する

Cloud Manager では、 AWS での Cloud Volumes ONTAP の実行に関連するリソースコストを確認できます。また、ネットアップの機能を使用してストレージコストを削減し、どれだけのコストを節約したかを確認することもできます。

このタスクについて

ページを更新すると、 Cloud Manager によってコストが更新されます。最終的なコストの詳細については、AWS を参照してください。

ステップ

1. Cloud Manager から AWS からコスト情報を取得できることを確認します。
   a. Cloud Manager に権限を提供する IAM ポリシーに次の操作が含まれていることを確認します。

   ```
   "ce:GetReservationUtilization",
   "ce:GetDimensionValues",
   "ce:GetCostAndUsage",
   "ce:GetTags"
   ```

   これらのアクションは最新のに含まれています "Cloud Manager ポリシー"。これらの権限は、NetApp Cloud Central から自動的に導入された新しいシステムに含まれます。

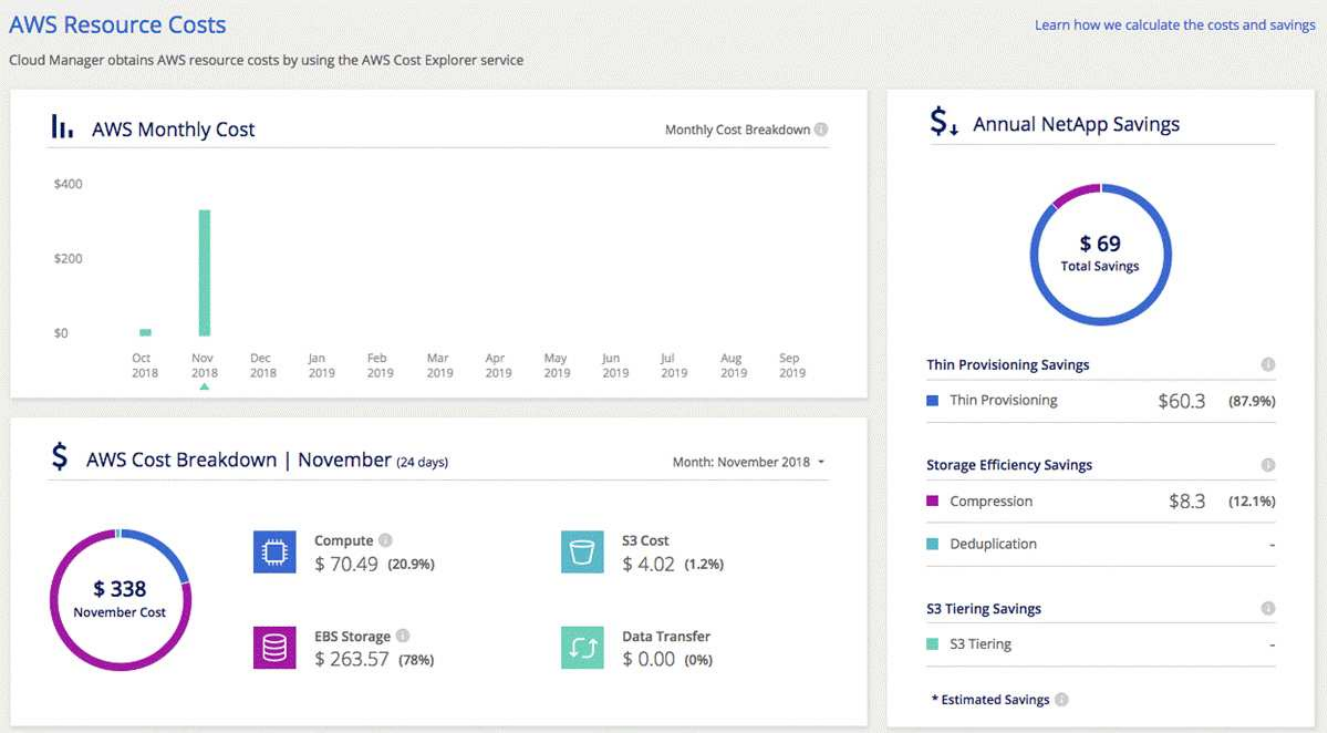
   b. "* WorkingEnvironmentId* タグをアクティブにします"。

   AWS のコストを追跡するために、 Cloud Manager はコスト割り当てタグを Cloud Volumes ONTAP インスタンスに割り当てます。最初の作業環境を作成したら、 * WorkingEnvironmentId * タグをアクティブ化します。ユーザ定義のタグは、請求とコスト管理のコンソールでアクティブ化するまでは AWS 請求レポートに表示されません。

2. 作業環境ページで Cloud Volumes ONTAP 作業環境を選択し、コスト * をクリックします。

   ボリュームでコスト削減機能を有効にしている場合、過去数カ月のコストと、ネットアップによる年間削減量が表示されます。

   次の図は、コストページの例を示しています。

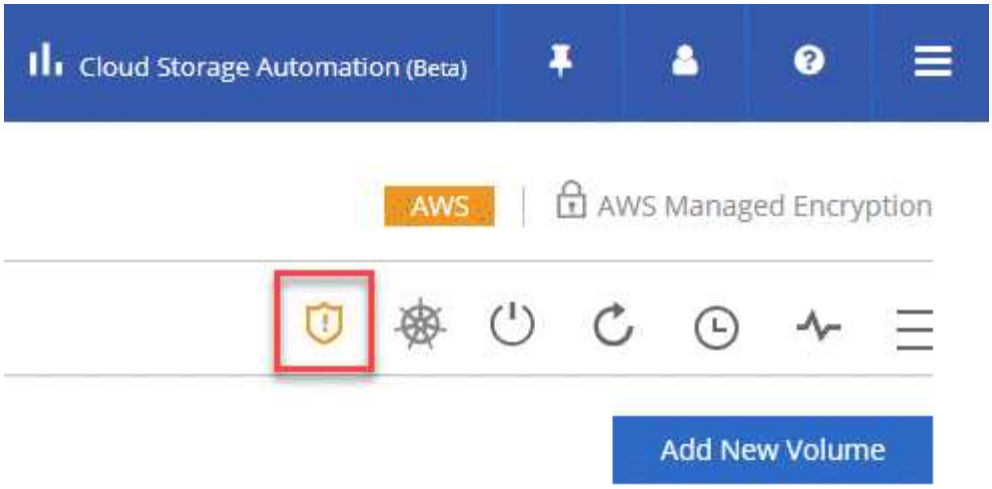


ランサムウェアからの保護を強化

ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。Cloud Manager では、ランサムウェアに対応したネットアップソリューションを実装できます。これにより、可視化、検出、修復のための効果的なツールが提供されます。

手順

1. 作業環境で、「 * ランサムウェア * 」アイコンをクリックします。

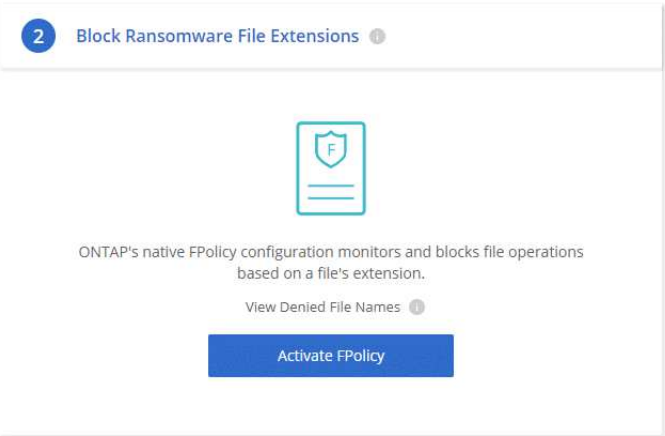


2. ネットアップのランサムウェア向けソリューションを導入する：
   a. Snapshot ポリシーが有効になっていないボリュームがある場合は、 * Snapshot ポリシーのアクティブ化 * をクリックします。

      NetApp Snapshot テクノロジは、ランサムウェアの修復に業界最高のソリューションを提供します。リカバリを成功させるには、感染していないバックアップからリストアすることが重要です。Snapshot コピーは読み取り専用であり、ランサムウェアによる破損を防止します。単一のファイルコピーまたは完全なディザスタリカバリソリューションのイメージを作成する際の単位を提供することもできます。

   b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

      この予防ソリューションは、ランサムウェア攻撃からの保護を強化する一般的なランサムウェアファイルタイプをブロックします。



Cloud Manager に既存の Cloud Volumes ONTAP システムを追加

既存の Cloud Volumes ONTAP システムを検出して Cloud Manager に追加できます。こ

の処理は、新しい Cloud Manager システムを導入した場合に実行できます。

作業を開始する前に

Cloud Volumes ONTAP 管理者ユーザアカウントのパスワードを知っている必要があります。

手順

1. 作業環境ページで、 * 検出 * をクリックし、 * Cloud Volumes ONTAP * を選択します。
2. システムが配置されているクラウドプロバイダを選択します。
3. [Region] ページで、インスタンスが実行されているリージョンを選択し、インスタンスを選択します。
4. [資格情報] ページで、 Cloud Volumes ONTAP 管理者ユーザーのパスワードを入力し、 [* 移動] をクリックします。

結果

Cloud Manager によって Cloud Volumes ONTAP インスタンスがワークスペースに追加されます。

Cloud Volumes ONTAP 作業環境を削除する

Cloud Volumes ONTAP システムは、クラウドプロバイダのコンソールからではなく、Cloud Manager から削除することを推奨します。たとえば、 AWS からライセンスが有効な Cloud Volumes ONTAP インスタンスを終了すると、別のインスタンスでこのライセンスキーを使用できなくなります。ライセンスをリリースするには、作業環境を Cloud Manager から削除する必要があります。

このタスクについて

作業環境を削除すると、 Cloud Manager はインスタンスを終了し、ディスクとスナップショットを削除します。

> Cloud Volumes ONTAP インスタンスでは、 AWS からの偶発的な終了を防止するために、終端保護が有効になっています。ただし、 AWS から Cloud Volumes ONTAP インスタンスを終了する場合は、 AWS CloudFormation コンソールに移動して、インスタンスのスタックを削除する必要があります。スタック名は、作業環境の名前です。

手順

1. 作業環境で、メニューアイコンをクリックし、 * 削除 * をクリックします。
2. 作業環境の名前を入力し、 * 削除 * をクリックします。

   作業環境を削除するには、最大 5 分かかります。

Cloud Manager の管理

Cloud Manager を更新しています

Cloud Manager は、最新バージョンにアップデートすることも、ネットアップの担当者が共有しているパッチを使用してアップデートすることもできます。

自動更新を有効にする

新しいバージョンが利用可能になると、 Cloud Manager は自動的に更新されます。これにより、最新バージョンが実行されていることを確認できます。

このタスクについて

Cloud Manager は、実行中の処理がない場合、自動的に深夜 12 時に更新されます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * Cloud Manager 設定 * を選択します。
2. Automatic Cloud Manager Updates の下のチェックボックスを選択し、 * Save * をクリックします。

Cloud Manager を最新バージョンに更新しています

Cloud Manager への自動更新を有効にする必要がありますが、 Web コンソールから直接手動で更新することもできます。Cloud Manager は、 AWS の NetApp 所有 S3 バケットからソフトウェアアップデートを取得します。

作業を開始する前に

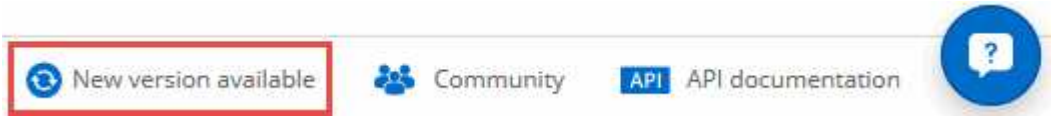
を確認しておきます "このリリースの新機能" をクリックして、サポートに関する新しい要件と変更点を特定します。

このタスクについて

ソフトウェアの更新には数分かかります。Cloud Manager は更新中に使用できません。

手順

1. コンソールの右下隅を見て、新しいバージョンが使用可能かどうかを確認します。



2. 新しいバージョンが利用可能な場合は、 [タイムライン *] をクリックして、進行中のタスクがあるかどうかを確認します。

   処理中のタスクがある場合は、完了するまで待ってから次の手順に進みます。

3. コンソールの右下にある [新しいバージョンを使用可能にする *] をクリックします。
4. Cloud Manager の Software Update ページで、目的のバージョンの横にある * Update * をクリックしま

す。

5. 確認ダイアログボックスに入力し、 * OK * をクリックします。

結果

Cloud Manager が更新プロセスを開始します。数分後にコンソールにログインできます。

パッチを使用した **Cloud Manager** の更新

ネットアップがパッチを共有している場合は、 Cloud Manager Web コンソールから直接、提供されたパッチを使用して Cloud Manager を更新できます。

このタスクについて

通常、パッチの更新には数分かかります。Cloud Manager は更新中に使用できません。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * ソフトウェア更新 * を選択します。

2. リンクをクリックして、提供されたパッチで Cloud Manager を更新します。

3. 確認ダイアログボックスに入力し、 * OK * をクリックします。
4. 提供されたパッチを選択します。

結果

Cloud Manager はパッチを適用します。数分後にコンソールにログインできます。

Cloud Central アカウントでのワークスペースとユーザの管理

"初期セットアップを実行したあと"を使用すると、ユーザ、ワークスペース、およびサービスコネクタの管理が必要になる場合があります。

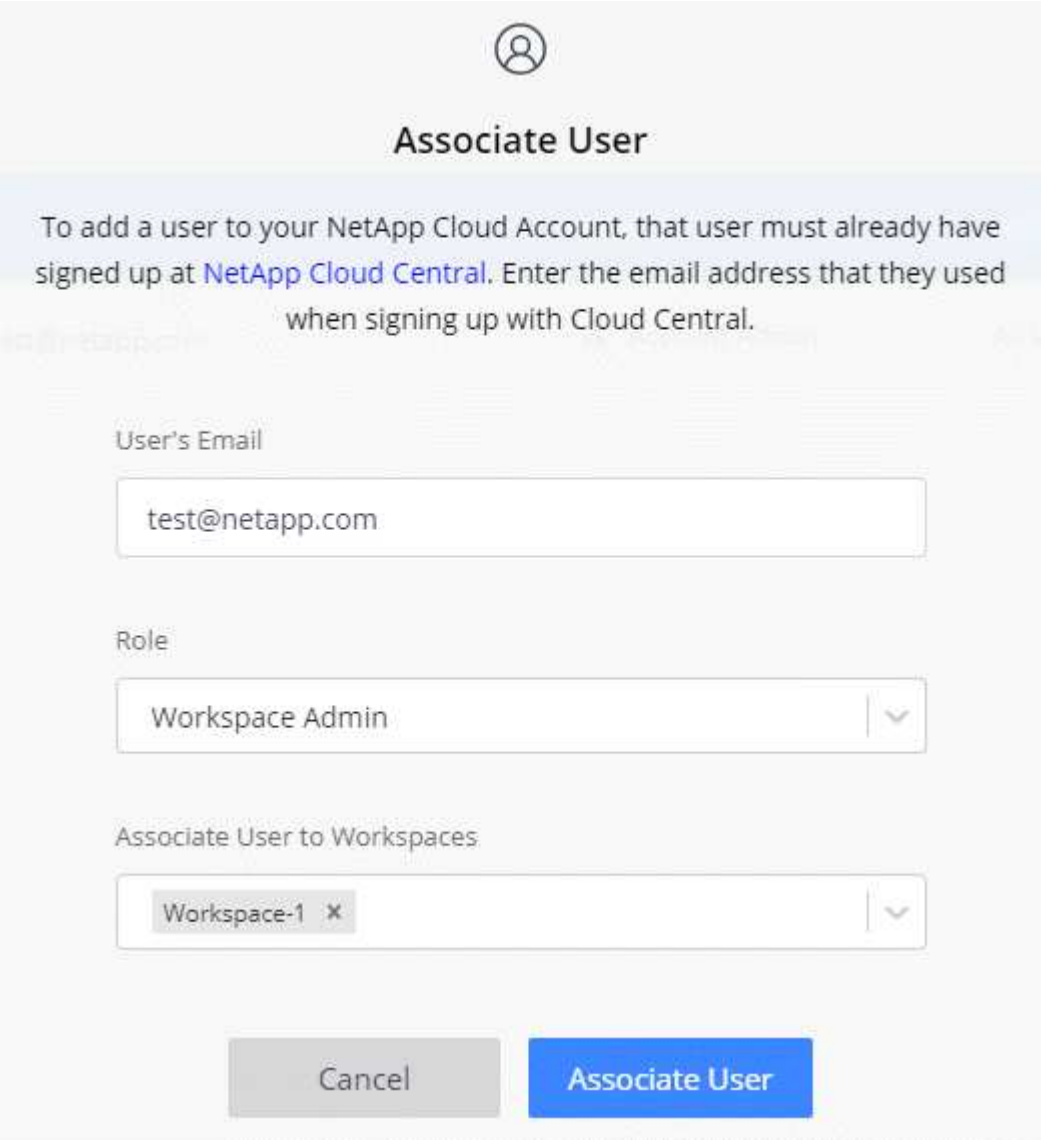
"Cloud Central アカウントの仕組みの詳細については、こちらをご覧ください"。

ユーザを追加する

Cloud Central ユーザを Cloud Central アカウントに関連付けて、これらのユーザが Cloud Manager で作業環境を作成および管理できるようにします。

手順

1. ユーザーがまだ行っていない場合は、にアクセスするようにユーザーに依頼します "NetApp Cloud Central" アカウントを作成します。
2. Cloud Manager で、 * アカウント設定 * をクリックします。
3. [ユーザー] タブで、 [ユーザーの関連付け] をクリックします。
4. ユーザの E メールアドレスを入力し、ユーザのロールを選択します。
   - * アカウント管理者 * ： Cloud Manager で任意の操作を実行できます。
   - * ワークスペース管理者 * ：割り当てられたワークスペースでリソースを作成および管理できます。
5. Workspace Admin を選択した場合は、 1 つ以上のワークスペースを選択してそのユーザーに関連付けます。



6. [ユーザーの関連付け] をクリックします。

結果

ユーザには、 NetApp Cloud Central の「 Account Association 」というタイトルの E メールが送信されます。 E メールには、 Cloud Manager にアクセスするために必要な情報が記載されています。

結果

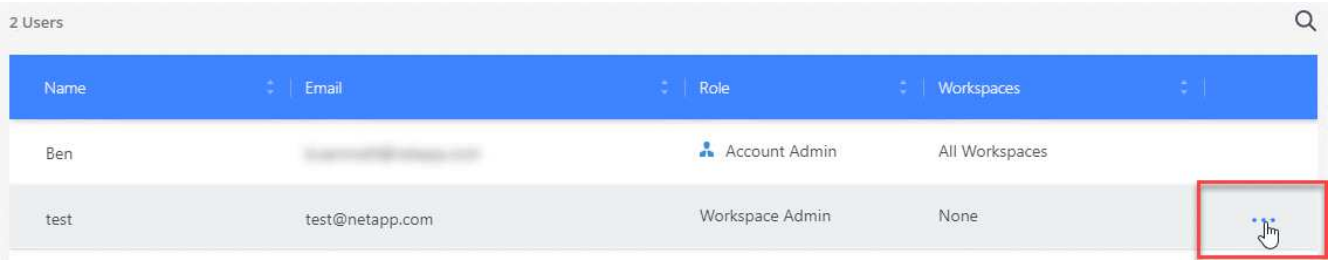
ユーザには、 NetApp Cloud Central の「 Account Association 」というタイトルの E メールが送信されます。 E メールには、 Cloud Manager にアクセスするために必要な情報が記載されています。

ユーザの削除

ユーザの関連付けを解除すると、 Cloud Central アカウント内のリソースにアクセスできなくなります。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. ユーザに対応する行のアクションメニューをクリックします。



3. [ユーザーの関連付けを解除（ Disassociate User ）] をクリックし、 [関連付けを解除（ Disassociate ）] をクリックして

結果

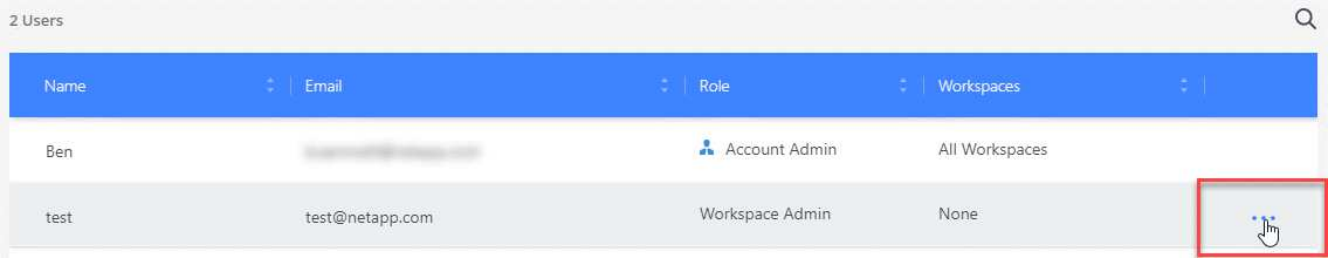
ユーザはこの Cloud Central アカウントのリソースにアクセスできなくなります。

ワークスペース管理者のワークスペースの管理

ワークスペース管理者は、いつでもワークスペースに関連付けたり、ワークスペースと関連付けを解除したりできます。ユーザーを関連付けると、ワークスペース内の作業環境を作成して表示できます。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. ユーザに対応する行のアクションメニューをクリックします。



3. * ワークスペースの管理 * をクリックします。
4. ユーザーに関連付けるワークスペースを選択し、 * 適用 * をクリックします。

結果

サービスコネクタもワークスペースに関連付けられていれば、ユーザは Cloud Manager からこれらのワーク

スペースにアクセスできるようになりました。

ワークスペースの管理

ワークスペースの作成、名前の変更、および削除により、ワークスペースを管理します。ワークスペースにリソースが含まれている場合、ワークスペースは削除できません。空である必要があります。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. [* ワークスペース *] をクリックします。
3. 次のいずれかのオプションを選択します。
    - 新しいワークスペースを作成するには、 * 新しいワークスペースを追加 * をクリックします。
    - * 名前変更 * をクリックして、ワークスペースの名前を変更します。
    - ワークスペースを削除するには、 * 削除 * をクリックします。

サービスコネクタのワークスペースを管理する

サービスコネクタをワークスペースに関連付けて、 Workspace 管理者がこれらのワークスペースに Cloud Manager からアクセスできるようにする必要があります。

アカウント管理者のみがいる場合は、サービスコネクタをワークスペースに関連付ける必要はありません。アカウント管理者は、デフォルトで Cloud Manager のすべてのワークスペースにアクセスできます。

"ユーザー、ワークスペース、サービスコネクタの詳細をご覧ください"。

手順

1. 「 * アカウント設定 * 」をクリックします。
2. サービスコネクター * をクリックします。
3. 関連付けるサービスコネクタの [ワークスペースの管理 *] をクリックします。
4. サービスコネクタに関連付けるワークスペースを選択し、 * 適用 * をクリックします。

Cloud Volumes ONTAP の動作環境を削除しています

アカウント管理者は、 Cloud Volumes ONTAP 作業環境を削除して別のシステムに移動したり、検出に関する問題のトラブルシューティングを行ったりできます。

このタスクについて

Cloud Volumes ONTAP の作業環境を削除すると、 Cloud Manager から削除されます。Cloud Volumes ONTAP システムは削除されません。作業環境は後で再検出できます。

Cloud Manager から作業環境を削除すると、次のことが可能になります。

- 作業環境を別のワークスペースで再検出します
- 別の Cloud Manager システムから再検出します

- 初期検出中に問題が発生した場合は、再検出します

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * Tools * を選択します。

2. [ツール] ページで、 [* 起動 *] をクリックします。
3. 削除する Cloud Volumes ONTAP の作業環境を選択します。
4. [レビューと承認] ページで、 [* 移動] をクリックします。

結果

Cloud Manager は、作業環境を削除します。ユーザーは、この作業環境をいつでも [作業環境] ページから再検出できます。

プロキシサーバを使用するように **Cloud Manager** を設定しています

Cloud Manager を初めて導入するときに、システムにインターネットアクセスがない場合は、プロキシサーバの入力を求めるプロンプトが表示されます。また、 Cloud Manager の設定からプロキシを手動で入力および変更することもできます。

このタスクについて

インターネットへのすべての HTTP 通信にプロキシサーバを使用するように社内ポリシーで指示されている場合は、そのプロキシサーバを使用するように Cloud Manager を設定する必要があります。プロキシサーバは、クラウドまたはネットワークに配置できます。

プロキシサーバを使用するように Cloud Manager を設定すると、 Cloud Manager 、 Cloud Volumes ONTAP 、および HA Mediator はすべてプロキシサーバを使用します。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * Cloud Manager 設定 * を選択します。

2. HTTP プロキシで、構文を使用してサーバを入力します http://address:portをクリックして、サーバーの基本認証が必要な場合はユーザー名とパスワードを指定し、 * 保存 * をクリックします。

> Cloud Manager では、 @ 文字を含むパスワードはサポートされていません。

結果

プロキシサーバを指定すると、 AutoSupport メッセージの送信時にプロキシサーバを使用するように、新しい Cloud Volumes ONTAP システムが自動的に設定されます。ユーザが Cloud Volumes ONTAP システムを作成する前にプロキシサーバを指定しない場合は、 System Manager を使用して、各システムの AutoSupport オプションでプロキシサーバを手動で設定する必要があります。

Cloud Manager の HTTPS 証明書を更新します

Cloud Manager Web コンソールへの安全なアクセスを確保するために、 Cloud Manager HTTPS 証明書は有効期限が切れる前に更新する必要があります。証明書の有効期限が切れる前に証明書を更新しないと、ユーザが HTTPS を使用して Web コンソールにアクセスしたときに警告が表示されます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、 * HTTPS セットアップ * を選択します。

   Cloud Manager 証明書の詳細が表示されます。有効期限も表示されます。

2. [HTTPS 証明書の更新] をクリックし、手順に従って CSR を生成するか、独自の CA 署名証明書をインストールします。

結果

Cloud Manager は新しい CA 署名付き証明書を使用して、セキュアな HTTPS アクセスを提供します。

Cloud Manager をリストアしています

。 "NetApp Cloud Central アカウント" Cloud Manager の設定を簡単にリストアできます。アカウントは Cloud Central で実行されるサービスであるため、アカウントに関連付けたユーザ、ワークスペース、およびサービスコネクタには常にアクセスできます。Cloud Manager システムが誤って削除された場合も同様です。

> 3.7.1 リリース以降、 Cloud Manager では、バックアップのダウンロードとリストアに使用することはできなくなりました。Cloud Manager をリストアするには、次の手順を実行する必要があります。

手順

1. 既存の Cloud Central アカウントに新しい Cloud Manager システムを導入します。

   "導入オプション"

2. Cloud Manager にクラウドプロバイダアカウントとネットアップサポートサイトアカウントを追加します。

   これにより、クラウドプロバイダで追加の Cloud Volumes ONTAP システムを作成できるようになり、Cloud Manager を使用できるようになります。

   この新しい Cloud Manager システムで検出する既存の Cloud Volumes ONTAP システムを AWS キーを使

用して導入した場合は、この手順を実行することが重要です。Cloud Volumes ONTAP を適切に検出して管理するには、 Cloud Manager で AWS キーが必要になります。

- "Cloud Manager に AWS アカウントを追加する"
- "Cloud Manager への Azure アカウントの追加"
- "Cloud Manager へのネットアップサポートサイトのアカウントの追加"

3. 作業環境を再検出します。 Cloud Volumes ONTAP システム、オンプレミスクラスタ、クラウド構成用の NetApp Private Storage などです。
   - "Cloud Manager に既存の Cloud Volumes ONTAP システムを追加"
   - "ONTAP クラスタの検出"

結果

これで、アカウント、設定、作業環境を使用して Cloud Manager の設定がリストアされます。

Cloud Manager をアンインストールしています

Cloud Manager にはアンインストールスクリプトが含まれており、このスクリプトを使用してソフトウェアをアンインストールし、問題のトラブルシューティングを行ったり、ホストからソフトウェアを完全に削除したりできます。

手順

1. Linux ホストからアンインストールスクリプトを実行します。
   - /opt/application/NetApp/cloudmanager/bin/uninstall.sh [サイレント] *

   silent_ 確認を求めずにスクリプトを実行します。

ファイルサービス用のボリュームをプロビジョニングしてください

Azure NetApp Files のボリュームの管理

の NFS ボリュームを表示および作成します "Azure NetApp Files の特長" Cloud Manager から直接削除できます。

構成をセットアップする

Azure NetApp Files 用のボリュームを Cloud Manager から管理するには、いくつかの要件を満たす必要があります。

1. Azure NetApp Files をセットアップするには、 Azure ポータルで次の手順を実行する必要があります。
   - "Azure NetApp Files に登録します"
   - "ネットアップアカウントを作成します"
   - "容量プールをセットアップする"
   - "サブネットを Azure NetApp Files に委譲します"
2. Cloud Manager は次のように設定する必要があります。
   - Azure NetApp Files をセットアップしたアカウントで、 Cloud Manager が Azure で実行されている必要があります。
   - Cloud Manager 仮想マシンは、を通じて権限を受け取る必要があります "管理された ID"。

     Cloud Central から Cloud Manager を導入した場合は、すべての設定が完了します。Cloud Central は、システムによって割り当てられた管理対象 ID を Cloud Manager 仮想マシンで自動的に有効にします。

   Azure Marketplace から Cloud Manager を導入した場合は、これに準拠する必要があります "管理 ID を有効にする手順"。

   - Cloud Manager 仮想マシンに割り当てられる Azure ロールに、最新のに記載されている権限が含まれている必要があります "Azure 向け Cloud Manager ポリシー"：

     ```
     "Microsoft.NetApp/netAppAccounts/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
     ```

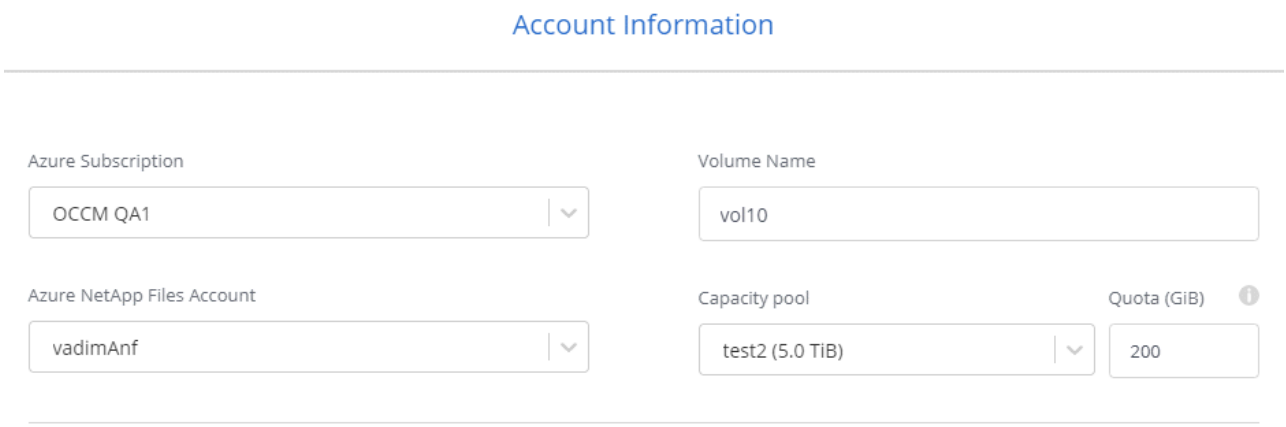
構成のセットアップが完了すると、 Cloud Manager の作業環境のページに Azure NetApp Files が自動的に表示されます。

ボリュームの作成

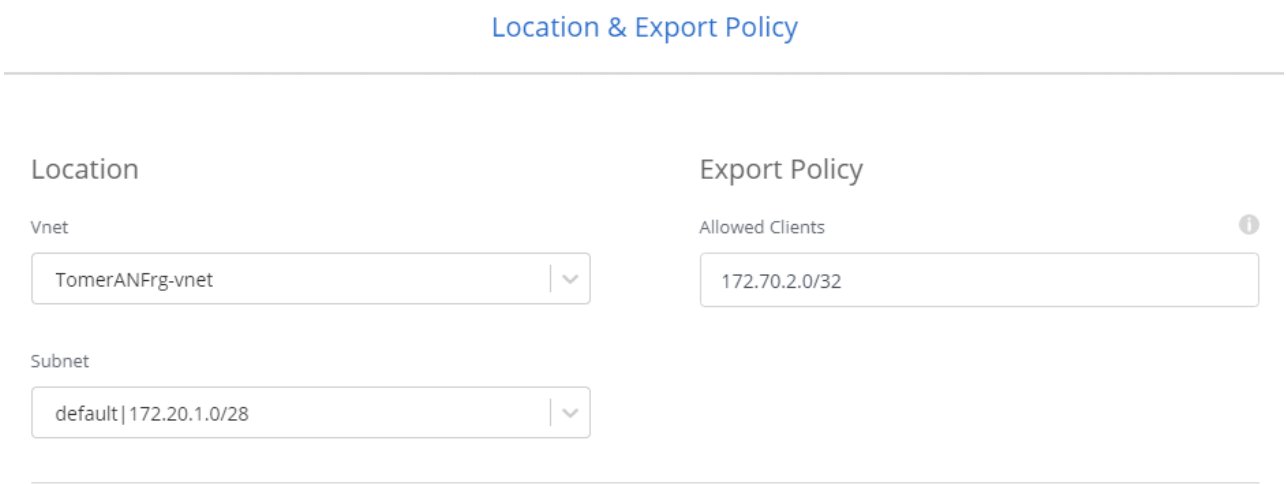
Cloud Manager では、 Azure NetApp Files 用の NFSv3 ボリュームを作成できます。

手順

1. 作業環境を開きます。
2. [新しいボリュームの追加] をクリックします。
3. 「 * アカウント情報 * 」ページで、ボリュームに関する基本的な詳細を入力します。
   a. Azure サブスクリプションと Azure NetApp Files アカウントを選択します。
   b. ボリュームの名前を入力します。
   c. 容量プールを選択し、ボリュームに割り当てられている論理ストレージの量であるクォータを指定します。



4. [場所とエクスポートポリシー *] ページに次の情報を入力します。
   a. VNet とサブネットを選択します。
   b. ボリュームへのアクセスを制御するエクスポートポリシーを設定します。



ページのスクリーンショット"]

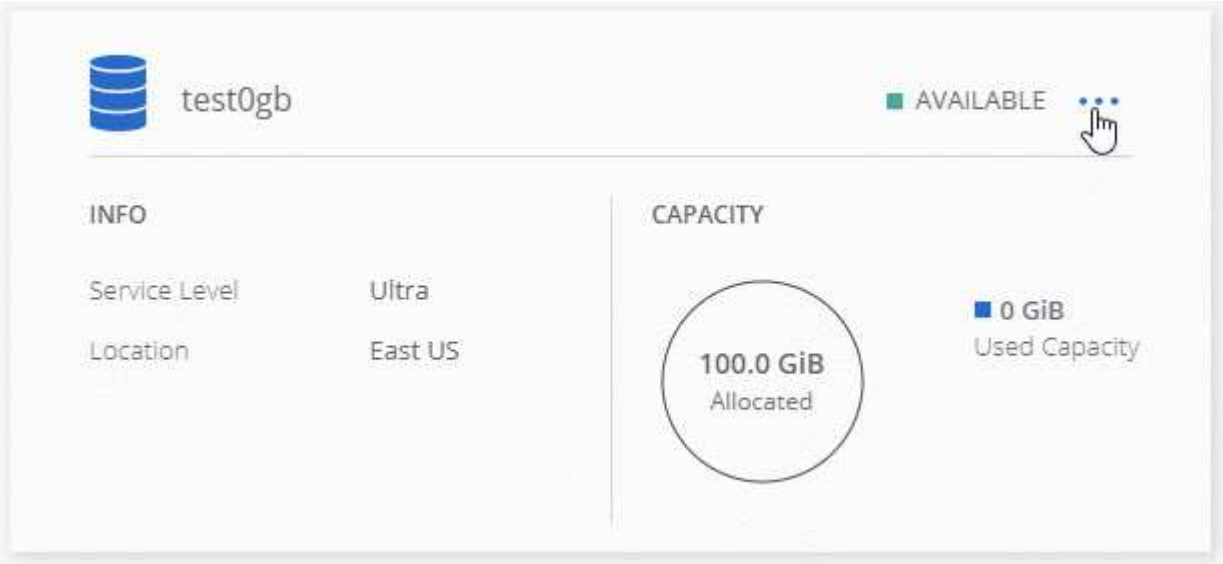
5. [Go*] をクリックします。

ボリュームのマウントパスを取得しています

Linux マシンにボリュームをマウントできるように、ボリュームのマウントパスをコピーします。

手順

1. 作業環境を開きます。
2. ボリュームにカーソルを合わせて、メニューをクリックします。



3. マウントコマンド * をクリックします。

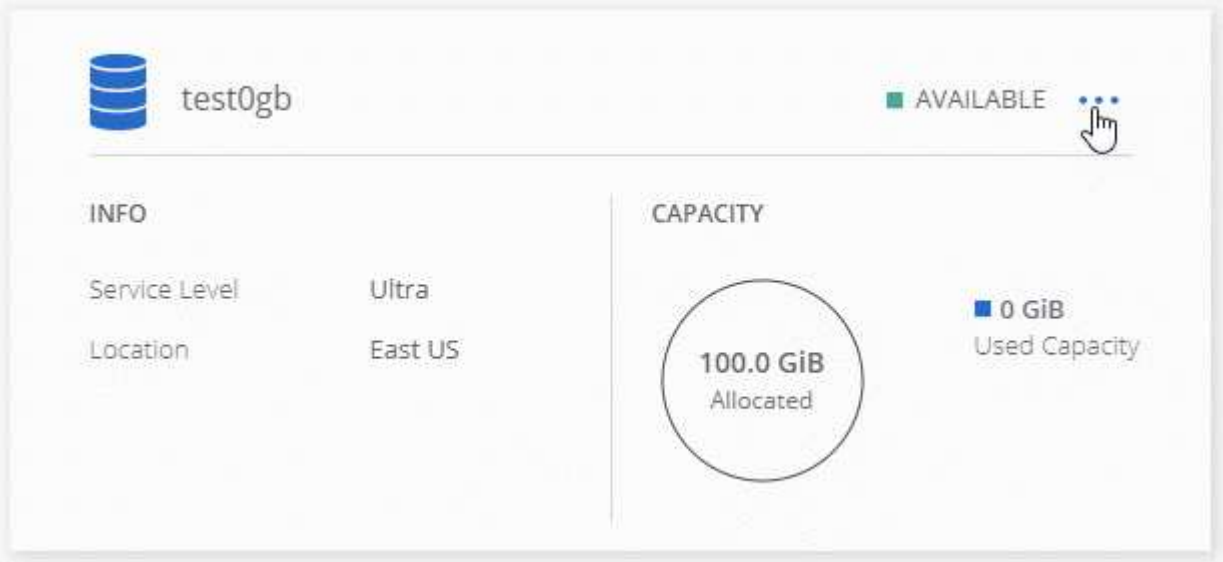
4. マウントパスをコピーし、コピーしたテキストを使用してボリュームを Linux マシンにマウントします。

ボリュームの削除

不要になったボリュームを削除します。

手順

1. 作業環境を開きます。
2. ボリュームにカーソルを合わせて、メニューをクリックします。



3. [削除（ Delete ）] をクリックします。
4. ボリュームを削除することを確定します。

サポートを受ける

サービスに関する一般的な質問については、 Cloud Manager のチャットを使用してください。

Azure NetApp Files に関連したテクニカルサポートの問題については、 Azure ポータルを使用して Microsoft にサポートリクエストを記録してください。関連する Microsoft サブスクリプションを選択し、「ストレージ」の下の「 Azure NetApp Files * 」サービス名を選択します。マイクロソフトサポートリクエストの作成に必要な残りの情報を入力します。

Cloud Manager では、 AutoSupport のローカルダウンロードをサポートダッシュボード * メニューオプションで実行できます。この 7z ファイルには、 Azure NetApp Files アカウントへのインバウンドおよびアウトバウンド通信を表示する Azure デバッグファイルが含まれます。

制限

- Cloud Manager では SMB ボリュームはサポートされません。
- Cloud Manager では、容量プールやボリューム Snapshot を管理することはできません。
- ボリュームは、初期サイズと単一のエクスポートポリシーで作成できます。ボリュームの編集は、 Azure ポータルの Azure NetApp Files インターフェイスから実行する必要があります。
- Cloud Manager は、 Azure NetApp Files との間のデータレプリケーションをサポートしていません。

関連リンク

- "NetApp Cloud Central ： Azure NetApp Files"
- "Azure NetApp Files のドキュメント"

Cloud Volumes Service for AWS を管理する

Cloud Manager を使用すると、で NFS Cloud Volume を検出できます "Cloud Volumes Service for AWS" サブスクリプション。検出後、 NFS Cloud Volume を Cloud Manager から直接追加することができます。

> Cloud Volumes Service for AWS では、 Cloud Manager で SMB ボリュームやデュアルプロトコルボリュームを使用することはできません。

始める前に

- Cloud Manager Cloud Volumes Service で、 AWS サブスクリプションに対する _existing_aws を検出できます。を参照してください "『 NetApp Cloud Volumes Service for AWS Account Setup Guide 』を参照してください" 月額プランをまだ設定していない場合は、

  Cloud Manager でリージョンを検出するには、リージョンごとに次のセットアッププロセスを実行し、Cloud Volumes Service から最初のボリュームをプロビジョニングする必要があります。

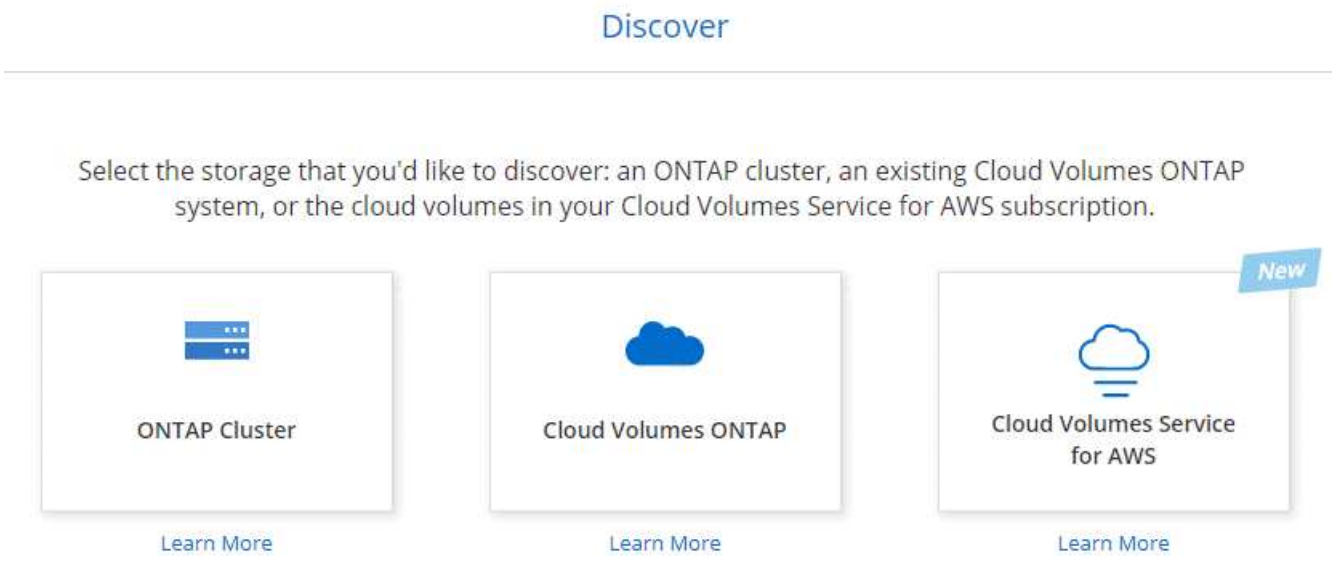
- Cloud Manager に提供するためには、 Cloud Volumes API のキーとシークレットキーを取得する必要があります。 "手順については、 Cloud Volumes Service for AWS のドキュメントを参照してください"。

Cloud Volumes Service for AWS サブスクリプションを検出しています

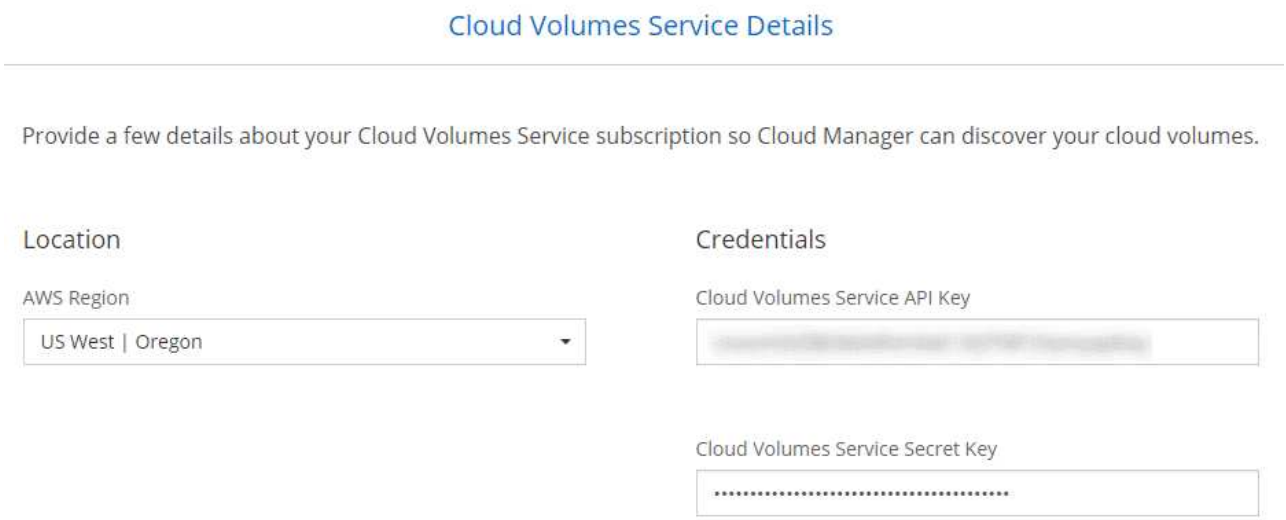
最初に、 AWS リージョンの Cloud Volume を検出する必要があります。追加のリージョンはあとで検出できます。

手順

1. 作業環境ページで、 * 検出 * をクリックします。
2. Cloud Volumes Service for AWS * を選択します。



3. Cloud Volumes Service サブスクリプションに関する情報を入力します。
   a. Cloud Volume が配置されている AWS リージョンを選択します。
   b. Cloud Volume の API キーとシークレットキーを入力します。 "手順については、 Cloud Volumes Service for AWS のドキュメントを参照してください"。
   c. [Go*] をクリックします。



結果

これで、 Cloud Manager の作業環境のページに Cloud Volumes Service for AWS の設定が表示されます。

追加のリージョンを検出する

追加のリージョンに Cloud Volume がある場合は、各リージョンを検出する必要があります。

手順

1. 作業環境ページで、作業環境を選択します（ダブルクリックして開かないでください）。
2. 右ペインで、 * 別の地域で Cloud Volumes Service を検出 * をクリックします。

3. Cloud Volumes Service サブスクリプションに関する情報を入力します。
   a. Cloud Volume が配置されている AWS リージョンを選択します。
   b. Cloud Volume の API キーとシークレットキーを入力します。 "手順については、 Cloud Volumes Service for AWS のドキュメントを参照してください"。
   c. [Go*] をクリックします。

結果

Cloud Manager によって、選択したリージョン内の Cloud Volume に関する情報が検出されます。

Cloud Volume を作成しています

Cloud Manager で NFSv3 Cloud Volume を作成できます。Cloud Volume は、初期サイズと単一のエクスポートポリシーでのみ作成できます。ボリュームの編集は、クラウドボリュームサービスのユーザインターフェイスから実行する必要があります。

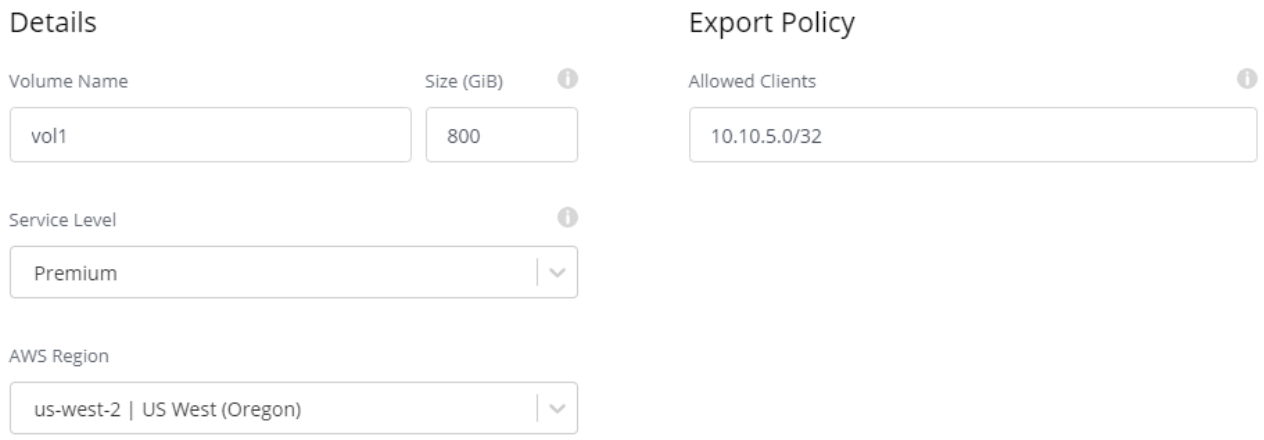
1. 作業環境を開きます。
2. [新しいボリュームの追加] をクリックします。
3. ボリュームの詳細を入力します。
   a. ボリュームの名前を入力します。
   b. 100GiB ~ 90,000GiB の範囲でサイズを指定します（ 88 TiB に相当）。

      Cloud Manager ではボリュームが GiB 単位で表示され、 Cloud Volumes Service では GB 単位で表示されます。

   c. サービスレベルとして、 Standard 、 Premium 、または Extreme を指定します。

      "これらのサービスレベルの詳細については、こちらをご覧ください"。

   d. リージョンを選択します。Cloud Manager によって検出されたリージョン内にボリュームを作成できます。
   e. IP アドレスまたは Classless Inter-Domain Routing （ CIDR ）を指定して、クライアントアクセスを制限します。



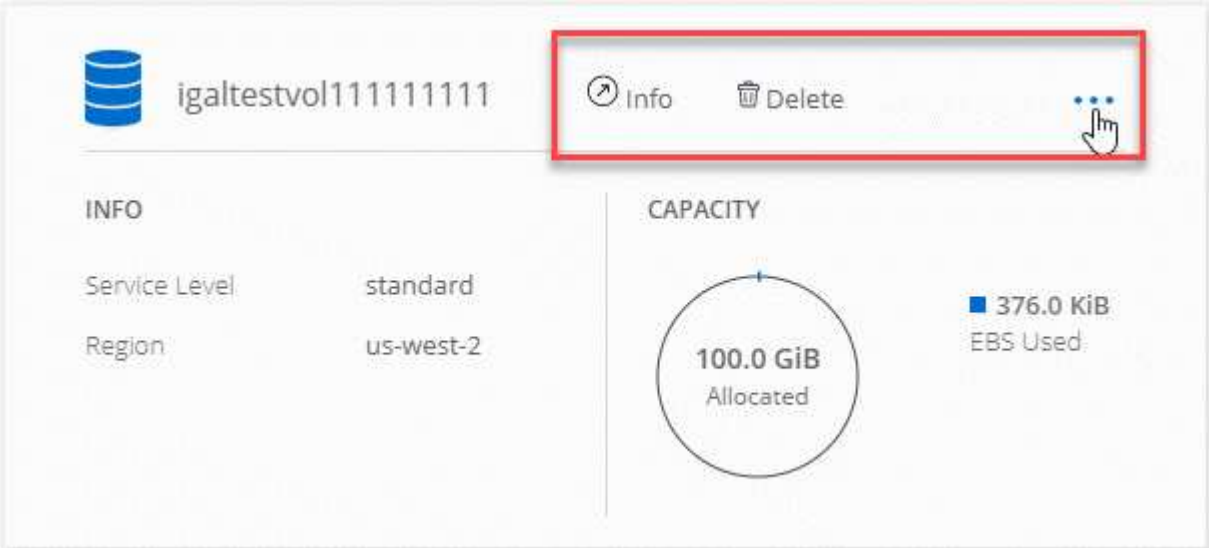
4. [Go*] をクリックします。

Cloud Volume を削除しています

不要になった Cloud Volume を削除します。

手順

1. 作業環境を開きます。
2. ボリュームにカーソルを合わせて、メニューをクリックします。[削除（ Delete ）] をクリックします。



3. ボリュームを削除することを確定します。

サポートを受ける

サービスに関する一般的な質問については、 Cloud Manager のチャットを使用してください。

クラウドボリュームに関連するテクニカルサポートの問題については、 Cloud Volumes Service ユーザーインタフェースの「サポート」タブにある 20 桁の「 930 」シリアル番号を使用してください。このサポート ID は、 Web チケットを開くとき、またはサポートに電話するときに使用します。Cloud Volumes Service のシリアル番号は、必ず Cloud Volumes Service のユーザインターフェイスから有効にしてください。 "ここでは、これらの手順について説明します"。

制限

- Cloud Manager では、 SMB またはデュアルプロトコルのボリュームはサポートされません。
- Cloud Volume は、初期サイズと単一のエクスポートポリシーでのみ作成できます。ボリュームの編集は、クラウドボリュームサービスのユーザインターフェイスから実行する必要があります。
- Cloud Manager では、 Cloud Volumes Service for AWS サブスクリプションとの間のデータレプリケーションはサポートされていません。
- Cloud Manager から Cloud Volumes Service for AWS サブスクリプションを削除することはできません。Cloud Manager からリージョンを検出する場合、料金は発生しません。

関連リンク

- "NetApp Cloud Central ： Cloud Volumes Service for AWS"
- "NetApp Cloud Volumes Service for AWS のドキュメント"

API と自動化

コードとしてのインフラの自動化サンプル

このページのリソースを使用して、の統合を支援します Cloud Manager と Cloud Volumes ONTAP の組み合わせをで使用できます "コードとしてのインフラ"。

DevOps チームは、さまざまなツールを使用して新しい環境のセットアップを自動化し、インフラをコードとして扱うことができます。Ansible と Terraform の 2 つのツールがあります。ネットアップでは、 Ansible と Terraform のサンプルを開発しました。このサンプルを使用することで、 DevOps チームは Cloud Manager を使用して Cloud Volumes ONTAP を自動化し、コードとしてインフラと統合できます。

"自動化のサンプルを表示します"。

たとえば、サンプルの Ansible プレイブックを使用して、 Cloud Manager と Cloud Volumes ONTAP を導入し、アグリゲートを作成し、ボリュームを作成できます。環境のサンプルを変更するか、サンプルに基づいて新しいプレイブックを作成します。

- 関連リンク *
- "NetApp Cloud ブログ： Using Cloud Manager REST API with Federated Access"
- "ネットアップのクラウドブログ：「 Cloud Automation with Cloud Volumes ONTAP and REST"
- "ネットアップのクラウドブログ： Automated Data Cloning for Cloud Based Testing of Software Applications"
- "ネットアップのブログ：「 Infrastructure-as-Code （ IAC ） Accelerated with Ansible + NetApp"
- "NetApp thePub ： Ansible による構成管理と自動化"
- "NetApp thePub ： Ansible ONTAP の役割"

参照

よくある質問： Cloud Manager と NetApp Cloud Central の統合

Cloud Manager 3.4 以前からのアップグレードの場合、 NetApp Cloud Central と統合する特定の Cloud Manager システムは選択されます（まだ統合されていない場合）。この FAQ では、このプロセスに関する質問にお答えします。

NetApp Cloud Central とは

NetApp Cloud Central は、 NetApp クラウドデータサービスにアクセスして管理するための一元化された場所を提供します。これらのサービスを利用すると、重要なアプリケーションをクラウドで実行したり、自動化された DR サイトを作成したり、 SaaS データをバックアップしたり、複数のクラウド間でデータを効果的に移行および制御したりすることができます。

ネットアップが Cloud Manager システムと Cloud Central を統合する理由は何ですか。

Cloud Manager と NetApp Cloud Central を統合すると、導入環境の簡易化、複数の Cloud Manager システムの表示と管理を行う単一の場所、ユーザ認証の一元化など、いくつかのメリットが得られます。

統合プロセスではどうなりますか。

NetApp は、 Cloud Manager システム内のすべてのローカルユーザアカウントを、 Cloud Central で使用可能な中央集中型ユーザ認証に移行します。

中央集中型のユーザ認証はどのように機能しますか。

一元的なユーザ認証では、 Cloud Manager システム全体、および Cloud Manager と他のデータサービス（ Cloud Sync など）の間で同じクレデンシャルセットを使用できます。パスワードを忘れた場合は、簡単にリセットできます。

Cloud Central ユーザーアカウントにサインアップする必要がありますか？

NetApp は、 Cloud Manager システムと Cloud Central を統合する際に、 Cloud Central ユーザアカウントを作成します。登録プロセスを完了するには、パスワードをリセットするだけです。

Cloud Central ユーザーアカウントをすでにお持ちの場合はどうなりますか？

Cloud Manager へのログインに使用する電子メールアドレスが Cloud Central ユーザーアカウントの電子メールアドレスと一致する場合は、 Cloud Manager システムにログインできます。

Cloud Manager システムに複数のユーザアカウントがある場合はどうなりますか。

ネットアップは、すべてのローカルユーザアカウントを Cloud Central ユーザアカウントに移行します。すべてのユーザがパスワードをリセットする必要があります。

複数の Cloud Manager システムで同じ電子メールアドレスを使用するユーザアカウントを使用している場合はどうなりますか。

パスワードを一度リセットするだけで、同じ Cloud Central ユーザーアカウントを使用して各 Cloud Manager システムにログインできます。

ローカルユーザアカウントで無効な電子メールアドレスを使用している場合はどうなりますか。

パスワードをリセットするには、有効なメールアドレスが必要です。Cloud Manager インターフェイスの右下にあるチャットアイコンを使用してお問い合わせください。

Cloud Manager API 用の自動化スクリプトを使用している場合はどうなりますか。

すべての API は下位互換性があります。パスワードをリセットしたときにパスワードを変更した場合は、パスワードを使用するスクリプトを更新する必要があります。

Cloud Manager システムで LDAP を使用している場合はどうなりますか。

システムで LDAP を使用している場合、ネットアップはシステムを Cloud Central と自動的に統合することはできません。次の手順を手動で実行する必要があります。

1. から新しい Cloud Manager システムを導入します "NetApp Cloud Central"。
2. "新しいシステムで LDAP を設定します。"。
3. "既存の Cloud Volumes ONTAP システムを検出" 新しい Cloud Manager システムから作成します。
4. 古い Cloud Manager システムを削除します。

Cloud Manager システムのインストール先はどこにいても問題ありませんか。

いいえネットアップは、 AWS 、 Azure 、オンプレミスなど、システムの場所に関係なく、 Cloud Central とシステムを統合します。

> 唯一の例外は、 AWS コマーシャルクラウドサービス環境です。

AWS のセキュリティグループルール

Cloud Manager は、 Cloud Manager と Cloud Volumes ONTAP が正常に動作するために必要なインバウンドルールとアウトバウンドルールを含む AWS セキュリティグループを作成します。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

Cloud Manager のルール

Security Group for Cloud Manager には、インバウンドルールとアウトバウンドルールの両方が必要です。

Cloud Manager のインバウンドルール

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

プロトコル	ポート	目的
SSH	22	Cloud Manager ホストへの SSH アクセスを提供します
HTTP	80	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTP アクセスと Cloud Compliance からの接続を提供します
HTTPS	443	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTPS アクセスを提供します
TCP	3128	AWS ネットワークで NAT やプロキシを使用していない場合に、 Cloud Compliance インスタンスにインターネットアクセスを提供します

Cloud Manager のアウトバウンドルール

Cloud Manager 用に事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Manager 用に事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

アウトバウンドトラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Manager によるアウトバウンド通信に必要なポートのみを開くことができます。

送信元 IP アドレスは Cloud Manager ホストです。

サービス	プロトコル	ポート	宛先	目的
Active Directory	TCP	88	Active Directory フォレスト	Kerberos V 認証
	TCP	139	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	Active Directory フォレスト	LDAP
	TCP	445	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	TCP	749	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（RPCSEC_GSS）
	UDP	137	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	Active Directory フォレスト	NetBIOS データグラムサービス
	UDP	464	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	HTTPS	443	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
API コール	TCP	3000	ONTAP クラスタ管理 LIF	ONTAP への API コール
	TCP	8088	S3 へのバックアップ	S3 へのバックアップを API で呼び出します
DNS	UDP	53	DNS	Cloud Manager による DNS 解決に使用されます
クラウドコンプライアンス	HTTP	80	Cloud Compliance インスタンス	Cloud Volumes ONTAP 向けクラウドコンプライアンス

Cloud Volumes ONTAP のルール

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

Cloud Volumes ONTAP のインバウンドルール

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
HTTPS	443	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
SSH	22	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	139	CIFS の NetBIOS サービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバデーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
UDP	111	NFS のリモートプロシージャコール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

Cloud Volumes ONTAP のアウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての ICMP	すべて	すべての発信トラフィック
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	プロトコル	ポート	ソース	宛先	目的
Active Directory	TCP	88	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	UDP	137	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	ノード管理 LIF	Active Directory フォレスト	LDAP
	TCP	445	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	UDP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	TCP	749	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）
	TCP	88	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V 認証
	UDP	137	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	データ LIF （NFS、CIFS）	Active Directory フォレスト	LDAP
	TCP	445	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	UDP	464	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos キー管理
	TCP	749	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）
S3 へのバックアップ	TCP	5010	クラスタ間 LIF	バックアップエンドポイントまたはリストアエンドポイント	S3 へのバックアップ処理とリストア処理 フィーチャー（Feature）

サービス	プロトコル	ポート	ソース	宛先	目的
クラスタ	すべてのトラフィック	すべてのトラフィック	1 つのノード上のすべての LIF	もう一方のノードのすべての LIF	クラスタ間通信（ Cloud Volumes ONTAP HA のみ）
	TCP	3000	ノード管理 LIF	HA メディエータ	ZAPI コール（ Cloud Volumes ONTAP HA のみ）
	ICMP	1.	ノード管理 LIF	HA メディエータ	キープアライブ（ Cloud Volumes ONTAP HA のみ）
DHCP	UDP	68	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	UDP	67	ノード管理 LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 ～ 18699	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	TCP	25	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	TCP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	TCP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	TCP	11104	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	TCP	11105	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	UDP	514	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

HA Mediator 外部セキュリティグループのルール

Cloud Volumes ONTAP HA Mediator 用に事前定義された外部セキュリティグループには、次のインバウンドルールとアウトバウンドルールが含まれています。

インバウンドルール

インバウンドルールの送信元は 0.0.0.0/0 です。

プロトコル	ポート	目的
SSH	22	HA メディエータへの SSH 接続
TCP	3000	Cloud Manager からの RESTful API アクセス

アウトバウンドルール

HA メディエータの定義済みセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

HA Mediator 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれます。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 HA メディエータによる発信通信に必要なポートだけを開くことができます。

プロトコル	ポート	宛先	目的
HTTP	80	Cloud Manager の IP アドレス	メディエーターのアップグレードをダウンロードします
HTTPS	443	AWS API サービス	ストレージのフェイルオーバーを支援します
UDP	53	AWS API サービス	ストレージのフェイルオーバーを支援します

ポート 443 および 53 を開く代わりに、ターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを作成できます。

HA Mediator 内部セキュリティグループのルール

Cloud Volumes ONTAP HA Mediator 用に事前定義された内部セキュリティグループには、次のルールが含まれています。Cloud Manager は常にこのセキュリティグループを作成します。独自のオプションはありません。

インバウンドルール

事前定義されたセキュリティグループには、次の着信ルールが含まれています。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信

アウトバウンドルール

定義済みのセキュリティグループには、次の発信ルールが含まれます。

プロトコル	ポート	目的
すべてのトラフィック	すべて	HA メディエータと HA ノード間の通信

Azure のセキュリティグループルール

Cloud Manager は、 Cloud Manager と Cloud Volumes ONTAP が正常に動作するために必要なインバウンドルールとアウトバウンドルールを含む Azure セキュリティグループを作成します。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

Cloud Manager のルール

Security Group for Cloud Manager には、インバウンドルールとアウトバウンドルールの両方が必要です。

Cloud Manager のインバウンドルール

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

ポート	プロトコル	目的
22	SSH	Cloud Manager ホストへの SSH アクセスを提供します
80	HTTP	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTP アクセスを提供します
443	HTTPS	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTPS アクセスを提供します

Cloud Manager のアウトバウンドルール

Cloud Manager 用に事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Manager 用に事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

アウトバウンドトラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Manager によるアウトバウンド通信に必要なポートのみを開くことができます。

送信元 IP アドレスは Cloud Manager ホストです。

サービス	ポート	プロトコル	宛先	目的
Active Directory	88	TCP	Active Directory フォレスト	Kerberos V 認証
	139	TCP	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP	Active Directory フォレスト	LDAP
	445	TCP	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	749	TCP	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（RPCSEC_GSS）
	137	UDP	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	Active Directory フォレスト	NetBIOS データグラムサービス
	464	UDP	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	443	HTTPS	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
API コール	3000	TCP	ONTAP クラスタ管理 LIF	ONTAP への API コール
DNS	53	UDP	DNS	Cloud Manager による DNS 解決に使用されます

Cloud Volumes ONTAP のルール

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

シングルノードシステムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
1000 inbound_ssh	22 TCP	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
1001 INBOUND _http	80 TCP	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
1002 INBOUND _111_TCP	111 TCP	Any から Any	NFS のリモートプロシージャコール
1003 INBONED_111_UDP	111 UDP	Any から Any	NFS のリモートプロシージャコール
1004 INBOUND _139	139 TCP	Any から Any	CIFS の NetBIOS サービスセッション
1005 inbound_161-162_TCP	161-162 TCP	Any から Any	簡易ネットワーク管理プロトコル
1006 INBOUND _161-162_UDP	UDP 161-162	Any から Any	簡易ネットワーク管理プロトコル
1007 INBOUND _443	443 tcp	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
1008 INBOUND _445	445 TCP	Any から Any	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
1009 INBOUND _635_TCP	635 TCP	Any から Any	NFS マウント
1010 INBOUND _635_UDP	635 UDP	Any から Any	NFS マウント
1011 INBOUND _749	749 TCP	Any から Any	Kerberos
1012 INBOUND _2049 _TCP	2049 TCP	Any から Any	NFS サーバデーモン
1013 INBOUND _2049 _UDP	2049 UDP	Any から Any	NFS サーバデーモン
1014 インバウンド _3260	3260 TCP	Any から Any	iSCSI データ LIF を介した iSCSI アクセス

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
1015 INBOUND _4045-4046_tcp の略	4045-4046 TCP	Any から Any	NFS ロックデーモンとネットワークステータスモニタ
1016 INBOUND _4045-4046_UDP	4045-4046 UDP	Any から Any	NFS ロックデーモンとネットワークステータスモニタ
1017 INBOUND _10000	10000 TCP	Any から Any	NDMP を使用したバックアップ
1018 INBOUND _11104-11105	11104-11105 TCP	Any から Any	SnapMirror によるデータ転送
3000 inbound_deny_all_tcp	任意のポート TCP	Any から Any	他のすべての TCP インバウンドトラフィックをブロックします
3001 INBOUND _DENY_ALL_UDP	任意のポート UDP	Any から Any	他のすべての UDP 着信トラフィックをブロックします
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

HA システムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。

> HA システムのインバウンドデータトラフィックは Azure Standard Load Balancer を経由するため、シングルノードシステムよりもインバウンドルールが少なくなります。そのため、「AllowAzureLoadBalancerInBound 」ルールに示されているように、ロードバランサからのトラフィックがオープンである必要があります。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
100 インバウンド _ 443	443 ：任意のプロトコル	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
101 INBOUND _111_TCP	111 すべてのプロトコル	Any から Any	NFS のリモートプロシージャコール

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
102 インバウンド _2049 _TCP	2049 任意のプロトコル	Any から Any	NFS サーバデーモン
111 inbound_ssh	22 すべてのプロトコル	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
121 INBOUND _53	53 任意のプロトコル	Any から Any	DNS と CIFS
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

Cloud Volumes ONTAP のアウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	ポート	プロトコル	ソース	宛先	目的
Active Directory	88	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	137	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP	ノード管理 LIF	Active Directory フォレスト	LDAP
	445	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	464	UDP	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	749	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）
	88	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V 認証
	137	UDP	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	LDAP
	445	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	464	UDP	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos キー管理
	749	TCP	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）
DHCP	68	UDP	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	67	UDP	ノード管理 LIF	DHCP	DHCP サーバ

サービス	ポート	プロトコル	ソース	宛先	目的
DNS	53	UDP	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	18600 ～ 18699	TCP	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	25	TCP	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	161	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	161	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	11104	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	11105	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	514	UDP	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

GCP のファイアウォールルール

Cloud Manager が作成する GCP ファイアウォールルールには、 Cloud Manager と Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールが含まれています。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

Cloud Manager のルール

Cloud Manager のファイアウォールルールには、インバウンドとアウトバウンドの両方のルールが必要です。

Cloud Manager のインバウンドルール

定義済みのファイアウォールルールのインバウンドルールのソースは 0.0.0.0/0 です。

プロトコル	ポート	目的
SSH	22	Cloud Manager ホストへの SSH アクセスを提供します

プロトコル	ポート	目的
HTTP	80	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTP アクセスを提供します
HTTPS	443	クライアント Web ブラウザから Cloud Manager Web コンソールへの HTTPS アクセスを提供します

Cloud Manager のアウトバウンドルール

Cloud Manager の事前定義されたファイアウォールルールで、すべてのアウトバウンドトラフィックがオープンされます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Manager 用の事前定義されたファイアウォールルールには、次のアウトバウンドルールが含まれています。

プロトコル	ポート	目的
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

アウトバウンドトラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Manager によるアウトバウンド通信に必要なポートのみを開くことができます。

送信元 IP アドレスは Cloud Manager ホストです。

サービス	プロトコル	ポート	宛先	目的
Active Directory	TCP	88	Active Directory フォレスト	Kerberos V 認証
	TCP	139	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	Active Directory フォレスト	LDAP
	TCP	445	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	TCP	749	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（RPCSEC_GSS）
	UDP	137	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	Active Directory フォレスト	NetBIOS データグラムサービス
	UDP	464	Active Directory フォレスト	Kerberos キー管理
API コールと AutoSupport	HTTPS	443	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	GCP および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
API コール	TCP	3000	ONTAP クラスタ管理 LIF	ONTAP への API コール
DNS	UDP	53	DNS	Cloud Manager による DNS 解決に使用されます

Cloud Volumes ONTAP のルール

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

Cloud Volumes ONTAP のインバウンドルール

定義済みセキュリティグループのインバウンドルールの送信元は 0.0.0.0/0 です。

プロトコル	ポート	目的
すべての ICMP	すべて	インスタンスの ping を実行します
HTTP	80	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
HTTPS	443	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
SSH	22	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
TCP	111	NFS のリモートプロシージャコール
TCP	139	CIFS の NetBIOS サービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
TCP	635	NFS マウント
TCP	749	Kerberos
TCP	2049	NFS サーバデーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFS ロックデーモン
TCP	4046	NFS のネットワークステータスモニタ
TCP	10000	NDMP を使用したバックアップ
TCP	11104	SnapMirror のクラスタ間通信セッションの管理
TCP	11105	クラスタ間 LIF を使用した SnapMirror データ転送
UDP	111	NFS のリモートプロシージャコール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFS マウント
UDP	2049	NFS サーバデーモン
UDP	4045	NFS ロックデーモン
UDP	4046	NFS のネットワークステータスモニタ
UDP	4049	NFS rquotad プロトコル

Cloud Volumes ONTAP のアウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれていま

す。

プロトコル	ポート	目的
すべての ICMP	すべて	すべての発信トラフィック
すべての TCP	すべて	すべての発信トラフィック
すべての UDP	すべて	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、 Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。

source は、 Cloud Volumes ONTAP システムのインターフェイス（ IP アドレス）です。

サービス	プロトコル	ポート	ソース	宛先	目的
Active Directory	TCP	88	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	UDP	137	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	ノード管理 LIF	Active Directory フォレスト	LDAP
	TCP	445	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	UDP	464	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	TCP	749	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）
	TCP	88	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V 認証
	UDP	137	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	138	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS データグラムサービス
	TCP	139	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP	389	データ LIF （NFS、CIFS）	Active Directory フォレスト	LDAP
	TCP	445	データ LIF （NFS、CIFS）	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	TCP	464	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE）
	UDP	464	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos キー管理
	TCP	749	データ LIF （NFS、CIFS）	Active Directory フォレスト	Kerberos V Change & Set Password（RPCSEC_GSS）

サービス	プロトコル	ポート	ソース	宛先	目的
クラスタ	すべてのトラフィック	すべてのトラフィック	1 つのノード上のすべての LIF	もう一方のノードのすべての LIF	クラスタ間通信（ Cloud Volumes ONTAP HA のみ）
	TCP	3000	ノード管理 LIF	HA メディエータ	ZAPI コール（ Cloud Volumes ONTAP HA のみ）
	ICMP	1.	ノード管理 LIF	HA メディエータ	キープアライブ（ Cloud Volumes ONTAP HA のみ）
DHCP	UDP	68	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	UDP	67	ノード管理 LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理 LIF とデータ LIF （ NFS 、 CIFS ）	DNS	DNS
NDMP	TCP	18600 ～ 18699	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	TCP	25	ノード管理 LIF	メールサーバ	SMTP アラート。 AutoSupport に使用できます
SNMP	TCP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	161	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	TCP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	UDP	162	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	TCP	11104	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	TCP	11105	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	UDP	514	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

AWS Marketplace の Cloud Manager と Cloud Volumes ONTAP のページ

AWS Marketplace では、 Cloud Manager と Cloud Volumes ONTAP 向けのサービスがいくつか提供されています。使用する必要があるページがわからない場合は、以下をお読みください。目標に基づいて適切なページに移動します。

いずれの場合も、 AWS Marketplace から AWS で Cloud Volumes ONTAP を起動することはできないことに注意してください。Cloud Manager から直接起動する必要があります。

目標	**AWS Marketplace** のページで使用できます	詳細情報
バージョン 9.6 以降では、 Cloud Volumes ONTAP PAYGO の導入を有効にします	"Cloud Manager （ Cloud Volumes ONTAP 用）"	この AWS Marketplace ページでは、 Cloud Volumes ONTAP 9.6 以降の PAYGO バージョンに課金できます。また、 Cloud Volumes ONTAP アドオン機能の課金も可能です。このページでは、 AWS で Cloud Manager を起動することはできません。から実行する必要があります "NetApp Cloud Central"または、この表の 4 行目に記載された AMI を使用することもできます。
Cloud Volumes ONTAP でアドオン機能を有効にする（ PAYGO または BYOL ）		
ネットアップから購入したライセンス（ BYOL ）を使用して Cloud Volumes ONTAP を導入可能	• "Cloud Volumes ONTAP for AWS （ BYOL ）" • "Cloud Volumes ONTAP for AWS - 高可用性（ BYOL ）"	これらの AWS Marketplace ページでは、単一のノードまたは HA バージョンの Cloud Volumes ONTAP BYOL をサブスクライブできます。
AWS Marketplace から AMI を使用して Cloud Manager を導入	"NetApp Cloud Manager （ NetApp Cloud Volumes ONTAP 用）"	から AWS で Cloud Manager を起動することを推奨します "NetApp Cloud Central"ただし、必要に応じて、この AWS Marketplace のページから起動することもできます。
Cloud Volumes ONTAP PAYGO （ 9.5 以前）の導入が可能	• "Cloud Volumes ONTAP for AWS" • "Cloud Volumes ONTAP for AWS - 高可用性"	AWS Marketplace のこれらのページでは、バージョン 9.5 以前の Cloud Volumes ONTAP の単一ノードまたは HA バージョンをサブスクライブできます。バージョン 9.6 以降では、 PAYGO の導入については、この表の 1 行目に記載された AWS Marketplace のページでサブスクライブする必要があります。

Cloud Manager でクラウドプロバイダの権限が使用される仕組み

Cloud Manager からクラウドプロバイダの処理を実行するには権限が必要です。これらの権限はに含まれています "ネットアップが提供するポリシー"。このような権限を持つ Cloud Manager の機能を理解しておく必要があるかもしれません。

Cloud Manager が AWS 権限を使用して実行する処理

Cloud Manager は AWS アカウントを使用して、 EC2 、 S3 、 CloudFormation 、 IAM 、 Security Token Service （ STS ）、 Key Management Service （ KMS ）などの複数の AWS サービスへの API コールを行います。

アクション	目的
"EC2:StartInstances" 、 "EC2:StopInstances" 、 "EC2:DescribeInstances" 、 "EC2:DescribeInstanceStatus" 、 "EC2:RunInstances" 、 "EC2:TerminateInstances" 、 "EC2:ModifyInstanceAttribute" 、	Cloud Volumes ONTAP インスタンスを起動し、インスタンスを停止、開始、監視します。
"EC2: DescribeInstanceAttribute" 、	サポートされているインスタンスタイプで Enhanced Networking が有効になっていることを確認します。
「 EC2 ：説明文」、「 EC2 ：説明文」、	Cloud Volumes ONTAP HA 構成を起動します。
EC2 ： createTags 、	Cloud Manager が作成するすべてのリソースに「 workingEnvironment 」タグと「 workingEnvironmId 」タグを付けます。Cloud Manager では、これらのタグを使用してメンテナンスとコスト割り当てを行います。
"EC2:CreateVolume" 、 "EC2:DescribeVolumes" 、 "EC2:ModifyVolumeAttribute" 、 "EC2:AttachVolume" 、 "EC2:DeleteVolume" 、 "EC2:DetachVolume" 、	Cloud Volumes ONTAP がバックエンドストレージとして使用する EBS ボリュームを管理します。
"EC2:CreateSecurityGroup" 、 "EC2:DeleteSecurityGroup" 、 "EC2:RevokeSecurityGroupEgress " 、 "EC2:AuthorizeSecurityGroupEgress " 、 "EC2:RevokeSecurityGroupIngress " 、 "EC2:RevokeSecurityGroupIngress " 、	Cloud Volumes ONTAP 用の定義済みセキュリティグループを作成します。
"EC2:CreateNetworkInterface", "EC2:DescribeNetworkInterfaces ", "EC2:DeleteNetworkInterface", "EC2:ModifyNetworkInterfaceAttribute",	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 EC2 ：説明サブネット」、「 EC2 ：説明 VPC 」、	Cloud Volumes ONTAP 用の新しい作業環境を作成するときに必要な、デスティネーションサブネットとセキュリティグループのリストを取得します。
EC2 ： DescribeDHCPOptions	Cloud Volumes ONTAP インスタンスの起動時に DNS サーバとデフォルトのドメイン名を決定します。
「 EC2 ： CreateSnapshot 」、「 EC2 ： DeleteSnapshot 」、「 EC2 ： DescribeSnapshot 」、	初期セットアップ時、および Cloud Volumes ONTAP インスタンスが停止したときに、 EBS ボリュームのスナップショットを作成します。
"EC2:GetConsoleOutput" 、	AutoSupport メッセージに添付された Cloud Volumes ONTAP コンソールをキャプチャします。
「 EC2 ：説明キーペア」、	インスタンスの起動時に使用可能なキーペアのリストを取得します。
「 EC2 ：説明論」、	使用可能な AWS リージョンのリストを取得します。
EC2 ： DeleteTags 、 EC2 ： DescribeTags 、	Cloud Volumes ONTAP インスタンスに関連付けられたリソースのタグを管理します。

アクション	目的
CloudFormation ： CreateStack 」、「 CloudFormation ： DeleteStack 」、「 CloudFormation ： DescribeStack 」、「 CloudFormation ： DescribeStackEvents 」、「 CloudFormation ： ValidateTemplate 」、	Cloud Volumes ONTAP インスタンスを起動します。
"iam ： PassRole" 、 "iam ： CREATEROLE" 、 "iam ： PutRolePolicy " 、 "iam ： CreateInstanceProfile" 、 "iam ： DeleteRolePolicy " 、 "iam ： AddRoleToInstanceProfile" 、 "IAM ： RemoveRoleInstanceFromProfile" 、 "iam ： DeleteInstanceProfile" 、 "iam ： DeleteInstanceProfile	Cloud Volumes ONTAP HA 構成を起動します。
"IAM:ListInstanceProfiles" 、 "STS: DecodeAuthorizationMessage" 、 "EC2:AssociateIamInstanceProfile" 、 "EC2:DescribeIamInstanceProfileAssociations" 、 "EC2:DisassociateIamInstanceProfileProfile" 、	Cloud Volumes ONTAP インスタンスのインスタンスプロファイルを管理します。
「 s3 ： GetBucketTagging 」、「 s3 ： GetBucketLocation 」、「 s3 ： ListAllMyBuckets 」、「 s3 ： ListBucket 」	AWS S3 バケットに関する情報を取得して、 Cloud Manager を NetApp Data Fabric Cloud Sync サービスと統合できるようにします。
s3 ： CreateBucket 、 s3 ： DeleteBucket 、 s3 ： GetLifecycleConfiguration 、 s3 ： PutLifecycleConfiguration 、 s3 ： PutBucketTagging "s3 ： ListBucketVersions " 、	Cloud Volumes ONTAP システムが容量階層として使用する S3 バケットを管理します。
"KMS: List*", "KMS: Describe*"	AWS キー管理サービスからキーに関する情報を取得します。
"CE:GetReservationUtilization" 、 "CE:GetDimensionValues" 、 "CE:GetCostAndUsage", "CE:GetTags"	Cloud Volumes ONTAP の AWS コストデータを取得します。
"EC2:CreatePlacementGroup" 、 "EC2:DeletePlacementGroup"	単一の AWS アベイラビリティゾーンに HA 構成を導入すると、 Cloud Manager は 2 つの HA ノードと AWS 分散配置グループ内のメディエーターを起動します。

クラウドマネージャーが **Azure** の権限で行うこと

Cloud Manager Azure ポリシーには、 Cloud Manager が Azure で Cloud Volumes ONTAP を導入および管理するために必要な権限が含まれています。

アクション	目的
「 Microsoft.Compute/locations/operations/read" 」、「 Microsoft.Compute/locations/vmSizes/read" 」、「 Microsoft.Compute/operations/read" 」、「 Microsoft.Compute/virtualMachines/instanceView/read " 」、「 Microsoft.Compute/virtualMachines/powerOff/action" 」、「 Microsoft.Compute/virtualMachines/read" 」、「 Microsoft.Compute/virtualMachines/restart/action" 」、「 Microsoft.Compute/virtualMachines/start/action" 」、「 Microsoft.Compute/virtualMachines/deallocate/action" 」、「 Microsoft.Compute/virtualMachines/vmSizes/read" 」、「 Microsoft.Compute/virtualMachines/write" 」、	Cloud Volumes ONTAP を作成し、システムのステータスを停止、開始、削除、取得します。
「 microsoft.compute/images/write 」、「 microsoft.compute/images/read 」、	VHD から Cloud Volumes ONTAP を導入できます。
Microsoft.Compute/disks/delete" 、 Microsoft.Compute/disks/read" 、 Microsoft.Compute/disks/write" 、 "Microsoft.Storage/checknameavailability/read" 、 "Microsoft.Storage/operations/read" 、 "microsoft.StorageAccounts/listkeyss/action" 、 "microsoft.Storage/storageAccounts/read" 、 "microsoft.Storage/regenerateAccounts/action" 、 "Microsoft.Storage/storageAccounts/action" 、 "/writeStorageAccounts" 、 "/StorageAccounts/StorageAccounts/write/StorageAccounts" 、 ","Microsoft 。	Azure ストレージアカウントとディスクを管理し、ディスクを Cloud Volumes ONTAP に接続します。
「 microsoft.network/networkinterfaces/read 」、「 microsoft.network/networkinterfaces/write 」、「 microsoft.network/networkinterfaces/join/action 」、	ターゲットサブネット内の Cloud Volumes ONTAP のネットワークインターフェイスを作成および管理します。
「 microsoft.network/networksecuritygroups/read 」、「 microsoft.network/networksecuritygroups/write 」、「 microsoft.network/networksecuritygroups/join/action 」、	Cloud Volumes ONTAP 用の定義済みネットワークセキュリティグループを作成します。

アクション	目的
「 microsoft.Resources/Subscriptions /locations /read 」、「 Microsoft.Network/locations/operationResults/read" 」、「 Microsoft.Network/locations/operations/read" 」、「 Microsoft.Network/virtualNetworks/read" 」、「 Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read" 」、「 Microsoft.Network/virtualNetworks/subnets/read" 」、「 Microsoft.Network/virtualNetworks/subnets/virtualMachines/read" 」、「 Microsoft.Network/virtualNetworks/virtualMachines/read" 」、「 Microsoft.Network/virtualNetworks/subnets/join/action" 」、	リージョン、ターゲット VNet 、およびサブネットに関するネットワーク情報を取得し、 vnet に Cloud Volumes ONTAP を追加します。
「 Microsoft.Network/virtualNetworks/subnets/write" 」、 Microsoft.Network/routeTables/join/action" 、	データ階層化のための VNet サービスエンドポイントを有効にします。
「 Microsoft.Resources/Deployments/Operations/Read 」、「 Microsoft.Resources/Deployments/Read 」、「 Microsoft.Resources/Deployments/Write 」、	テンプレートから Cloud Volumes ONTAP を導入します。
"microsoft.Resources/Deployments/operations/read" 、 "microsoft.Resources/Deployments/read" 、 "microsoft.Resources/resources/read" 、 "microsoft.resources/resources/operationresults/read" 、 "microsoft.resources/Subscriptions /resourceGroups/delete" 、 "microsoft.resources/Subscriptions /resources/groups/resources/resources/reads/resources/resources/resources/resources/resources/resources/resources/reading" 、 ",",",","resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/resources/groups/	Cloud Volumes ONTAP のリソースグループを作成および管理します。
「 microsoft.compute/snapshots/write 」、「 microsoft.compute/snapshots/read 」、「 microsoft.compute/disks/beginingAccess/action 」	Azure マネージドスナップショットを作成および管理します。
"microsoft.compute/availabilitySets/write", "microsoft.compute/availabilitySets/read",	Cloud Volumes ONTAP の可用性セットを作成および管理します。
"Microsoft.MarketplaceOrdering/Offered Types/publishers/capers/plans/agreements/read" 、 "Microsoft.MarketplaceOrdering / offerTypes/publishers/capes/plans/agreements/write"	Azure Marketplace からのプログラムによる展開を可能にします。

アクション	目的
「 Microsoft.Network/loadBalancers/read" 」、「 Microsoft.Network/loadBalancers/write" 」、「 Microsoft.Network/loadBalancers/delete" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/read" 」、「 Microsoft.Network/loadBalancers/backendAddressPools/join/action" 」、「 Microsoft.Network/loadBalancers/frontendIPConfigurations/read" 」、「 Microsoft.Network/loadBalancers/loadBalancingRules/read" 」、「 Microsoft.Network/loadBalancers/probes/read" 」、「 Microsoft.Network/loadBalancers/probes/join/action" 」	HA ペアの Azure ロードバランサを管理します。
"Microsoft 許可 / ロック /*"	Azure ディスクのロックの管理を有効にします。
"Microsoft.Authorization/roleDefinites/write" 、 "Microsoft.Authorization/rolrolわり あて /write" 、 "Microsoft.Web/sites/*"	HA ペアのフェイルオーバーを管理します。

Cloud Manager が GCP 権限を使用して実行する処理

GCP の Cloud Manager ポリシーには、 Cloud Volumes ONTAP の導入と管理に Cloud Manager が必要とする権限が含まれています。

アクション	目的
-compute.disks .create -computedisks .createsnapshot - compute.disks.delete -computedisks .get-compute.diskList - compute.disks.setLabels - compute.disks.us	Cloud Volumes ONTAP 用のディスクを作成および管理します。
-compute-firewalls .create - compute.firewalls.delete -comput領域 .firewalls .get-comput領域 .firewalls リスト	Cloud Volumes ONTAP のファイアウォールルールを作成します。
-computer.globalOperationsGet	処理のステータスを確認できます。
-compute.image.get-compute.image.getFromFamily -compute.image.list - compute.images.useReadOnly	VM インスタンスのイメージを取得します。
- compute.instances.attachDisk - compute.instances.detachDisk	ディスクを Cloud Volumes ONTAP に接続して接続解除します。
- compute.instances.create - compute.instances.delete	Cloud Volumes ONTAP VM インスタンスを作成および削除します。
- compute.instances.get	VM インスタンスを一覧表示します。
- compute.instances.getSerialPortOutput	をクリックしてコンソールログを取得してください
- compute.instances.list	ゾーン内のインスタンスのリストを取得します。
- compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。
- compute.instances.setLabels	ラベルを追加します。

アクション	目的
- compute.instances.setMachineType	Cloud Volumes ONTAP のマシンタイプを変更します。
- compute.instances.setMetadata	をクリックしてください。
- compute.instances.setTags	ファイアウォールルールのタグを追加します。
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Cloud Volumes ONTAP を開始および停止します。
-computesCompute .machineTypes.get	コア数を取得して qoutas をチェックしてください。
- compute.projects.get	複数のプロジェクトをサポートするため。
-compute-snapshots-create - compute.snapshots.delete -compute-snapshots -getCompute-snapshots-list - compute.snapshots.setLabels	永続ディスクスナップショットを作成および管理するには、次の手順に従います。
- compute.networks.get - compute.networks.list - comput.regions.Get-comput領域 .list-comput領域 .subnetworks -compute.subnetworks .listCompute.zoneOperations-get-compute.zones .get-compute.zones リスト	新しい Cloud Volumes ONTAP 仮想マシンインスタンスの作成に必要なネットワーク情報を取得するため。
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list -deploymentmanager. マニフェスト .get-deploymentmanager. マニフェスト .list-list-deploymentmanager. operations-get-deploymentmanager. operationlist -deploymentmanager. resources.get-deploymentmanager. resources.list-deploymentmanager. typeProviders.get-deploymentmanager. typeProviders.list-deploymentmanager. -deploymentmanager. types] リスト	Google Cloud Deployment Manager を使用して Cloud Volumes ONTAP 仮想マシンインスタンスを導入します。
-logging.logEntries.list-logging.privateLogEntries.list	スタックログドライブを取得する方法
- resourcemanager.projects.get	複数のプロジェクトをサポートするため。
-storagバケット 。 create - storage.buckets.delete -storage-buckets-get-storage-buckets-list	Google Cloud Storage バケットを作成して管理し、データを階層化します。
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms .cryptoKeys.get-cloudkms .cryptoKeys.list-cloudkm.keyringlist.list	Cloud Volumes ONTAP でクラウドキー管理サービスからお客様が管理する暗号化キーを使用するため。

デフォルト設定

Cloud Manager と Cloud Volumes ONTAP のデフォルト設定方法の詳細は、システムの

管理に役立ちます。

Linux での Cloud Manager のデフォルト設定

Cloud Manager または Linux ホストのトラブルシューティングを行う必要がある場合は、 Cloud Manager の設定方法を理解することができます。

- NetApp Cloud Central （またはクラウドプロバイダのマーケットプレイスから直接）から Cloud Manager を導入した場合は、次の点に注意してください。
  - AWS では、 EC2 Linux インスタンスのユーザ名は EC2-user です。
  - Cloud Manager イメージのオペレーティングシステムは、 Red Hat Enterprise Linux 7.4 （ HVM ）です。

    オペレーティングシステムには GUI は含まれていません。システムにアクセスするには、端末を使用する必要があります。
- Cloud Manager のインストールフォルダは、次の場所にあります。

  /opt/application/netapp/cloudmanager です
- ログファイルは次のフォルダに格納されます。

  /opt/application/netapp/cloudmanager/log を選択します
- Cloud Manager サービスの名前は occm です。
- OCCM サービスは MySQL サービスに依存します。

  MySQL サービスがダウンしている場合は、 OCCM サービスもダウンしています。
- 次のパッケージがまだインストールされていない場合は、 Cloud Manager によって Linux ホストにインストールされます。
  - 7 郵便番号
  - AWSCLI
  - Java
  - Kubectl のように入力する
  - MySQL
  - Tridentctl
  - 取得

Cloud Volumes ONTAP のデフォルト設定

Cloud Volumes ONTAP がデフォルトでどのように設定されているかを理解すると、システムのセットアップと管理に役立ちます。特に、 ONTAP に精通している場合は、 Cloud Volumes ONTAP のデフォルト設定は ONTAP とは異なるためです。

- Cloud Volumes ONTAP は、 AWS 、 Azure 、 GCP ではシングルノードシステムとして、 AWS と Azure では HA ペアとして利用できます。

- Cloud Manager は、 Cloud Volumes ONTAP の導入時に 1 つのデータサービス SVM を作成します。複数のデータを提供する SVM の使用はサポートされていません。
- Cloud Manager は、次の ONTAP 機能ライセンスを Cloud Volumes ONTAP に自動的にインストールします。
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - NetApp Volume Encryption （ライセンス使用システムまたは登録従量課金制システムの場合のみ）
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- デフォルトでは、いくつかのネットワークインターフェイスが作成されます。
  - クラスタ管理 LIF
  - クラスタ間 LIF
  - Azure の HA システム、 AWS のシングルノードシステム、および複数の AWS アベイラビリティゾーンの HA システム上の SVM 管理 LIF の 1 つ
  - ノード管理 LIF
  - iSCSI データ LIF
  - CIFS および NFS データ LIF

> EC2 の要件により、 Cloud Volumes ONTAP の LIF フェイルオーバーはデフォルトで無効になっています。LIF を別のポートに移行すると、インスタンス上の IP アドレスとネットワークインターフェイス間の外部マッピングが解除され、 LIF にアクセスできなくなります。

- Cloud Volumes ONTAP は、 HTTPS を使用して設定バックアップを Cloud Manager に送信します。

  Cloud Manager にログインすると、からバックアップにアクセスできます https://ipaddress/occm/offboxconfig/

- Cloud Manager は、他の管理ツール（ System Manager や CLI など）とは異なるボリューム属性をいくつか設定します。

  次の表に、 Cloud Manager がデフォルトとは異なる設定にしたボリューム属性を示します。

属性	**Cloud Manager** によって設定される値
オートサイズモード	成長

属性	**Cloud Manager** によって設定される値
最大オートサイズ	1,000 パーセント アカウント管理者は、 [設定] ページからこの値を変更できます。
セキュリティ形式	CIFS ボリューム UNIX の場合は NTFS 、 NFS ボリュームの場合は NTFS
スペースギャランティスタイル	なし
UNIX 権限（ NFS のみ）	777

これらの属性の詳細については、 _volume create のマニュアルページを参照してください。

Cloud Volumes ONTAP のブートデータとルートデータ

Cloud Manager は、ユーザデータ用のストレージに加えて、各 Cloud Volumes ONTAP システムのブートデータとルートデータ用のクラウドストレージも購入します。

AWS

- 汎用 SSD ディスク × 2 ：
  - ルートデータ用に 140GB ディスク × 1 （ノードごとに 1 つ）
  - 9.6 以降：ブートデータ用に 86 GB のディスクが 1 つ（ノードごとに 1 つ）
  - 9.5 以前：ブートデータ用に 45GB のディスク 1 本（ノードごとに 1 本）
- ブートディスクとルートディスクごとに 1 つの EBS スナップショット
- HA ペアの場合は、メディエーターインスタンス用の EBS ボリュームが 1 つで、約 8GB です

Azure （シングルノード）

- Premium SSD ディスク × 2 ：
  - ブートデータ用に 90 GB のディスクを 1 台
  - ルートデータ用に 140GB のディスクが 1 つ
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot

Azure （ HA ペア）

- ブートボリューム用に 90GB の Premium SSD ディスクを 2 本（各ノードに 1 本）
- ルート用の 140 GB Premium Storage ページブロブ 2 つ ボリューム（ノードごとに 1 つ）
- コアを節約するために 128 GB の標準 HDD ディスク 2 台 （ノードごとに 1 つ）
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot

GCP

- 起動データ用に 10 GB 標準永続ディスクを 1 台
- ルートデータ用に 64 GB の標準パーシステントディスクを 1 台
- NVRAM 用に 500GB の標準永続的ディスクを 1 本
- コアを節約するための 216 GB 標準永続ディスク 1 台
- 各 GCP スナップショット（起動ディスクとルート用） ディスク

ディスクが存在する場所

Cloud Manager は次のようにストレージを配置します。

- ブートデータは、インスタンスまたは仮想マシンに接続されたディスクにあります。

  このディスクにはブートイメージが含まれており、 Cloud Volumes ONTAP では使用できません。

- システム構成とログを含むルートデータは、 aggr0 にあります。
- Storage Virtual Machine （ SVM ）ルートボリュームは aggr1 にあります。
- データボリュームも aggr1 にあります。

暗号化

ブートディスクとルートディスクは、これらのクラウドプロバイダではデフォルトで暗号化が有効になるため、 Azure と Google Cloud Platform では常に暗号化されます。

キー管理サービス（ KMS ）を使用して AWS でデータ暗号化を有効にすると、 Cloud Volumes ONTAP のブートディスクとルートディスクも暗号化されます。これには、 HA ペアのメディエーターインスタンスのブートディスクが含まれます。ディスクは、作業環境の作成時に選択した CMK を使用して暗号化されます。

ロール

アカウント管理者ロールとワークスペース管理者ロールは、ユーザーに特定の権限を提供します。

タスク	アカウント管理者	ワークスペース管理者
作業環境の管理	はい。	はい、関連付けられたワークスペースの場合
データ複製ステータスを表示します	はい。	はい、関連付けられたワークスペースの場合
タイムラインを表示します	はい。	はい、関連付けられたワークスペースの場合
作業環境を削除します	はい。	いいえ
Kubernetes クラスタを Cloud Volumes ONTAP に接続	はい。	いいえ

タスク	アカウント管理者	ワークスペース管理者
Cloud Volumes ONTAP レポートを受信します	はい。	いいえ
Cloud Central アカウントを管理します	はい。	いいえ
クラウドプロバイダのアカウントを管理	はい。	いいえ
Cloud Manager の設定を変更	はい。	いいえ
サポートダッシュボードを表示および管理します	はい。	いいえ
Cloud Manager から作業環境を削除します	はい。	いいえ
Cloud Manager を更新します	はい。	いいえ
HTTPS 証明書をインストールします	はい。	いいえ
Active Directory をセットアップします	はい。	いいえ

関連リンク

- "Cloud Central アカウントでのワークスペースとユーザのセットアップ"
- "Cloud Central アカウントでのワークスペースとユーザの管理"

ヘルプを参照したり、詳細情報を参照したりするには

Cloud Manager と Cloud Volumes ONTAP の詳細については、ビデオ、フォーラム、サポートなどのさまざまなリソースを参照してください。

- "Cloud Manager と Cloud Volumes ONTAP のビデオ"

  Cloud Volumes ONTAP の導入と管理の方法、ハイブリッドクラウド全体でデータをレプリケートする方法を紹介したビデオをご覧ください。

- "Cloud Manager のポリシー"

  Cloud Manager がクラウドプロバイダ内でアクションを実行するために必要な権限を含む JSON ファイルをダウンロードします。

- "Cloud Manager API 開発者ガイド"

  API の概要、使用方法の例、 API リファレンスを紹介します。

- Cloud Volumes ONTAP のトレーニング
  - "Cloud Volumes ONTAP の基礎"
  - "Azure 向け Cloud Volumes ONTAP の導入と管理"

- "AWS 向けの Cloud Volumes ONTAP の導入と管理"

- テクニカルレポート
  - "NetApp テクニカルレポート 4383 ：アプリケーションワークロードを使用した Amazon Web Services における Cloud Volumes ONTAP のパフォーマンス特性"
  - "NetApp テクニカルレポート 4671 ：アプリケーションワークロードを使用した Azure における Cloud Volumes ONTAP のパフォーマンス特性評価"

- SVM ディザスタリカバリ

  SVM ディザスタリカバリは、ソース SVM からデスティネーション SVM への SVM のデータと設定の非同期ミラーリングです。ソース SVM が使用できなくなった場合は、デスティネーション SVM をデータアクセス用に簡単にアクティブ化できます。

  - "『 Cloud Volumes ONTAP 9SVM Disaster Recovery Preparation Express Guide 』を参照してください"

    ディザスタリカバリに備えて、デスティネーション SVM を迅速に設定する方法について説明します。

  - "『 Cloud Volumes ONTAP 9SVM Disaster Recovery Express Guide 』を参照してください"

    災害発生後にデスティネーション SVM を迅速にアクティブ化し、ソース SVM を再アクティブ化する方法について説明します。

- "『 FlexCache Volumes for Faster Data Access Power Guide 』を参照してください"

  データ access.es を高速化するために、データを高速化するために元のボリュームと同じクラスタまたは別のクラスタに FlexCache ボリュームを作成および管理する方法について説明します。災害発生後にデスティネーション SVM をアクティブ化し、ソース SVM を再アクティブ化する簡単な方法について説明します。

- "セキュリティアドバイザリ"

  ONTAP を含むネットアップ製品の既知の脆弱性（ CSE ）を特定するCloud Volumes ONTAP のセキュリティの脆弱性は、 ONTAP のドキュメントに従って修正できます。

- "ONTAP 9 ドキュメンテーション・センター"

  Cloud Volumes ONTAP の使用に役立つ ONTAP の製品マニュアルにアクセスしてください。

- "NetApp Cloud Volumes ONTAP のサポート"

  サポートリソースにアクセスして、 Cloud Volumes ONTAP に関するヘルプやトラブルシューティングを参照してください。

- "ネットアップコミュニティ：クラウドデータサービス"

  同僚とつながり、質問をしたり、アイデアを交換したり、リソースを見つけたり、ベストプラクティスを共有したりします。

- "NetApp Cloud Central"

クラウド向けのその他のネットアップ製品とソリューションに関する情報をご覧ください。

- "ネットアップの製品マニュアル"

  手順、リソース、回答については、ネットアップの製品マニュアルを参照してください。

それよりも前のバージョンの Cloud Manager のドキュメント

Cloud Manager の以前のリリースのドキュメントは、最新バージョンを実行していない場合に利用できます。

"Cloud Manager 3.6"

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

http://www.netapp.com/us/legal/copyright.aspx

商標

NetApp 、 NetApp のロゴ、および NetApp の商標ページに記載されているマークは、 NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

http://www.netapp.com/us/legal/netapptmlist.aspx

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

https://www.netapp.com/us/media/patents-page.pdf

プライバシーポリシー

https://www.netapp.com/us/legal/privacypolicy/index.aspx

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

- "Cloud Manager 3.7.4 の通知です"
- "Cloud Manager 3.7.1 の通知です"
- "Cloud Manager 3.7 に関する注意事項"
- "Cloud Backup Service の注意事項を参照してください"