Cloud Volumes ONTAP のドキュメント

Cloud Volumes ONTAP

NetApp
June 27, 2024

目次

Cloud Volumes ONTAP のドキュメント

リリースノート

新機能

BlueXPのCloud Volumes ONTAP Managementの新機能をご紹介します。

このページで説明Cloud Volumes ONTAP する機能拡張は'BlueXPの機能に固有のものであり'BlueXPの管理を可能にしますCloud Volumes ONTAP ソフトウェア自体の新機能については、 "Cloud Volumes ONTAP のリリースノートに移動します"

2023年9月10日

コネクタの3.9.33リリースでは、次の変更が導入されました。

Azureでの**Lsv3**シリーズ**VM**のサポート

AzureのCloud Volumes ONTAPでは、9.13.1リリース以降で、単一のアベイラビリティゾーンと複数のアベイラビリティゾーンに管理対象ディスクを共有するシングルノード環境とハイアベイラビリティペア環境で、L48s_v3とL64s_v3のインスタンスタイプがサポートされるようになりました。これらのインスタンスタイプでは、Flash Cacheがサポートされます。

"AzureでサポートされるCloud Volumes ONTAP構成を確認する"
"AzureでのCloud Volumes ONTAPのストレージ制限を表示"

2023年7月30日

コネクタの3.9.32リリースでは、次の変更が導入されました。

Google Cloudで**Flash Cache**と高速書き込み速度をサポート

Google Cloud for Cloud Volumes ONTAP 9.13.1以降では、Flash Cacheと高速書き込み速度を個別に有効にすることができます。高速の書き込み速度は、サポートされているすべてのインスタンスタイプで使用できます。Flash Cacheは、次のインスタンスタイプでサポートされています。

- N2-STANDARD-16
- N2-STANDARD-32
- N2-STANDARD-48
- N2-STANDARD-64

これらの機能は、シングルノード環境とハイアベイラビリティペア環境の両方で個別に使用することも、一緒に使用することもできます。

"Google CloudでCloud Volumes ONTAP を起動します"

使用状況レポートの機能拡張

使用状況レポートに表示される情報に対するさまざまな改善が利用可能になりました。使用状況レポートの機能拡張は次のとおりです。

- TiB単位が列名に追加されました。
- シリアル番号の新しい「ノード」フィールドが追加されました。
- [Storage VMs]使用状況レポートに新しい[Workload Type]列が追加されました。
- 作業環境の名前がStorage VMとボリュームの使用状況レポートに表示されるようになりました。
- ボリュームタイプ「file」のラベルが「Primary（Read/Write）」に変更されました。
- ボリュームタイプ「secondary」のラベルが「Secondary（DP）」に変更されました。

使用状況レポートの詳細については、を参照してください。 "使用状況レポートをダウンロードします"。

2023年7月26日

コネクタの3.9.31リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.13.1 GA

BlueXPで、AWS、Azure、Google CloudにCloud Volumes ONTAP 9.13.1 General Availabilityリリースを導入、管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

2023年7月2日

コネクタの3.9.31リリースでは、次の変更が導入されました。

AzureでのHAマルチアベイラビリティゾーン環境のサポート

Azureの東日本および韓国中部では、Cloud Volumes ONTAP 9.12.1 GA以降でHAマルチアベイラビリティゾーンの導入がサポートされるようになりました。

複数のアベイラビリティゾーンをサポートするすべてのリージョンのリストについては、を参照してください "Azureのグローバルリージョンマップ"。

自律型ランサムウェア対策のサポート

Cloud Volumes ONTAPでAutonomous Ransomware Protection（ARP）がサポートされるようになりました。ARPサポートは、Cloud Volumes ONTAPバージョン9.12.1以降で使用できます。

Cloud Volumes ONTAPを使用したARPの詳細については、を参照してください "自律的なランサムウェア防御"。

2023年6月26日

コネクタの3.9.30リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.13.1 RC1

BlueXPで、AWS、Azure、Google CloudにCloud Volumes ONTAP 9.13.1を導入、管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

2023年6月4日

コネクタの3.9.30リリースでは、次の変更が加えられました。

Cloud Volumes ONTAPアップグレードバージョンセレクタの更新

Upgrade Cloud Volumes ONTAPページで、Cloud Volumes ONTAPの最新バージョンまたは古いバージョンへのアップグレードを選択できるようになりました。

BlueXPを使用したCloud Volumes ONTAPのアップグレードの詳細については、を参照してください "Cloud Volumes ONTAP をアップグレードします"。

2023年5月7日

コネクタの3.9.29リリースでは、次の変更が加えられました。

カタール地域が**Google Cloud**でサポートされるようになりました

カタール地域は、Google Cloud for Cloud Volumes ONTAP およびConnector for Cloud Volumes ONTAP 9.12.1 GA以降でサポートされるようになりました。

Sweden Centralリージョンが**Azure**でサポートされるようになりました

Sweden Centralリージョンは、Azure for Cloud Volumes ONTAP およびConnector for Cloud Volumes ONTAP 9.12.1 GA以降でサポートされるようになりました。

Azure Australia Eastでの**HA**複数アベイラビリティゾーンの導入のサポート

Azureのオーストラリア東部リージョンでは、Cloud Volumes ONTAP 9.12.1 GA以降でHAマルチアベイラビリティゾーンの導入がサポートされるようになりました。

充電使用量の内訳

容量ベースのライセンスにサブスクライブしたときに課金される料金を確認できるようになりました。次のタイプの使用状況レポートは、BlueXPのデジタルウォレットからダウンロードできます。使用状況レポートには、サブスクリプションの容量の詳細と、Cloud Volumes ONTAP サブスクリプションのリソースに対する課金状況が表示されます。ダウンロード可能なレポートは、他のユーザーと簡単に共有できます。

- Cloud Volumes ONTAP パッケージの使用状況
- 使用状況の概要
- Storage VMの使用状況
- ボリュームの使用状況

詳細については、を参照してください "容量ベースのライセンスを管理します"。

Marketplaceのサブスクリプションなしで**BlueXP**にアクセスすると通知が表示されるようになりました

Marketplaceのサブスクリプションを購入せずにBlueXPでCloud Volumes ONTAP にアクセスすると、必ず通

知が表示されるようになりました。通知には、「この作業環境のマーケットプレイスサブスクリプションは、Cloud Volumes ONTAP の利用規約に準拠する必要があります」と記載されています。

2023年4月4日

Cloud Volumes ONTAP 9.12.1 GA以降では、次のように中国リージョンがAWSでサポートされるようになりました。

- シングルノードシステムがサポートされます。
- ネットアップから直接購入したライセンスはサポートされます。

地域ごとの可用性については、を参照してください "Cloud Volumes ONTAP のグローバルリージョンマップ"。

2023年4月3日

コネクタの3.9.28リリースでは、次の変更が導入されました。

Turinリージョンが**Google Cloud**でサポートされるようになりました

Turinリージョンは、Google Cloud for Cloud Volumes ONTAP およびConnector for Cloud Volumes ONTAP 9.12.1 GA以降でサポートされるようになりました。

BlueXPのデジタルウォレット機能の強化

BlueXPのデジタルウォレットに、Marketplaceのプライベートオファーで購入したライセンス容量が表示されるようになりました。

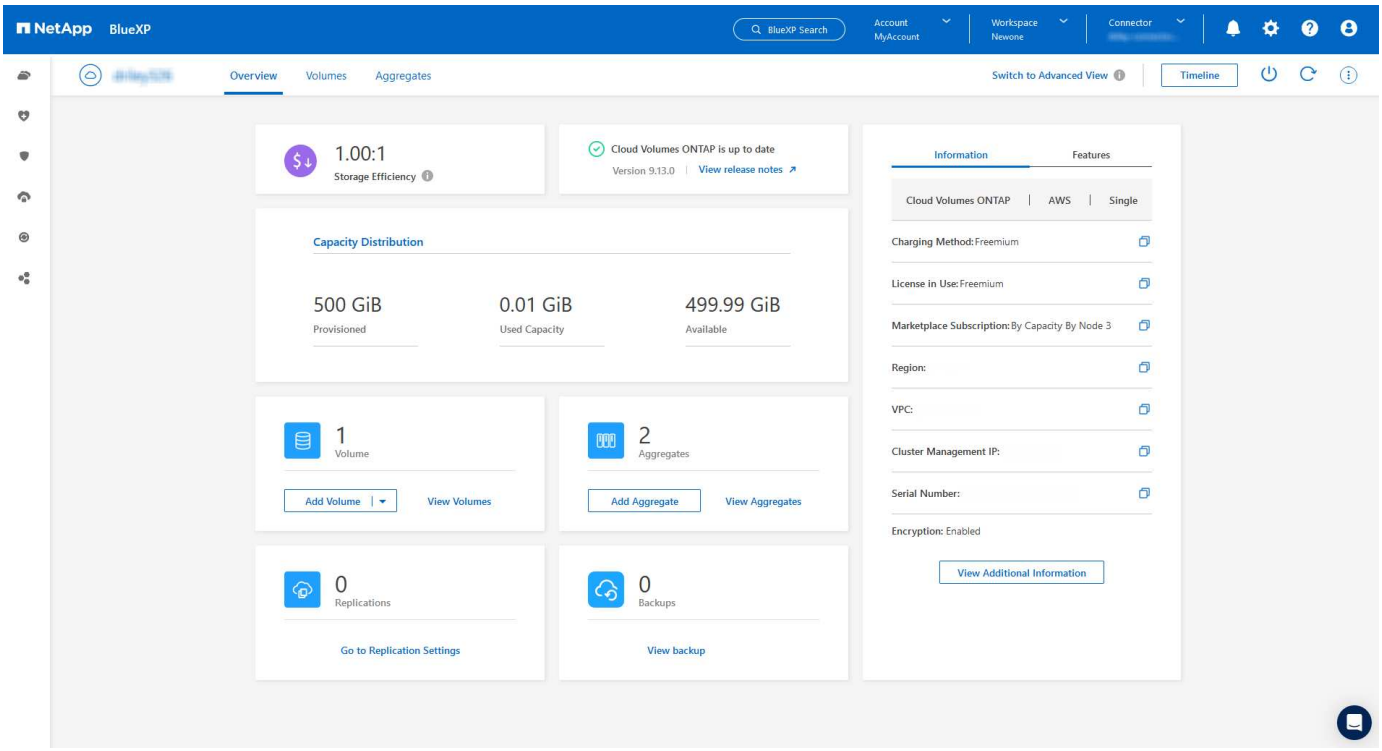
"アカウントの使用済み容量を表示する方法について説明します"。

ボリューム作成時のコメントがサポートされます

このリリースでは、APIを使用してCloud Volumes ONTAP FlexGroup ボリュームまたはFlexVol ボリュームを作成する際にコメントを作成することができます。

Cloud Volumes ONTAP の**[Overview]**、**[Volumes]**、**[Aggregates]**ページで**BlueXP**のユーザインターフェイスが再設計されました

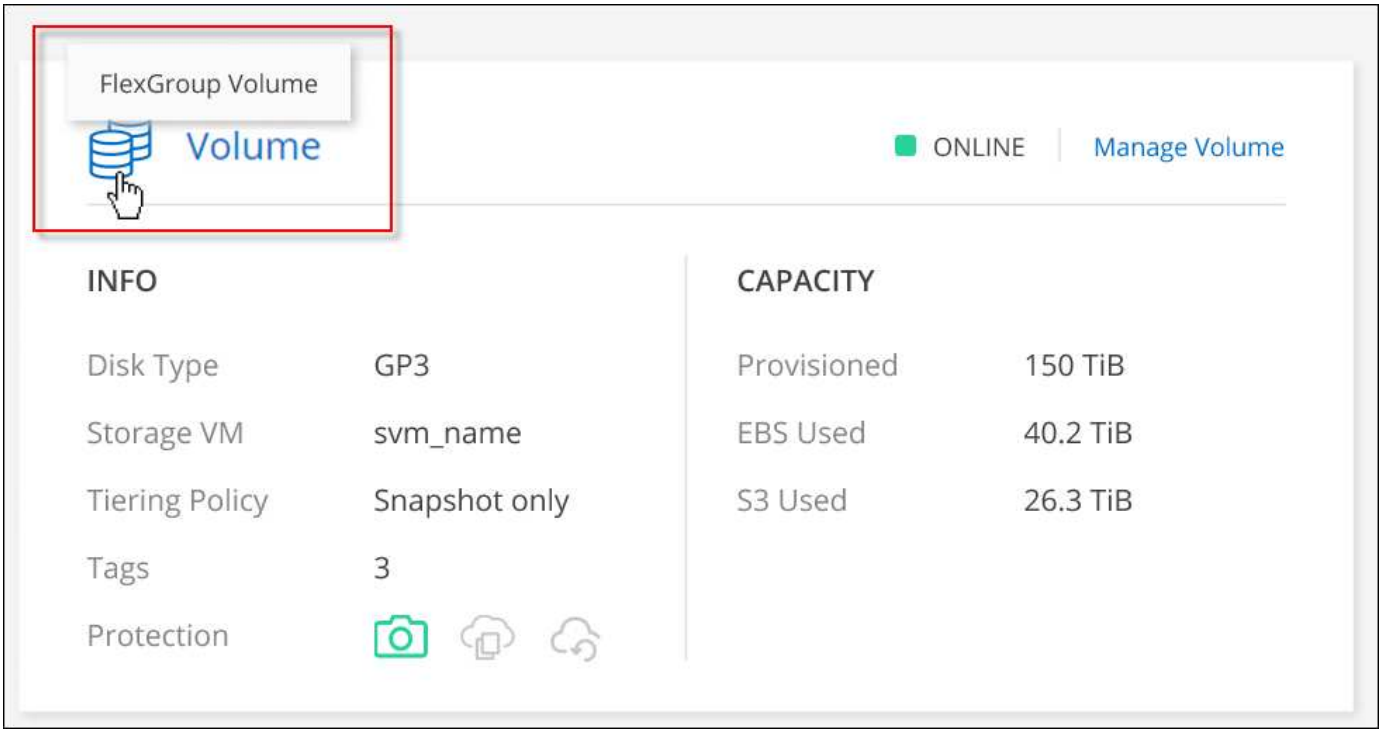
Cloud Volumes ONTAP の[概要]、[ボリューム]、[アグリゲート]ページで使用できるユーザインターフェイスが再設計されました。タイルベースのデザインでは、より包括的な情報が各タイルに表示され、ユーザーエクスペリエンスが向上します。



FlexGroup ボリュームは**Cloud Volumes ONTAP** で確認できます

CLIまたはSystem Managerで作成したFlexGroup ボリュームは、BlueXPの再設計された[ボリューム]タイルで直接表示できるようになりました。FlexVol ボリュームの場合と同じように、作成したFlexGroup ボリュームの詳細情報は専用の[Volumes]タイルで確認できます。

現時点では、BlueXPでは既存のFlexGroup ボリュームのみを表示できます。BlueXPでFlexGroup ボリュームを作成することはできませんが、今後のリリースでサポートする予定です。



タイルの下にFlexGroup ボリュームアイコンが配置されたテキストを示すスクリーンショット。"]

"作成したFlexGroup ボリュームの表示について詳しくは、こちらをご覧ください。"

2023年3月13日

中国地域のサポート

Cloud Volumes ONTAP 9.12.1 GA以降では、次のように中国リージョンのサポートがAzureでサポートされるようになりました。

- Cloud Volumes ONTAP は中国北部3でサポートされています。
- シングルノードシステムがサポートされます。
- ネットアップから直接購入したライセンスはサポートされます。

地域ごとの可用性については、を参照してください "Cloud Volumes ONTAP のグローバルリージョンマップ"。

2023年3月5日

コネクタの3.9.27リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.13.0

BlueXPで、AWS、Azure、Google CloudにCloud Volumes ONTAP 9.13.0を導入、管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

Azureで**16TiB**と**32TiB**をサポート

Cloud Volumes ONTAP では、Azureのマネージドディスクで実行される高可用性環境向けに、16TiBと32TiBのディスクサイズがサポートされるようになりました。

の詳細を確認してください "Azureでサポートされるディスクサイズ"。

MTEKMライセンス

バージョン9.12.1 GA以降を実行する新規および既存のCloud Volumes ONTAP システムに、マルチテナント暗号化キー管理（MTEKM）ライセンスが含まれるようになりました。

マルチテナントの外部キー管理を使用すると、NetApp Volume Encryptionの使用時に、個々のStorage VM（SVM）でKMIPサーバを介して独自のキーを保持できます。

"ネットアップの暗号化ソリューションでボリュームを暗号化する方法について説明します"。

インターネットを使用しない環境のサポート

インターネットから完全に分離されたすべてのクラウド環境でCloud Volumes ONTAP がサポートされるようになりました。これらの環境では、ノードベースのライセンス（BYOL）のみがサポートされます。容量単位のライセンスはサポートされていません。開始するには、コネクタソフトウェアを手動でインストールし、コ

ネクタで実行されているBlueXPコンソールにログインし、BlueXPデジタルウォレットにBYOLライセンスを追加してから、Cloud Volumes ONTAP を導入します。

- "インターネットにアクセスできない場所にコネクタを取り付けます"
- "コネクタのBlueXPコンソールにアクセスします"
- "未割り当てライセンスを追加します"

Google Cloudでの**Flash Cache**と高速書き込み

Cloud Volumes ONTAP 9.13.0リリースでは、Flash Cache、高速な書き込み速度、最大転送単位（MTU）8、896バイトがサポートされるようになりました。

の詳細を確認してください "Google Cloudのライセンスごとにサポートされる構成"。

2023年2月5日

コネクタの3.9.26リリースでは、次の変更が導入されました。

AWSでの配置グループの作成

AWS HA単一アベイラビリティゾーン（AZ）環境で配置グループを作成するための新しい設定が追加されました。失敗した配置グループの作成をバイパスして、AWS HA単一のAZ環境を正常に完了できるようにすることができます。

配置グループの作成設定の詳細については、を参照してください "AWS HA単一AZ用の配置グループの作成を設定する"。

プライベート**DNS**ゾーン設定の更新

Azureプライベートリンクの使用時にプライベートDNSゾーンと仮想ネットワークの間にリンクを作成しないように、新しい設定が追加されました。作成はデフォルトで有効になっています。

"AzureプライベートDNSの詳細をBlueXPに提供します"

WORMストレージとデータ階層化

Cloud Volumes ONTAP 9.8以降のシステムを作成するときに、データ階層化とWORMストレージの両方を有効にできるようになりました。WORMストレージによるデータ階層化を有効にすると、データをクラウドのオブジェクトストアに階層化できます。

"WORMストレージについて説明します。"

2023年1月1日

コネクタの3.9.25リリースでは、次の変更が導入されました。

Google Cloudで提供されているライセンスパッケージ

最適化さCloud Volumes ONTAP れた容量ベースのライセンスパッケージとエッジキャッシュ容量ベースのライセンスパッケージは、Google Cloud Marketplaceで従量課金制サービスまたは年間契約として提供されます。

を参照してください "Cloud Volumes ONTAP ライセンス"。

Cloud Volumes ONTAP のデフォルト設定

マルチテナント暗号化キー管理（MTEKM）ライセンスは新しいCloud Volumes ONTAP 環境には含まれなくなりました。

Cloud Volumes ONTAP とともに自動的にインストールされるONTAP 機能ライセンスの詳細については、を参照してください "Cloud Volumes ONTAP のデフォルト設定"。

2022年12月15日

Cloud Volumes ONTAP 9.12.0

BlueXPでは、AWSとGoogle CloudにCloud Volumes ONTAP 9.12.0を導入して管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

2022年12月8日

Cloud Volumes ONTAP 9.12.1

BlueXPでは、Cloud Volumes ONTAP 9.12.1を導入および管理できるようになりました。新機能やその他のクラウドプロバイダリージョンのサポートが含まれます。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"

2022年12月4日

コネクタの3.9.24リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP の作成中に、Worm+ Cloud Backupを利用できるようになりました

Cloud Volumes ONTAP の作成プロセスで、Write Once、Read Many（WORM）、およびCloud Backupの両方の機能をアクティブ化できるようになりました。

イスラエルでGoogle Cloudがサポートされるようになりました

イスラエルのリージョンは、Google Cloud for Cloud Volumes ONTAP とConnector for Cloud Volumes ONTAP 9.11.1 P3以降でサポートされるようになりました。

2022年11月15日

コネクタの3.9.23リリースでは、次の変更が導入されました。

Google CloudのONTAP S3ライセンス

ONTAP Cloud Platformでバージョン9.12.1以降を実行する新規および既存のCloud Volumes ONTAP システムに、S3ライセンスが含まれるようになりました。

"ONTAP で S3 オブジェクトストレージサービスを設定および管理する方法について説明します"

2022年11月6日

コネクタの3.9.23リリースでは、次の変更が導入されました。

Azureでリソースグループを移動しています

同じAzureサブスクリプション内で、Azure内の1つのリソースグループから別のリソースグループに作業環境を移動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 "リソースグループを移動しています"。

NDMP-copy証明書

ONTAP VolumeでのNDMPコピーの使用が認定されました。

NDMPの設定方法および使用方法については、を参照してください "NDMP構成の概要"。

Azureのマネージドディスク暗号化機能をサポート

作成時にすべての管理対象ディスクを暗号化できる、新しいAzure権限が追加されました。

この新機能の詳細については、を参照してください "Azure でお客様が管理するキーを使用するように Cloud Volumes ONTAP を設定します"。

2022年9月18日

コネクタの3.9.22リリースでは、次の変更が導入されました。

デジタルウォレットの機能強化

- デジタルウォレットに、最適化されたI/Oライセンスパッケージと、アカウント全体でCloud Volumes ONTAP システム用にプロビジョニングされたWORM容量の概要が表示されます。

  これらの詳細情報は、充電状況や容量の追加購入が必要かどうかを把握するのに役立ちます。

  "アカウントの使用済み容量を表示する方法について説明します"。

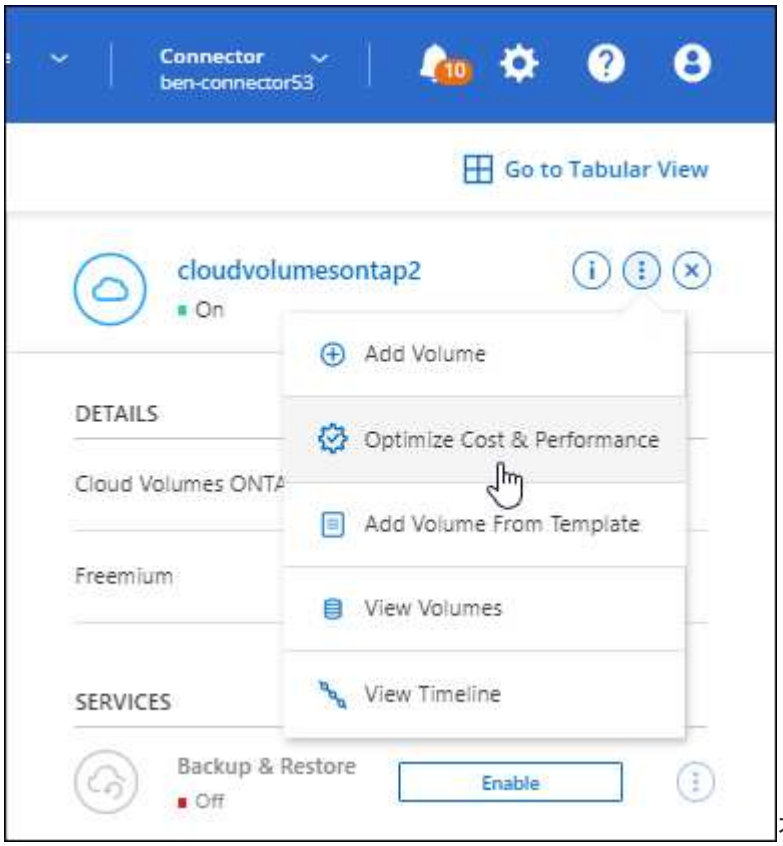
- 1つの充電方法から最適化された充電方法に変更できるようになりました。

  "充電方法を変更する方法について説明します"。

コストとパフォーマンスを最適化

Cloud Volumes ONTAP システムのコストとパフォーマンスをキャンバスから直接最適化できるようになりました。

作業環境を選択したら、コストとパフォーマンスの最適化*オプションを選択して、Cloud Volumes ONTAP のインスタンスタイプを変更できます。サイズの小さいインスタンスを選択するとコストを削減できますが、サイズの大きいインスタンスに変更することでパフォーマンスを最適化できます。



オプションのスクリーンショット。"]

AutoSupport 通知

Cloud Volumes ONTAP システムがAutoSupport メッセージを送信できない場合、BlueXPは通知を生成するようになりました。この通知には、ネットワークの問題のトラブルシューティングに使用できる手順へのリンクが記載されています。

2022年7月31日

コネクタの3.9.21リリースでは、次の変更が導入されました。

MTEKMライセンス

バージョン9.11.1以降を実行している新規および既存のCloud Volumes ONTAP システムに、Multi-tenant Encryption Key Management（MTEKM）ライセンスが追加されました。

マルチテナントの外部キー管理を使用すると、NetApp Volume Encryptionの使用時に、個々のStorage VM（SVM）でKMIPサーバを介して独自のキーを保持できます。

"ネットアップの暗号化ソリューションでボリュームを暗号化する方法について説明します"。

プロキシサーバ

Cloud Volumes ONTAP AutoSupport メッセージの送信にアウトバウンドのインターネット接続を使用できない場合、BlueXPでは、コネクタをプロキシサーバとして使用するようにシステムが自動的に設定されるようになりました。

AutoSupport は、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセー

ジを送信します。

唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

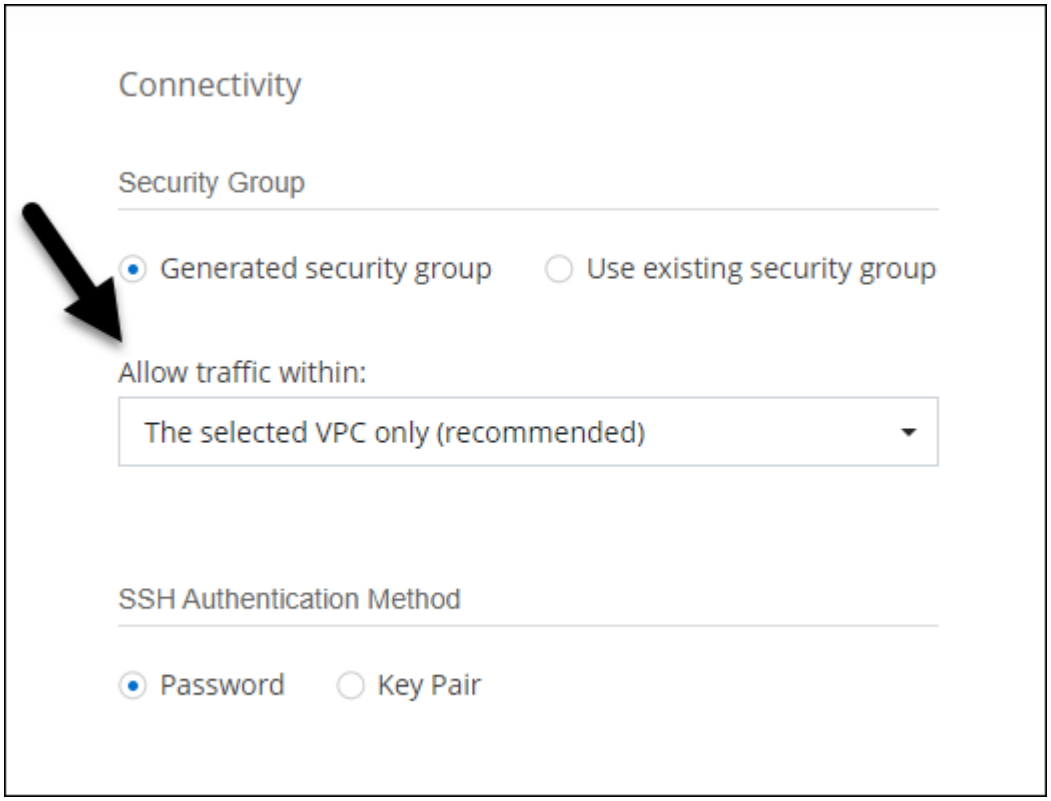
充電方法を変更します

容量ベースのライセンスを使用するCloud Volumes ONTAP システムの充電方法を変更できるようになりました。たとえば、Essentialsパッケージを含むCloud Volumes ONTAP システムを導入した場合、ビジネスニーズの変化に応じて、そのシステムをProfessionalパッケージに変更できます。この機能は、デジタルウォレットから使用できます。

"充電方法を変更する方法について説明します"。

セキュリティグループの機能拡張

Cloud Volumes ONTAP 作業環境を作成するときに、ユーザインターフェイスを使用して、事前定義されたセキュリティグループで選択したネットワークのみ（推奨）またはすべてのネットワーク内のトラフィックを許可するかどうかを選択できるようになりました。



2022年7月18日

Azureの新しいライセンスパッケージです

Azure Marketplaceサブスクリプションでのお支払い時に、Cloud Volumes ONTAP 用に2つの容量ベースのライセンスパッケージが新たに提供されます。

- 最適化：プロビジョニングされた容量とI/O処理に別々に課金します

- * Edge Cache*:のライセンス "Cloud Volume エッジキャッシュ"

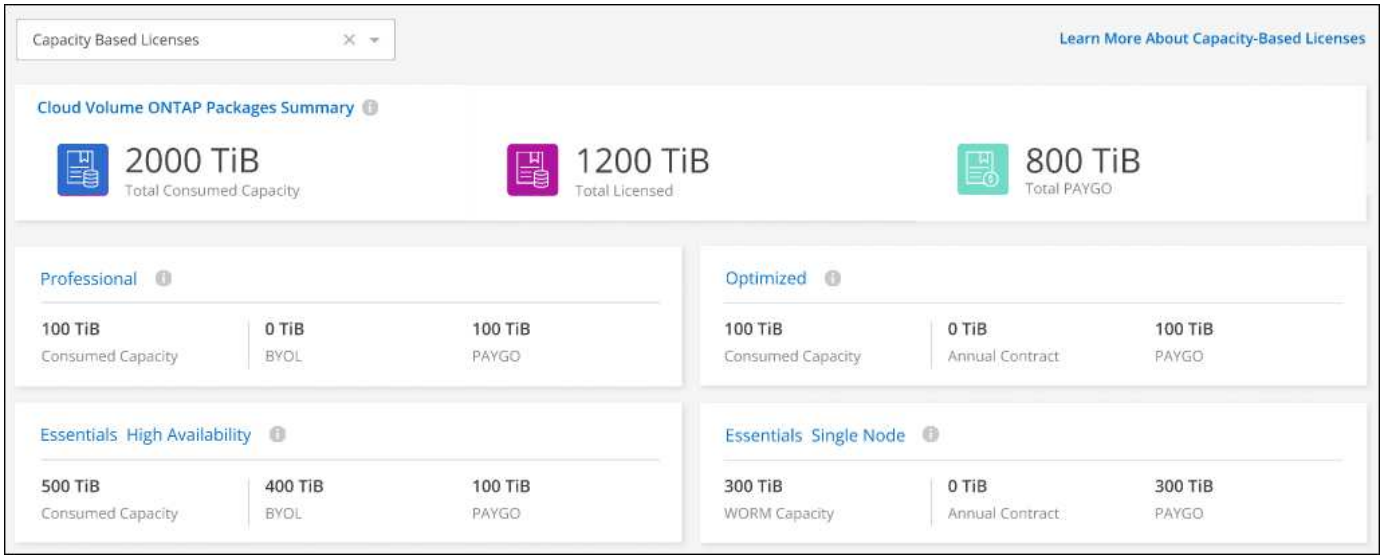
"これらのライセンスパッケージの詳細については、こちらをご覧ください"。

2022年7月3日

コネクタの3.9.20リリースでは、次の変更が導入されました。

デジタルウォレット

デジタルウォレットに、アカウントで消費された合計容量とライセンスパッケージで消費された容量が表示されるようになりました。この情報は、料金の支払い方法や、容量の追加購入が必要かどうかを把握するのに役立ちます。



Elastic Volumesの機能拡張

BlueXPでは、ユーザーインターフェイスからCloud Volumes ONTAP 作業環境を作成する際に、Amazon EBS Elastic Volumes機能がサポートされるようになりました。Elastic Volumes機能は、GP3またはio1ディスクを使用している場合、デフォルトで有効になっています。初期容量はストレージのニーズに基づいて選択し、Cloud Volumes ONTAP の導入後に変更することができます。

"Elastic VolumesのAWSサポートの詳細については、こちらをご覧ください"。

AWSの**ONTAP S3**ライセンス

AWSでバージョン9.11.0以降を実行している新規および既存のCloud Volumes ONTAP システムにONTAP S3ライセンスが追加されました。

"ONTAP で S3 オブジェクトストレージサービスを設定および管理する方法について説明します"

Azure Cloudリージョンが新たにサポートされます

9.10.1リリース以降、Azure West US 3リージョンでCloud Volumes ONTAP がサポートされるようになりました。

"Cloud Volumes ONTAP でサポートされるリージョンの完全なリストを表示します"

AzureのONTAP S3ライセンス

バージョン9.9.1以降を実行する新規および既存のCloud Volumes ONTAP システムにONTAP S3ライセンスが追加されました。

"ONTAP で S3 オブジェクトストレージサービスを設定および管理する方法について説明します"

2022年6月7日

コネクタの3.9.19リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.11.1

BlueXPでは、Cloud Volumes ONTAP 9.11.1の導入と管理ができるようになりました。これには、新機能のサポートとその他のクラウドプロバイダリージョンの追加が含まれています。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"

新しい詳細ビュー

Cloud Volumes ONTAP の高度な管理を行う必要がある場合は、ONTAP システムに付属の管理インターフェイスであるONTAP System Managerを使用します。BlueXPにはSystem Managerインターフェイスが搭載されているので、高度な管理のためにBlueXPを残す必要はありません。

この拡張ビューは、Cloud Volumes ONTAP 9.10.0以降でプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

"詳細については、「詳細ビュー」を参照してください"。

Amazon EBS Elastic Volumesのサポート

Cloud Volumes ONTAP アグリゲートでAmazon EBS Elastic Volumes機能がサポートされるため、パフォーマンスが向上し、容量が追加されます。また、必要に応じて基盤となるディスク容量が自動的に拡張されます。

Elastic Volumeは、Cloud Volumes ONTAP 9.11.0システム以降、GP3およびio1 EBSディスクタイプでサポートされます。

"Elastic Volumesのサポートに関する詳細情報"。

Elastic Volumesをサポートするために、Connectorに対する新しいAWS権限が必要になることに注意してください。

```
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
```

BlueXPに追加したAWSクレデンシャルの各セットに、これらの権限を必ず付与してください。 "AWSの最新のコネクタポリシーを確認します"。

共有AWSサブネットでのHAペアの導入をサポートします

Cloud Volumes ONTAP 9.11.1では、AWS VPC共有がサポートされています。このリリースのコネクタでは、APIを使用するときにAWS共有サブネットにHAペアを導入できます。

"共有サブネットにHAペアを導入する方法について説明します"。

サービスエンドポイントを使用する場合は、ネットワークアクセスが制限されます

Cloud Volumes ONTAP とストレージアカウント間の接続にVNetサービスエンドポイントを使用する場合に、ネットワークアクセスが制限されるようになりました。Azure Private Link接続を無効にすると、BlueXPはサービスエンドポイントを使用します。

"Cloud Volumes ONTAP でのAzureプライベートリンク接続の詳細については、こちらをご覧ください"。

Google CloudでのStorage VMの作成がサポートされます

Google CloudのCloud Volumes ONTAP では、9.11.1リリース以降、複数のStorage VMがサポートされています。このリリースのコネクタから、BlueXPでは、Cloud Volumes ONTAP を使用してGoogle CloudのHAペアにStorage VMを作成できるようになりました。

Storage VMの作成をサポートするには、次のコネクタに対する新しいGoogle Cloud権限が必要です。

```
- compute.instanceGroups.get
- compute.addresses.get
```

ONTAP CLIまたはSystem Managerを使用して、シングルノードシステムにStorage VMを作成する必要があります。

- "Google CloudのStorage VMの制限に関する詳細を確認できます"
- "Google CloudでCloud Volumes ONTAP 向けのデータ提供用Storage VMを作成する方法をご確認ください"

2022年5月2日

コネクタの3.9.18リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.11.0

BlueXPでCloud Volumes ONTAP 9.11.0の導入と管理が可能になりました

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

メディエーターのアップグレードに関する機能拡張

BlueXPがHAペアのメディエーターをアップグレードすると、新しいメディエーターイメージがブートディスクを削除する前に使用可能であることが検証されるようになりました。この変更により、アップグレードプロセスが失敗した場合でもメディエーターは正常に動作し続けることができます。

K8sタブが削除されました

K8sタブは以前のでは廃止されており、現在は削除されています。KubernetesとCloud Volumes ONTAP を併用する場合は、高度なデータ管理のための作業環境として、管理対象- Kubernetesクラスタをキャンバスに追加できます。

"BlueXPでのKubernetesのデータ管理について説明します"

Azureの年間契約

EssentialsパッケージとProfessionalパッケージは、年間契約を通じてAzureで利用できるようになりました。年間契約を購入するには、ネットアップの営業担当者にお問い合わせください。この契約は、Azure Marketplaceでのプライベートオファーとして提供されます。

ネットアップがお客様とプライベートオファーを共有したあとは、Azure Marketplaceでの作業環境の作成時にサブスクリプションするときに、年間プランを選択できます。

"ライセンスの詳細については、こちらをご覧ください"。

S3 Glacierのインスタント検索

Amazon S3 Glacier Instant Retrievalストレージクラスに階層化データを格納できるようになりました。

"階層化データのストレージクラスを変更する方法について説明します"。

コネクタに新しいAWS権限が必要です

単一のAvailability Zone（AZ；アベイラビリティゾーン）にHAペアを導入する際にAWS分散配置グループを作成するためには、次の権限が必要です。

```
"ec2:DescribePlacementGroups",
"iam:GetRolePolicy",
```

これらの権限は、BlueXPによる配置グループの作成方法を最適化するために必要になりました。

BlueXPに追加したAWSクレデンシャルの各セットに、これらの権限を必ず付与してください。 "AWSの最新のコネクタポリシーを確認します"。

新しいGoogle Cloudリージョンサポート

9.10.1リリース以降、Cloud Volumes ONTAP は次のGoogle Cloudリージョンでサポートされるようになりました。

- デリー（アジア-サウス2）
- メルボルン（オーストラリア-スモアカス2）
- Milan（Europe - west8）-シングルノードのみ
- Santiago（southamerica-west1）-シングルノードのみ

"Cloud Volumes ONTAP でサポートされるリージョンの完全なリストを表示します"

Google Cloudでのn2標準16のサポート

Google CloudのCloud Volumes ONTAP では、9.10.1リリース以降のn2標準-16マシンタイプがサポートされます。

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

Google Cloudファイアウォールポリシーの機能強化

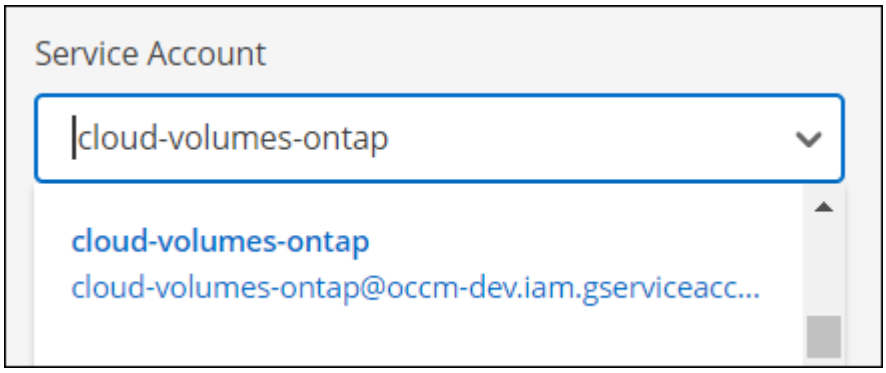
- Google CloudでCloud Volumes ONTAP HAペアを作成すると、VPC内の既存のすべてのファイアウォールポリシーがBlueXPに表示されるようになりました。

  以前は、ターゲットタグがないVPC -1、VPC -2、またはVPC -3のポリシーは表示されませんでした。

- Google CloudでCloud Volumes ONTAP シングルノードシステムを作成する際に、定義済みのファイアウォールポリシーで、選択したVPC内のトラフィックのみを許可するか（推奨）、すべてのVPC内のトラフィックを許可するかを選択できるようになりました。

Google Cloudサービスアカウントの機能強化

Cloud Volumes ONTAP で使用するGoogle Cloudサービスアカウントを選択すると、各サービスアカウントに関連付けられているメールアドレスがBlueXPに表示されるようになりました。メールアドレスを表示すると、同じ名前を共有するサービスアカウントを区別しやすくなります。



2022年4月3日

System Manager のリンクが削除されました

Cloud Volumes ONTAP 作業環境内から以前に利用可能だった System Manager のリンクを削除しました。

Cloud Volumes ONTAP システムに接続している Web ブラウザにクラスタ管理 IP アドレスを入力しても、System Manager に接続できます。 "System Manager への接続に関する詳細情報"。

WORM ストレージの充電

導入時の特別料金が期限切れになり、 WORM ストレージの使用料が請求されます。WORM ボリュームのプロビジョニング済みの合計容量に基づいて、 1 時間ごとに課金されます。この環境 の新規および既存の Cloud Volumes ONTAP システムです。

"WORM ストレージの価格設定については、こちらをご覧ください"。

(2022年2月27日).

コネクタの3.9.16リリースでは、次の変更が加えられました。

ボリュームウィザードの再設計

特定のアグリゲートに * Advanced allocation * オプションからボリュームを作成するときに、新しいボリューム作成ウィザードを使用できるようになりました。

"特定のアグリゲートにボリュームを作成する方法について説明します"。

2022年2月9日

市場の最新情報

- EssentialsパッケージとProfessionalパッケージは、すべてのクラウドプロバイダマーケットプレイスで利用できるようになりました。

  容量単位の課金方法では、時間単位での支払いや、年間契約の購入をクラウドプロバイダから直接行うことができます。容量単位のライセンスは、ネットアップから直接購入することもできます。

  クラウドマーケットプレイスで既存のサブスクリプションがある場合は、それらの新しいサービスにも自動的にサブスクライブされます。新しい Cloud Volumes ONTAP 作業環境の導入時に、容量単位の課金を選択できます。

  新規のお客様の場合は、新しい作業環境を作成するときに登録を求めるメッセージが表示されます。

- すべてのクラウドプロバイダマーケットプレイスからのノード単位のライセンスが廃止され、新しいユーザには提供されなくなりました。これには、年間契約と時間単位のサブスクリプション（ Explore 、 Standard 、 Premium ）が含まれます。

  この充電方法は、有効なサブスクリプションをお持ちの既存のお客様には引き続きご利用いただけます。

"Cloud Volumes ONTAP のライセンスオプションの詳細については、こちらをご覧ください"。

2022年2月6日

未割り当ての **Exchange** ライセンス

Cloud Volumes ONTAP 用の未割り当てのノードベースライセンスがあり、使用していない場合は、そのライセンスを Cloud Backup ライセンス、 Cloud Data Sense ライセンス、 Cloud Tiering ライセンスに変換してライセンスを交換できるようになりました。

この操作により、 Cloud Volumes ONTAP ライセンスが取り消され、同じ有効期限のサービスに対してドル相当のライセンスが作成されます。

"未割り当てのノードベースライセンスを交換する方法について説明します"。

(2022年1月30日).

コネクタの3.9.15リリースでは、次の変更が加えられました。

ライセンスの選択を再設計

新しい Cloud Volumes ONTAP 作業環境を作成する際に、ライセンス選択画面を再設計しました。この変更は、 2021 年 7 月に導入された容量別課金方法と、クラウドプロバイダマーケットプレイスを通じて提供される予定のサービスを反映しています。

デジタルウォレットの更新

Cloud Volumes ONTAP ライセンスを 1 つのタブに統合し、 * デジタルウォレット * を更新しました。

2022年1月2日

コネクタの3.9.14リリースでは、次の変更が導入されました。

追加の**Azure VM**タイプがサポートされます

Cloud Volumes ONTAP は、 9.10.1 リリース以降、 Microsoft Azure で次の VM タイプでサポートされるようになりました。

- e4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

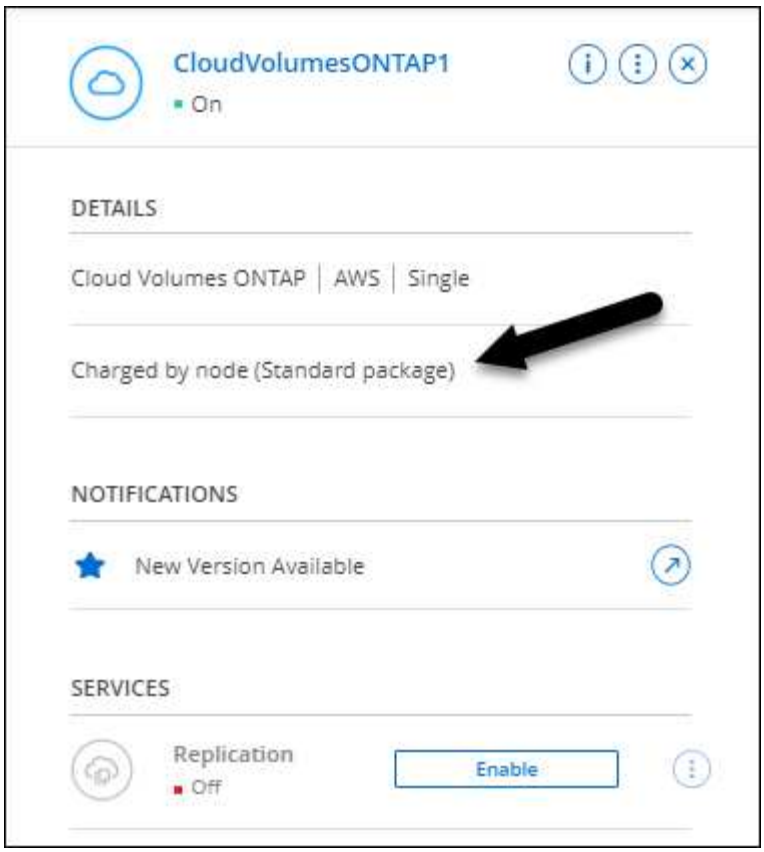
にアクセスします "Cloud Volumes ONTAP リリースノート" サポートされる構成の詳細については、を参照してください。

FlexClone による課金の更新

を使用する場合 "容量単位のライセンスです" Cloud Volumes ONTAP については、 FlexClone ボリュームで使用される容量の追加料金は発生しません。

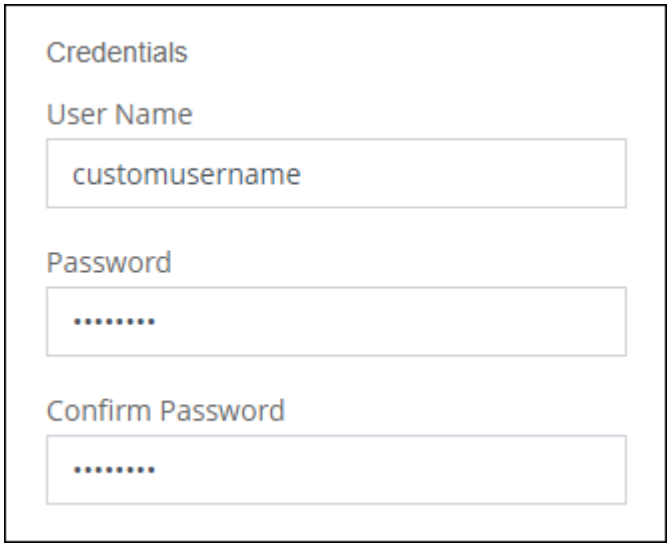
充電方法が表示されます

Cloud Volumes ONTAP の各作業環境の充電方法がキャンバスの右側のパネルに表示されるようになりました。



ユーザ名を選択します

Cloud Volumes ONTAP 作業環境を作成する際に、デフォルトの admin ユーザ名ではなく、優先ユーザ名を入力できるようになりました。



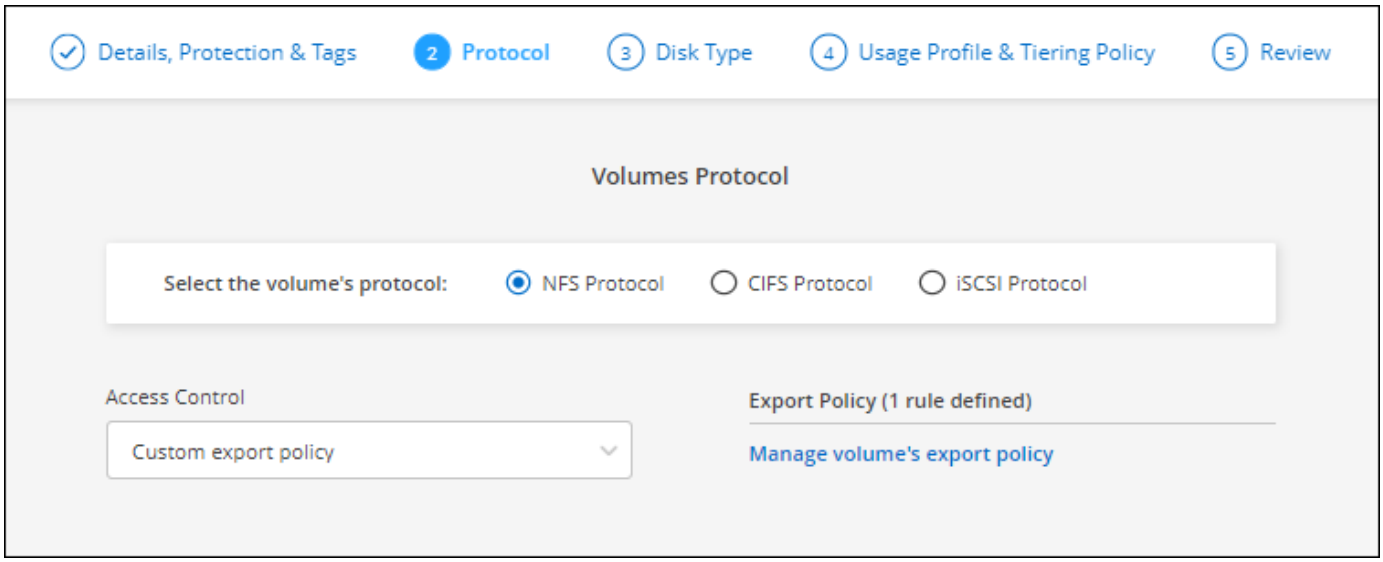
ボリューム作成の機能拡張

ボリューム作成機能がいくつか強化されました。

- 使いやすいようにボリューム作成ウィザードの設計が変更されました。
- ボリュームに追加するタグがアプリケーションテンプレートサービスに関連付けられ、リソースの管理を

整理して簡単にすることができます。

- これで、 NFS 用のカスタムエクスポートポリシーを選択できるようになりました。



(2021年11月28日).

コネクタの3.9.13リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.10.1

BlueXPでCloud Volumes ONTAP 9.10.1の導入と管理が可能になりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

NetApp Keystone サブスクリプション

Keystoneサブスクリプションを使用して、Cloud Volumes ONTAP HAペアの料金を支払うことができるようになりました。

Keystoneサブスクリプションは、CAPEX（設備投資）やリースよりもOPEX（運用コスト）消費モデルを希望するお客様に、シームレスなハイブリッドクラウドエクスペリエンスを提供する、従量課金制のサブスクリプションベースのサービスです。

Keystoneサブスクリプションは、BlueXPから導入できるすべての新しいバージョンのCloud Volumes ONTAPでサポートされます。

- "NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。
- "BlueXPでKeystoneサブスクリプションの利用を開始する方法をご紹介します"。

AWS リージョンが新たにサポートされるようになり

Cloud Volumes ONTAP は、 AWS アジア太平洋（大阪）リージョン（ AP-F北東 -3 ）でサポートされるようになりました。

ポート削減

Azure の Cloud Volumes ONTAP システムでは、シングルノードシステムと HA ペアの両方に対してポート 8023 と 49000 が開かれなくなりました。

これにより、 Cloud Volumes ONTAP の _new_環境 システムが、 3.9.13 リリース以降のコネクタから変更されます。

2021年10月4日

コネクタの3.9.11リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.10.0

BlueXPはCloud Volumes ONTAP 9.10.0を導入して管理できるようになりました

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

導入時間を短縮

通常の書き込み速度が有効な場合、 Microsoft Azure または Google Cloud で Cloud Volumes ONTAP 作業環境を導入するための時間を短縮しました。導入時間が平均して 3~4 分短縮されます。

2021年9月2日

コネクタの3.9.10リリースでは、次の変更が導入されました。

Azure のお客様が管理する暗号化キー

データは、を使用して Azure の Cloud Volumes ONTAP で自動的に暗号化されます "Azure Storage Service Encryption の略" Microsoft が管理するキーを使用する場合：ただし、次の手順を実行する代わりに、お客様が管理する独自の暗号化キーを使用できるようになりました。

1. Azure で、キーヴォールトを作成し、そのヴォールトでキーを生成します。
2. BlueXPから'APIを使用して'キーを使用するCloud Volumes ONTAP 作業環境を作成します

"これらの手順の詳細については、こちらをご覧ください"。

2021 年 7 月 7 日

3.9.8リリースのコネクタには、次の変更が加えられています。

新しい充電方法

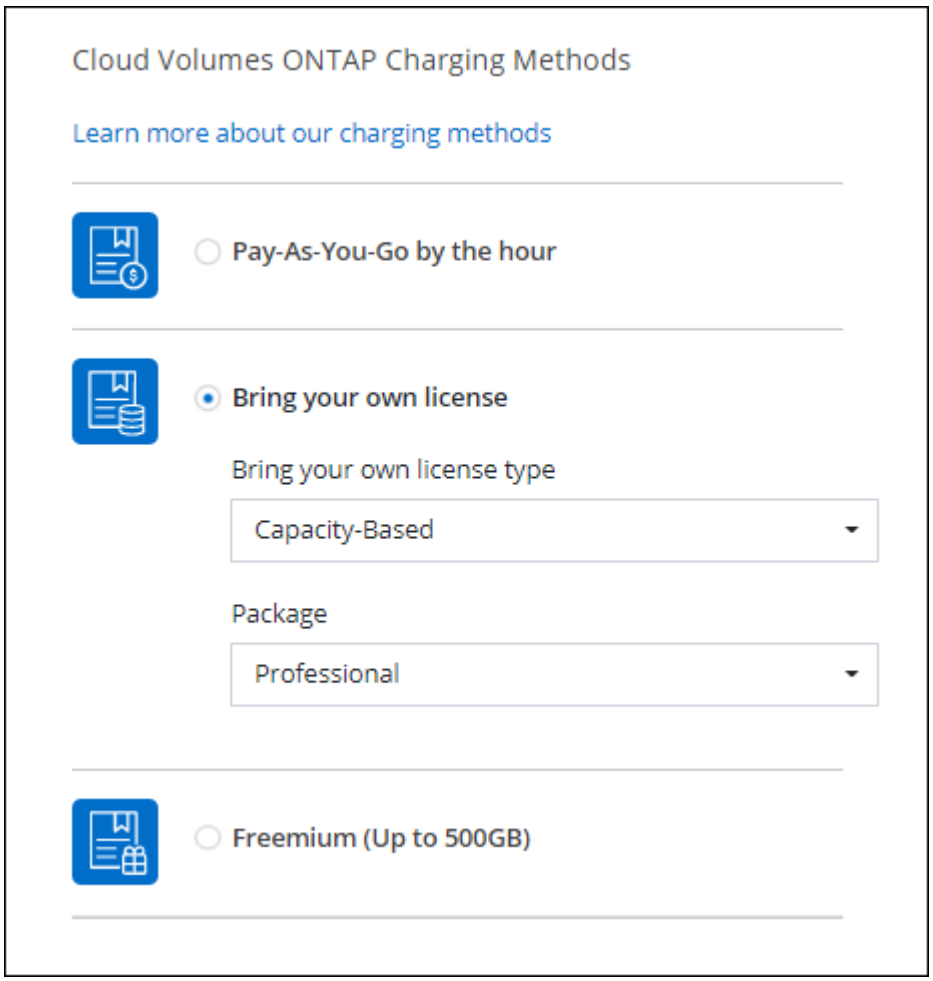
Cloud Volumes ONTAP では、新しい充電方法を利用できます。

- * 容量ベースの BYOL * ：容量ベースのライセンスでは、 TiB あたりの Cloud Volumes ONTAP 料金を支払うことができます。このライセンスはネットアップアカウントに関連付けられており、ライセンスで十分な容量が確保されていれば、複数の Cloud Volumes ONTAP システムを作成できるようになっています。容量ベースのライセンスは、 *Essentials_or_Professional* のいずれかのパッケージ形式で提供されます。

- * Freemium offering * ： Freemium により、ネットアップのすべての Cloud Volumes ONTAP 機能を無償で使用できます（クラウドプロバイダの料金は引き続き適用されます）。システムあたりのプロビジョニング可能な容量は 500 GiB に制限されており、サポート契約はありません。最大 10 個の Freemium システムを使用できます。

  "これらのライセンスオプションの詳細については、こちらをご覧ください"。

  以下に、充電方法の例を示します。



一般的に使用できる **WORM** ストレージ

Write Once 、 Read Many （ WORM ）ストレージはプレビューではなくなり、 Cloud Volumes ONTAP で一般的に使用できるようになりました。 "WORM ストレージの詳細については、こちらをご覧ください。"。

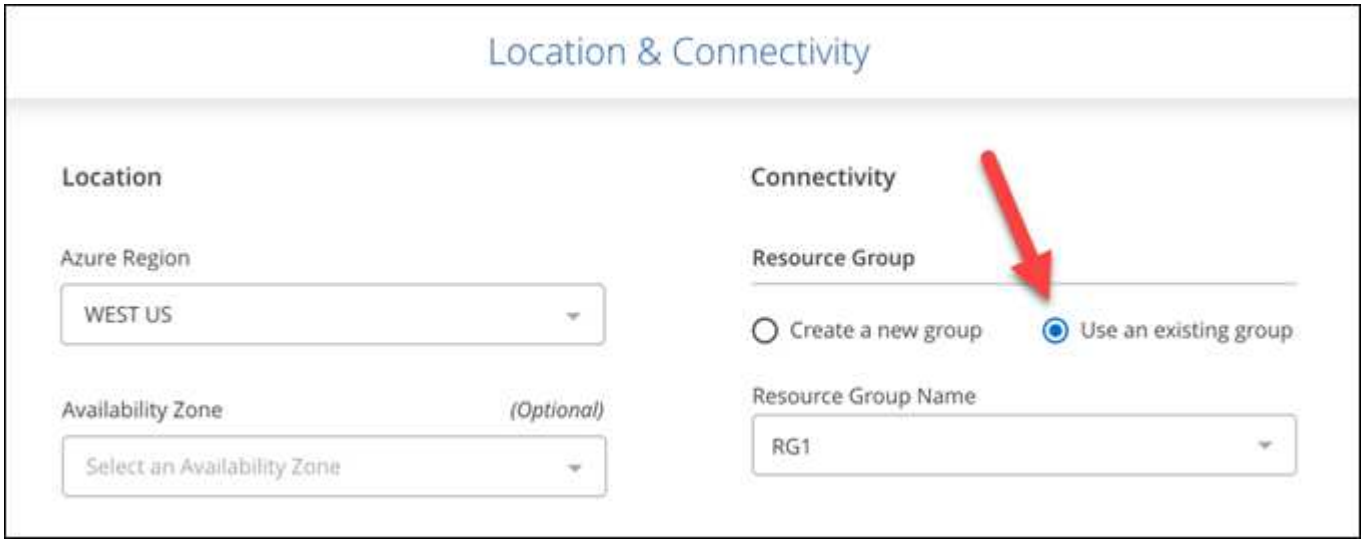
AWS で **m5dn.24xlarge** をサポートしています

9.9.1 リリース以降、 Cloud Volumes ONTAP では m5dn.24xlarge インスタンスタイプがサポートされるようになりました。課金方式は PAYGO Premium 、 Bring Your Own License （ BYOL ；お客様所有のライセンスを使用）、 Freemium です。

"AWS で Cloud Volumes ONTAP のサポートされている構成を表示します"。

既存の **Azure** リソースグループを選択します

Azure で Cloud Volumes ONTAP システムを作成する際に、 VM とその関連リソースに対して既存のリソースグループを選択できるようになりました。



次の権限を使用すると、展開に失敗したり削除したりした場合に、Cloud Volumes ONTAP リソースをリソースグループから削除できます。

```
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
```

BlueXPに追加したAzureクレデンシャルの各セットに、これらの権限を必ず付与してください。 "Azureの最新のコネクタポリシーを表示します"。

Blob パブリックアクセスが **Azure** で無効になりました

セキュリティの強化として、Cloud Volumes ONTAP 用のストレージアカウントを作成する際に、BlueXPは*Blobパブリックアクセス*を無効にするようになりました。

Azure Private Link の機能強化

BlueXPでは、新しいCloud Volumes ONTAP システムのブート診断ストレージアカウントでAzure Private Link接続がデフォルトで有効になっています。

つまり、 Cloud Volumes ONTAP の _all_storage アカウントでプライベートリンクが使用されるようになります。

"Azure プライベートリンクとクラウドの使用の詳細については、こちらをご覧ください Volume ONTAP の略"。

Google Cloud 内の分散型の永続的ディスク

9.9.1 リリース以降、 Cloud Volumes ONTAP では Balanced Persistent Disk （ pd-bBalanced ）がサポートされるようになりました。

この SSD は、 GiB あたりの IOPS を下げて、パフォーマンスとコストのバランスを取ります。

Custom-4-16384 は **Google Cloud** でサポートされなくなりました

新しい Cloud Volumes ONTAP システムでは、 custom-4-16384 マシンタイプはサポートされなくなりました。

このタイプのマシンで既存のシステムを実行している場合は、引き続き使用できますが、 n2 標準 -4 マシンタイプに切り替えることをお勧めします。

"GCPのCloud Volumes ONTAPでサポートされている構成を表示する"。

2021年5月30日

コネクタの3.9.7リリースでは、次の変更が導入されました。

AWS での新しいプロフェッショナルパッケージ

新しいプロフェッショナルパッケージでは、 AWS Marketplace で毎年契約を締結し、 Cloud Volumes ONTAP と Cloud Backup Service をバンドルできます。支払いは TiB あたりです。このサブスクリプションでは、オンプレミスのデータをバックアップすることはできません。

この支払いオプションを選択すると、 EBS ディスクを介して Cloud Volumes ONTAP システムあたり最大 2PiB をプロビジョニングし、 S3 オブジェクトストレージ（シングルノードまたは HA ）に階層化することができます。

にアクセスします "AWS Marketplace のページ" 価格の詳細を表示するには、を参照してください "Cloud Volumes ONTAP リリースノート" このライセンスオプションの詳細については、を参照してください。

AWS の **EBS** ボリュームでタグを使用します

新しいCloud Volumes ONTAP 作業環境を作成すると、EBSボリュームにタグが追加されます。タグは、Cloud Volumes ONTAP の導入後に作成されたものです。

この変更は、サービス制御ポリシー（ SCP ）を使用して権限を管理する場合に役立ちます。

auto 階層化ポリシーの最小クーリング期間

auto 階層化ポリシーを使用してボリュームのデータ階層化を有効にした場合、 API を使用して最小クーリング期間を調整できるようになりました。

"最小クーリング期間の調整方法について説明します。"

カスタムエクスポートポリシーの機能拡張

新しいNFSボリュームを作成すると、カスタムのエクスポートポリシーが昇順に表示されるようになり、必要なエクスポートポリシーを簡単に見つけることができます。

古いクラウド **Snapshot** の削除

BlueXPは、Cloud Volumes ONTAP システムの導入時に作成されたルートディスクと起動ディスクの古いクラウドスナップショットを、電源がオフになるたびに削除するようになりました。ルートボリュームとブートボ

リュームの両方に対して最新の 2 つの Snapshot のみが保持されます。

この機能拡張により、不要になった Snapshot を削除することでクラウドプロバイダのコストを削減できます。

Azure スナップショットを削除するには、 Connector で新しい権限が必要になることに注意してください。"Azureの最新のコネクタポリシーを表示します"。

```
"Microsoft.Compute/snapshots/delete"
```

2021年5月24日

Cloud Volumes ONTAP 9.9.1

BlueXPでCloud Volumes ONTAP 9.9.1の導入と管理が可能になりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

2021年4月11日

コネクタの3.9.5リリースでは、次の変更が導入されました。

論理スペースのレポート

BlueXPでは、Cloud Volumes ONTAP 用に作成された最初のStorage VMで論理スペースのレポートが可能になりました。

スペースが論理的に報告されると、 ONTAP は、 Storage Efficiency 機能で削減されたすべての物理スペースが使用済みと報告するようにボリュームスペースを報告します。

AWS で **GP3** ディスクがサポートされます

Cloud Volumes ONTAP では、 9.7 リリース以降、 _General Purpose SSD （ GP3 ） _disks がサポートされるようになりました。GP3 ディスクは、幅広いワークロードのコストとパフォーマンスのバランスが取れた、最も低コストの SSD です。

"Cloud Volumes ONTAP で GP3 ディスクを使用する方法については、こちらをご覧ください"。

コールド **HDD** ディスクは **AWS** ではサポートされなくなりました

Cloud Volumes ONTAP はコールド HDD （ sc1 ）ディスクをサポートしなくなりました。

TLS 1.2 を使用して **Azure** ストレージアカウントを作成します

BlueXPがAzure for Cloud Volumes ONTAP でストレージアカウントを作成すると、ストレージアカウントのTLSバージョンがバージョン1.2になります。

2021年3月8日

コネクタの3.9.4リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.9.

BlueXPでは、Cloud Volumes ONTAP 9.9.2.0を展開および管理できるようになりました。

"このリリースのに含まれる新機能について説明します Cloud Volumes ONTAP"。

AWS C2S 環境をサポートします

クラウドサービス 9.8 を AWS Commercial Cloud Volumes ONTAP （ C2S ）環境に導入できるようになりました。

"C2S の使用を開始する方法をご確認ください"。

AWS 暗号化でユーザが管理する **CMK** を使用

BlueXPでは、AWS Key Management Service（KMS）を使用してCloud Volumes ONTAP データを暗号化できるようになりました。Cloud Volumes ONTAP 9.9.9..0 以降では、お客様が管理する CMK を選択すると、EBS ディスク上のデータと S3 に階層化されたデータが暗号化されます。これまでは、 EBS データだけが暗号化されていました。

Cloud Volumes ONTAP IAM ロールに CMK を使用するためのアクセス権を付与する必要があります。

"Cloud で AWS KMS を設定する方法については、こちらをご覧ください Volume ONTAP の略"。

Azure DoD のサポート

Cloud Volumes ONTAP 9.8 を、国防総省（ DoD ）の影響レベル 6 （ IL6 ）に導入できるようになりました。

Google Cloud での **IP** アドレスの削減

Google Cloud で Cloud Volumes ONTAP 9.8 以降に必要な IP アドレスの数が削減されました。デフォルトでは、 IP アドレスを 1 つ減らす必要があります（インタークラスタ LIF をノード管理 LIF と統合しました）。また、 API を使用する場合は SVM 管理 LIF の作成を省略でき、追加の IP アドレスが不要になります。

"Google Cloud の IP アドレス要件の詳細については、こちらをご覧ください"。

Google Cloud での共有 **VPC** サポート

Google Cloud で Cloud Volumes ONTAP HA ペアを導入する際に、 VPC -1 、 VPC -2 、および VPC -3 の共有 VPC を選択できるようになりました。以前は、 VPC を共有できるのは VPC のみでした。この変更は Cloud Volumes ONTAP 9.8 以降でサポートされています。

"Google Cloud のネットワーク要件の詳細については、こちらをご覧ください"。

2021年1月4日

コネクタの3.9.2リリースでは、次の変更が加えられています。

AWS がアウトポスト

数カ月前に、 Cloud Volumes ONTAP が Amazon Web Services （ AWS ）の提供開始を宣言したことを発表しました。本日は、AWSのアウトポストでBlueXPとCloud Volumes ONTAP を検証しました。

AWS Outpost を使用している場合は、 Working Environment ウィザードで Outpost VPC を選択して、その Outpost に Cloud Volumes ONTAP を導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。最初に、 AWS Outpost にコネクタを導入する必要があります。

指摘すべき制限事項はいくつかあります。

- でサポートされるのはシングルノードの Cloud Volumes ONTAP システムのみです 今回は
- Cloud Volumes で使用できる EC2 インスタンス ONTAP は、 Outpost で利用できる機能に限定されています
- 現時点では、汎用 SSD （ gp2 ）のみがサポートされます

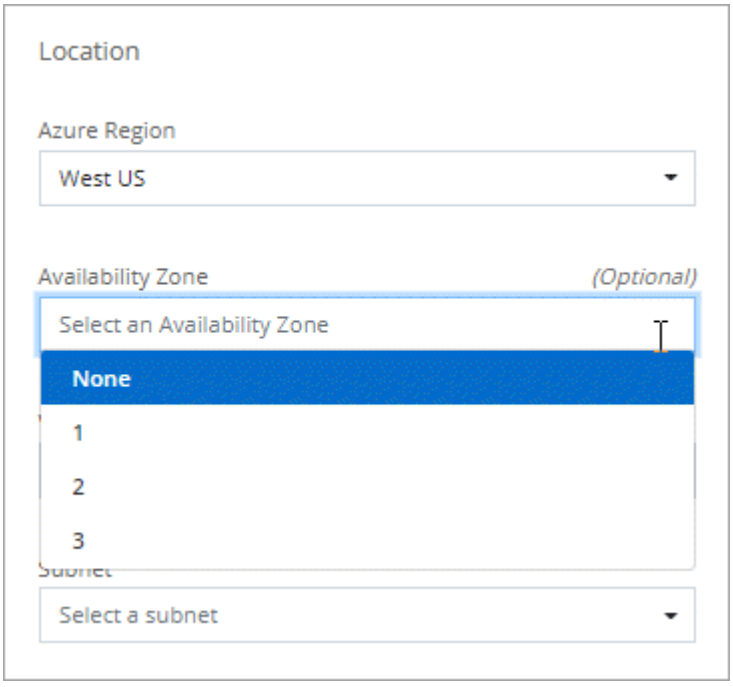
サポートされている Azure リージョンで Ultra SSD VNVRAM を使用します

Cloud Volumes ONTAP では、 Ultra SSD をとして使用できるようになりました VNVRAM （ E32s_v3 VM タイプをで使用する場合） シングルノードシステム "サポートされる任意の Azure リージョン"。

VNVRAM により、書き込みパフォーマンスが向上します。

Azure でアベイラビリティゾーンを選択してください

これで、シングルノードの Cloud Volumes ONTAP システムを導入するアベイラビリティゾーンを選択できます。AZを選択しない場合は、BlueXPによってそのAZが選択されます。



Google Cloud の大容量ディスク

Cloud Volumes ONTAP は GCP で 64 TB のディスクをサポートするようになりました。

GCP の制限により、ディスクのみの場合の最大システム容量は 256 TB のままです。

Google Cloud の新しいマシンタイプ

Cloud Volumes ONTAP では、次のマシンタイプがサポートされるようになりました

- N2 - 標準 -4 （ Explore ライセンスを含む、 BYOL を含む）
- 標準ライセンスを使用し、 BYOL を使用した N2-standard-8
- N2 - Standard - 32 （ Premium ライセンスを使用、 BYOL を使用）

2020年11月3日

コネクタの3.9.0リリースでは、次の変更が導入されました。

Azure Private Link for Cloud Volumes ONTAP の略

デフォルトでは、BlueXPはCloud Volumes ONTAP とそれに関連付けられたストレージアカウント間のAzure Private Link接続を有効にします。プライベートリンクは、 Azure のエンドポイント間の接続を保護します。

- "Azure プライベートリンクの詳細については、こちらをご覧ください"
- "Azure プライベートリンクとクラウドの使用の詳細については、こちらをご覧ください Volume ONTAP の略"

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

これらの制限は、BlueXPでのCloud Volumes ONTAP 管理に固有のものです。Cloud Volumes ONTAP ソフトウェア自体の制限を確認するには、次の手順を実行します。 "Cloud Volumes ONTAP のリリースノートに移動します"

BlueXPでは、FlexGroup ボリュームの作成はサポートされていません

Cloud Volumes ONTAP ではFlexGroup ボリュームがサポートされますが、現時点ではFlexGroup ボリュームの作成はサポートされていません。System ManagerまたはCLIからFlexGroup ボリュームを作成する場合は、BlueXP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。

今後のリリースでは、BlueXPでFlexGroup ボリュームを作成できるようになる予定です。

BlueXPは、Cloud Volumes ONTAP でS3をサポートしていません

Cloud Volumes ONTAPはスケールアウトストレージのオプションとしてS3をサポートしていますが、BlueXPにはこの機能の管理機能はありません。CLI を使用することが、 Cloud Volumes ONTAP からの S3 クライアントアクセスを設定するためのベストプラクティスです。詳細については、を参照してください "S3 構成パ

ワーガイド"。

"S3およびその他のクライアントプロトコルに対するCloud Volumes ONTAP のサポートに関する詳細を確認できます"。

BlueXPでは、Storage VMのディザスタリカバリはサポートされていません

BlueXPは、Storage VM（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のサポートは提供していません。System Manager または CLI を使用する必要があります。

"SVMディザスタリカバリに関する詳細情報"。

AsciiDocの文字置換と組み込み属性のテスト

すべての言語のローカリゼーションと公開を通じて、エンドツーエンドのテストを実施します。

アスタリスク

{アスタリスク}
text{アスタリスク}
text{アスタリスク}
text{アスタリスク}テキスト

二重コロン

{2コロン}
text{2つのコロン}
text{2つのコロン}
text::テキスト

垂直バー

{vbar}
text|
text|
text|テキスト

プラス

{plus}
text+
text+
text+テキスト

角かっこ

{startsb} および {endsb}
text[およびtext]
text[およびtext]
text[およびtext]テキスト

解除されないスペース

{nbsp} 以前

ゼロ幅スペース

Cloud Volumes ONTAP リリースノート

Cloud Volumes ONTAP のリリースノートには、リリース固有の情報が記載されています。リリースの新機能、サポートされる構成、ストレージの制限、および製品の機能に影響する可能性がある既知の制限事項や問題。

"Cloud Volumes ONTAP のリリースノートに移動します"

はじめに

Cloud Volumes ONTAP の詳細をご覧ください

Cloud Volumes ONTAP を使用すると、データ保護、セキュリティ、コンプライアンスを強化しながら、クラウドストレージのコストとパフォーマンスを最適化できます。

Cloud Volumes ONTAP は、クラウドで ONTAP データ管理ソフトウェアを実行するソフトウェア型のストレージアプライアンスです。次回のテストでは、次の主要機能を備えたエンタープライズクラスのストレージを提供します。

- ストレージの効率化

  組み込みのデータ重複排除、データ圧縮、シンプロビジョニング、クローニングを活用して、ストレージコストを最小限に抑えます。

- 高可用性

  クラウド環境で障害が発生した場合でも、エンタープライズクラスの信頼性と継続的な運用を確保できます。

- データ保護

  Cloud Volumes ONTAP は、業界をリードするネットアップのレプリケーションテクノロジである SnapMirror を利用してオンプレミスのデータをクラウドにレプリケートするため、セカンダリコピーを複数のユースケースに簡単に利用できます。

  また、Cloud Volumes ONTAP はBlueXPのバックアップとリカバリと統合することで、クラウドデータの保護と長期アーカイブのためのバックアップとリストアの機能を提供します。

  "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

- データの階層化

  アプリケーションをオフラインにすることなく、ハイパフォーマンスとローパフォーマンスのストレージプールをオンデマンドで切り替えます。

- 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。

  "SnapCenter の詳細については、こちらをご覧ください"

- データセキュリティ

  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。

- プライバシーコンプライアンスの管理

  BlueXPの分類機能と統合することで、データのコンテキストを把握し、機密データを特定できます。

"BlueXPの分類の詳細については、こちらをご覧ください"

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"

新規導入でサポートされるバージョン

BlueXPでは'新しいCloud Volumes ONTAP 作業環境を作成するときに'いくつかの異なるONTAP バージョンから選択できます

それ以外のCloud Volumes ONTAP バージョンは、新規導入ではサポートされません。

AWS

シングルノード

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7
- 9.5 P6.

HA ペア

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7
- 9.5 P6.

Azure

シングルノード

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6.

HA ペア

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

シングルノード

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- P5 9.7

HA ペア

- 9.13.1 GA
- 9.12.1 GA

- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Services の利用を開始しましょう

AWS での Cloud Volumes ONTAP のクイックスタート

いくつかの手順で、 AWS で Cloud Volumes ONTAP を使い始めましょう。

コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "AWS でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"

構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。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。 "詳細はこちら。"。

ネットワークをセットアップします

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

   インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

3. 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。

"ネットワーク要件の詳細については、こちらをご覧ください"。

4 AWS KMS を設定します

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、アクティブなカスタマーマスターキー（ CMK ）が存在することを確認する必要があります。また、コネクタに「 a_key user__ 」という権限を付与する IAM ロールを追加して、各 CMK のキーポリシーを変更する必要があります。 "詳細はこちら。"。

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

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからコネクタを作成しています"
- "AWS Marketplace から Connector を起動する"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPがAWS権限で実行できる機能"

AWSでCloud Volumes ONTAP 構成を計画

AWS に Cloud Volumes ONTAP を導入する場合は、ワークロードの要件に応じて事前設定されたシステムを選択するか、または独自の設定を作成できます。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。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP はほとんどの AWS リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

新しい AWS リージョンは、それらのリージョンでリソースを作成および管理する前に有効にする必要があります。 "リージョンを有効にする方法について説明します"。

サポートされているインスタンスを選択します

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数のインスタンスタイプがサポートされます。

"AWS で Cloud Volumes ONTAP がサポートされる構成"

ストレージの制限を確認

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 での Cloud Volumes ONTAP のストレージの制限"

AWSでシステムのサイズを設定します

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

EBS ディスクタイプの違いは次のとおりです。EBS 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 "AWS ドキュメント：「 EBS Volume Types"。

- _General Purpose SSD （ GP3 ） _ ディスクは、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る最も低コストの SSD です。パフォーマンスは、 IOPS とスループットを基準に定義されます。GP3 ディスクは Cloud Volumes ONTAP 9.7 以降でサポートされています。

  GP3ディスクを選択すると、選択したディスクサイズに基づいて、gp2ディスクに相当するパフォーマンスを提供するデフォルトのIOPSとスループットの値がBlueXPによって設定されます。この値を増やすと、コストを高くしてもパフォーマンスを向上させることができますが、パフォーマンスが低下する可能性があるため、値を小さくすることはできません。つまり、デフォルト値をそのまま使用するか、値を大きくします。低くしないでください。 "GP3 ディスクとそのパフォーマンスについては、こちらをご覧ください"。

  Cloud Volumes ONTAP は、GP3ディスクを使用したAmazon EBS Elastic Volumes機能をサポートしています。 "Elastic Volumesのサポートに関する詳細情報"。

- _ 汎用 SSD （ gp2 ） _ ディスクは、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 （ io1 ） _disks は、コストが高くても最高のパフォーマンスが求められる重要なアプリケーション用です。

  Cloud Volumes ONTAP では、io1ディスクを使用したAmazon EBS Elastic Volumes機能がサポートされています。 "Elastic Volumesのサポートに関する詳細情報"。

- _Throughput Optimized HDD （ st1 ） _disks は、高速で安定したスループットを必要とする、アクセス頻度の高いワークロード用です。価格は低くなります。

スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

EBS ディスクサイズ

をサポートしない構成を選択した場合 "Amazon EBS Elastic Volumes機能"を選択した場合、Cloud Volumes ONTAP システムの起動時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BlueXPが管理できるようにします"必要に応じて "アグリゲートの作成は自分で行います"、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 TiB 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"。

  前述したように、ディスクサイズの選択は、Amazon EBS Elastic Volumes機能をサポートするCloud Volumes ONTAP 構成ではサポートされていません。 "Elastic Volumesのサポートに関する詳細情報"。

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

"AWS で Cloud Volumes ONTAP システムデータのデフォルトディスクを表示する"。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

AWSアウトポストに**Cloud Volumes ONTAP** を導入する準備をします

AWS Outpost を使用している場合は、 Working Environment ウィザードで Outpost VPC を選択して、その Outpost に Cloud Volumes ONTAP を導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。最初に、 AWS Outpost にコネクタを導入する必要があります。

指摘すべき制限事項はいくつかあります。

- でサポートされるのはシングルノードの Cloud Volumes ONTAP システムのみです 今回は
- Cloud Volumes で使用できる EC2 インスタンス ONTAP は、 Outpost で利用できる機能に限定されています
- 現時点では、汎用 SSD （ gp2 ）のみがサポートされます

ネットワーク情報を収集

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。

単一の**AZ**における単一のノードまたは**HA**ペア

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**AZ**にまたがる**HA**ペアを作成します

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のアベイラビリティゾーン	
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	
ノード2のデータのフローティング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	

書き込み速度を選択します

BlueXPでは、Cloud Volumes ONTAP 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。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

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。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または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。

ネットワークをセットアップします

Cloud Volumes ONTAP in AWS のネットワーク要件

BlueXPは、IPアドレス、ネットマスク、ルートなど、Cloud Volumes ONTAP のネットワークコンポーネントのセットアップを処理します。アウトバウンドのインターネットアクセスが可能であること、十分な数のプライベート IP アドレスを利用できること、適切な接続が確立されていることなどを確認する必要があります。

一般的な要件

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 ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

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

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。

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で_OUTBOUND接続を許可する必要もあります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

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 ）"。

プライベート **IP** アドレス

BlueXPは、必要な数のプライベートIPアドレスを自動的にCloud Volumes ONTAP に割り当てます。ネットワークに十分な数のプライベート IP アドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。LIF は、物理ポートに関連付けられた IP アドレスです。

シングルノードシステムの **IP** アドレス

BlueXPでは、1つのノードシステムに6つのIPアドレスが割り当てられます。

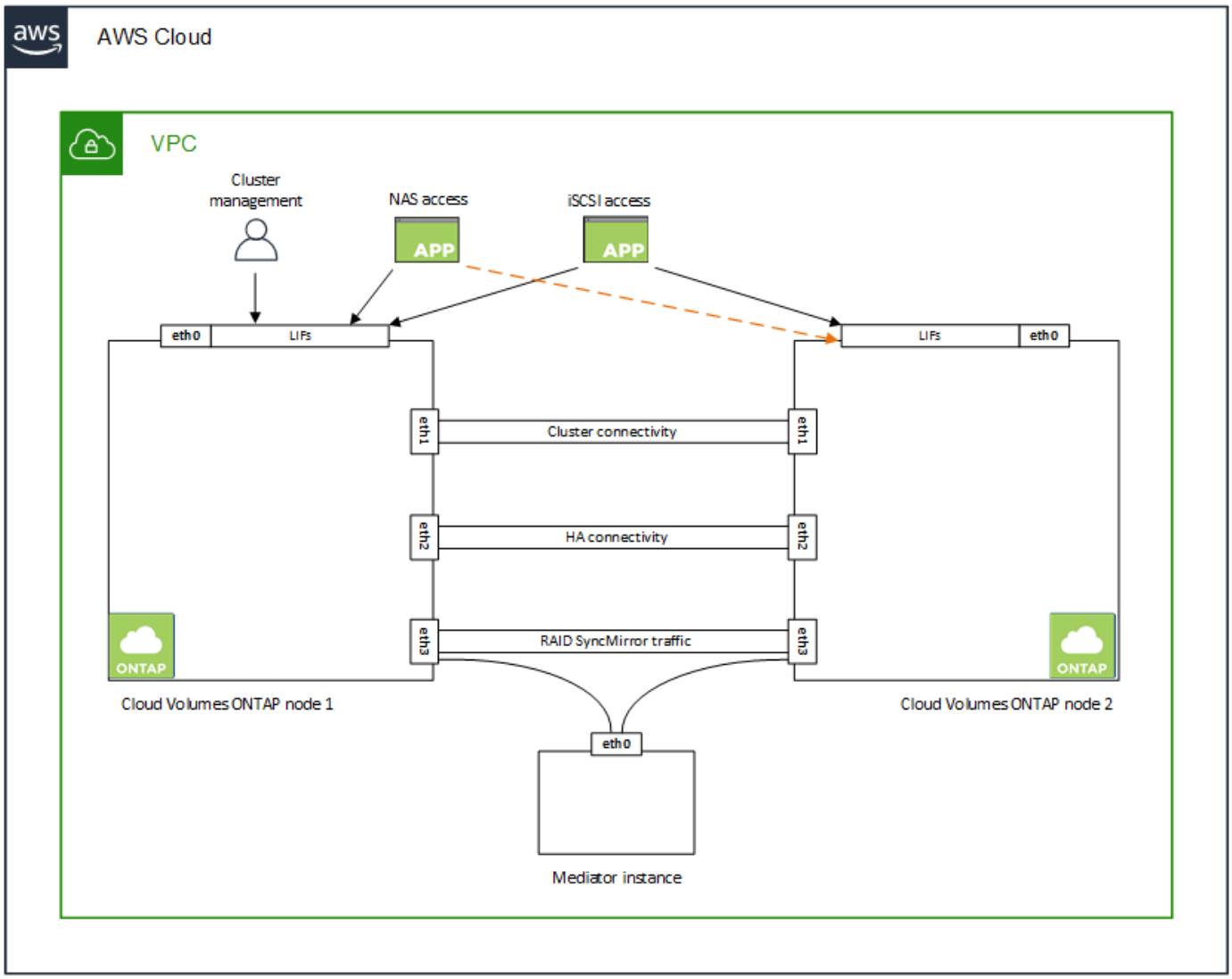
次の表に、各プライベートIPアドレスに関連付けられているLIFの詳細を示します。

LIF	目的
クラスタ管理	クラスタ全体（ HA ペア）の管理。
ノード管理	ノードの管理。
クラスタ間	クラスタ間の通信、バックアップ、レプリケーション。
NAS データ	NAS プロトコルを使用したクライアントアクセス。
iSCSI データ	iSCSI プロトコルを使用したクライアントアクセス。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

LIF	目的
Storage VM管理	Storage VM 管理 LIF は、 SnapCenter などの管理ツールで使用されます。

HA ペアの **IP** アドレス

HA ペアには、シングルノードシステムよりも多くの IP アドレスが必要です。次の図に示すように、これらの IP アドレスは異なるイーサネットインターフェイスに分散されています。



HA ペアに必要なプライベート IP アドレスの数は、選択する導入モデルによって異なります。A_SILE_AWS アベイラビリティゾーン（ AZ ）に導入する HA ペアには 15 個のプライベート IP アドレスが必要です。一方、 _multiple_AZs に導入する HA ペアには、 13 個のプライベート IP アドレスが必要です。

次の表に、各プライベート IP アドレスに関連付けられている LIF の詳細を示します。

単一の **AZ** にある **HA** ペアの **LIF**

LIF	インターフェイス	ノード	目的
クラスタ管理	eth0	ノード 1	クラスタ全体（ HA ペア）の管理。

LIF	インターフェイス	ノード	目的
ノード管理	eth0	ノード 1 とノード 2	ノードの管理。
クラスタ間	eth0	ノード 1 とノード 2	クラスタ間の通信、バックアップ、レプリケーション。
NAS データ	eth0	ノード 1	NAS プロトコルを使用したクライアントアクセス。
iSCSI データ	eth0	ノード 1 とノード 2	iSCSI プロトコルを使用したクライアントアクセス。システムでは、その他の重要なネットワークワークフローにも使用されます。これらのLIFは必須であり、削除しないでください。
クラスタ接続	Eth1	ノード 1 とノード 2	ノード間の通信およびクラスタ内でのデータの移動を可能にします。
HA 接続	eth2	ノード 1 とノード 2	フェイルオーバー時の 2 つのノード間の通信。
RSM iSCSI トラフィック	eth3	ノード 1 とノード 2	RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。
メディエーター	eth0	メディエーター	ストレージのテイクオーバーとギブバックのプロセスを支援するための、ノードとメディエーターの間の通信チャネル。

複数の **AZ** にまたがる **HA** ペア用の **LIF** です

LIF	インターフェイス	ノード	目的
ノード管理	eth0	ノード 1 とノード 2	ノードの管理。
クラスタ間	eth0	ノード 1 とノード 2	クラスタ間の通信、バックアップ、レプリケーション。
iSCSI データ	eth0	ノード 1 とノード 2	iSCSI プロトコルを使用したクライアントアクセス。 また、ノード間でのフローティングIPアドレスの移行も管理します。これらのLIFは必須であり、削除しないでください。
クラスタ接続	Eth1	ノード 1 とノード 2	ノード間の通信およびクラスタ内でのデータの移動を可能にします。
HA 接続	eth2	ノード 1 とノード 2	フェイルオーバー時の 2 つのノード間の通信。
RSM iSCSI トラフィック	eth3	ノード 1 とノード 2	RAID SyncMirror iSCSI トラフィック、および 2 つの Cloud Volumes ONTAP ノードとメディエーター間の通信。
メディエーター	eth0	メディエーター	ストレージのテイクオーバーとギブバックのプロセスを支援するための、ノードとメディエーターの間の通信チャネル。

複数のアベイラビリティゾーンに導入すると、いくつかの LIF が関連付けられます "フローティング IP アドレス"AWS のプライベート IP 制限にはカウントされません。

セキュリティグループ

セキュリティグループを作成する必要はありません。BlueXPではセキュリティグループが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 "セキュリティグループのルール"。

コネクタに関する情報をお探しですか？ "コネクタのセキュリティグループルールを表示します"

データ階層化のための接続

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。"

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（社内ネットワークなど）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"。

vPC共有

9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

"共有サブネットにHAペアを導入する方法について説明します"。

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、作業環境の作成時にBlueXPでネットワークの詳細を入力する必要があるため、これらの要件を確認してください。

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。

サブネットが各アベイラビリティゾーンに存在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"。

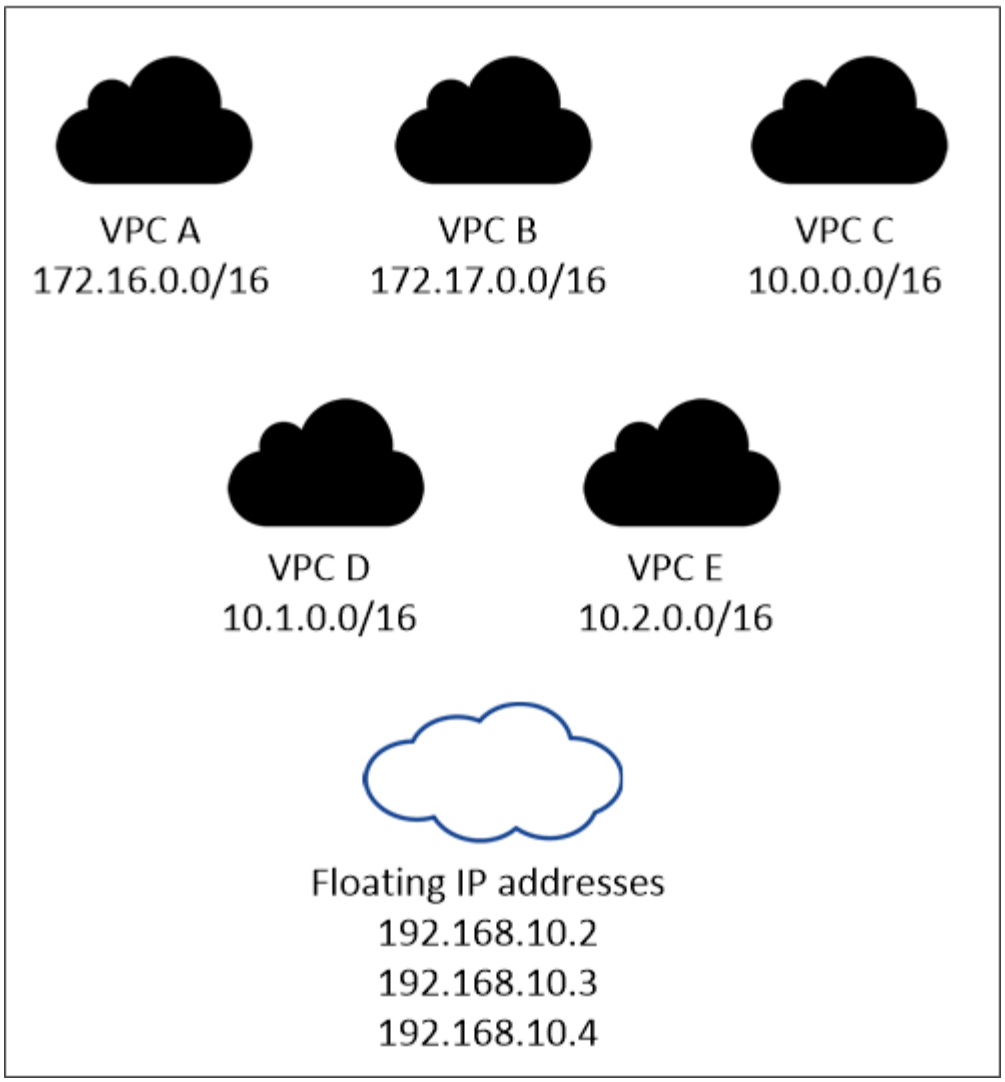
フローティング IP アドレスの 1 つはクラスタ管理用、 1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。SVM 管理用の 4 つ目のフローティング IP アドレスはオプションです。

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。

Cloud Volumes ONTAP HA作業環境を作成する場合は、BlueXP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。システムの起動時に、HAペアにIPアドレスが割り当てられます。

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。



BlueXPでは、VPCの外部にあるクライアントからのiSCSIアクセスとNASアクセスに対して、自動的に静的IPアドレスが作成されます。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**

必要に応じて、 "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

BlueXPでフローティングIPアドレスを指定すると、フローティングIPアドレスへのルートを含むルートテーブルを選択するように求められます。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内のサブネット用のルーティングテーブルが1つ（メインルーティングテーブル）だけの場合は、そのルーティングテーブルにフローティングIPアドレスが自動的に追加されます。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"。

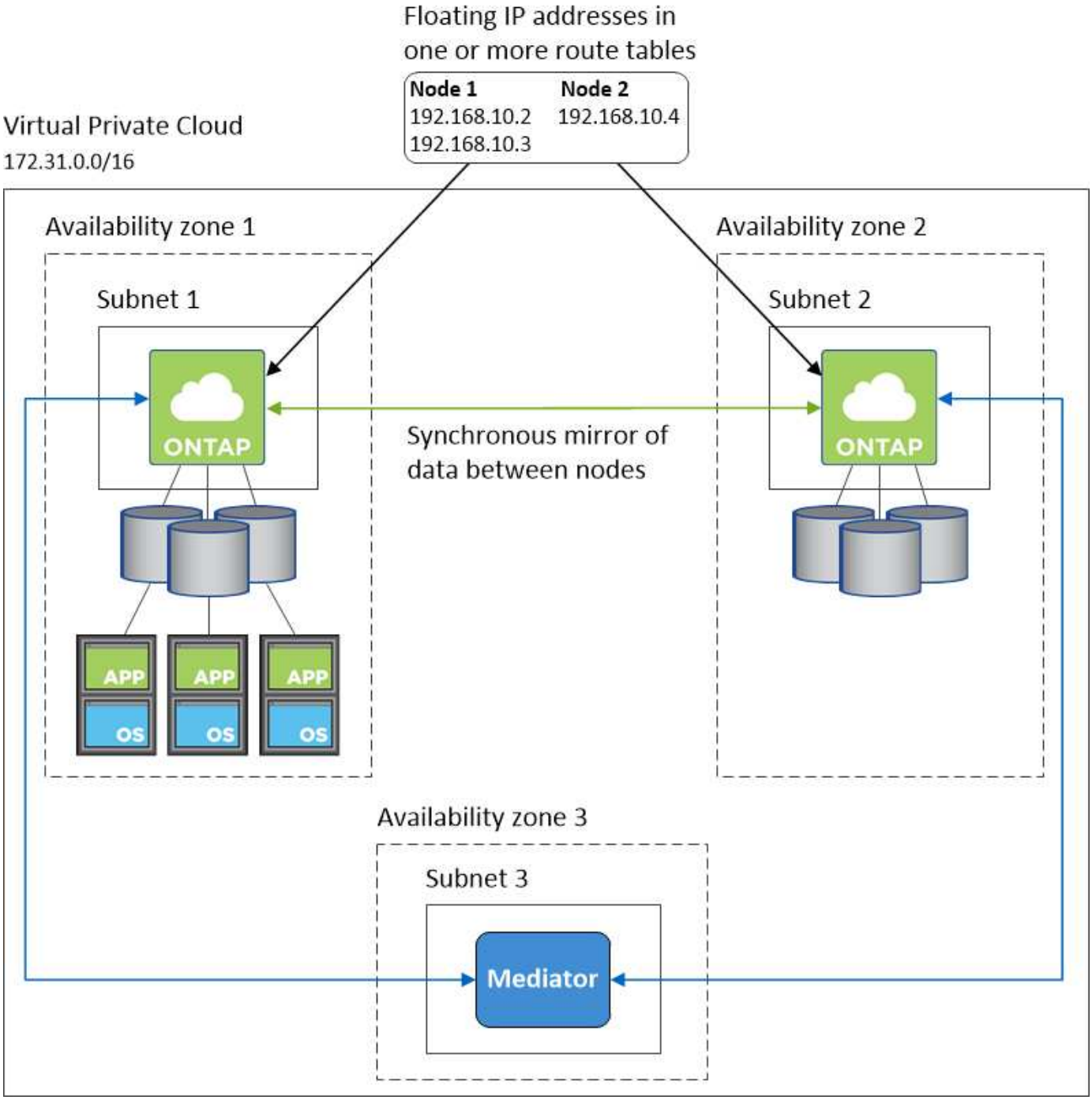
ネットアップの管理ツールとの連携

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。

HA 構成の例

次の図は、複数の AZ にまたがる HA ペアに固有のネットワークコンポーネントを示しています。 3 つのアベイラビリティゾーン、 3 つのサブネット、フローティング IP アドレス、およびルートテーブルです。



コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "AWSのセキュリティグループのルール"

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**

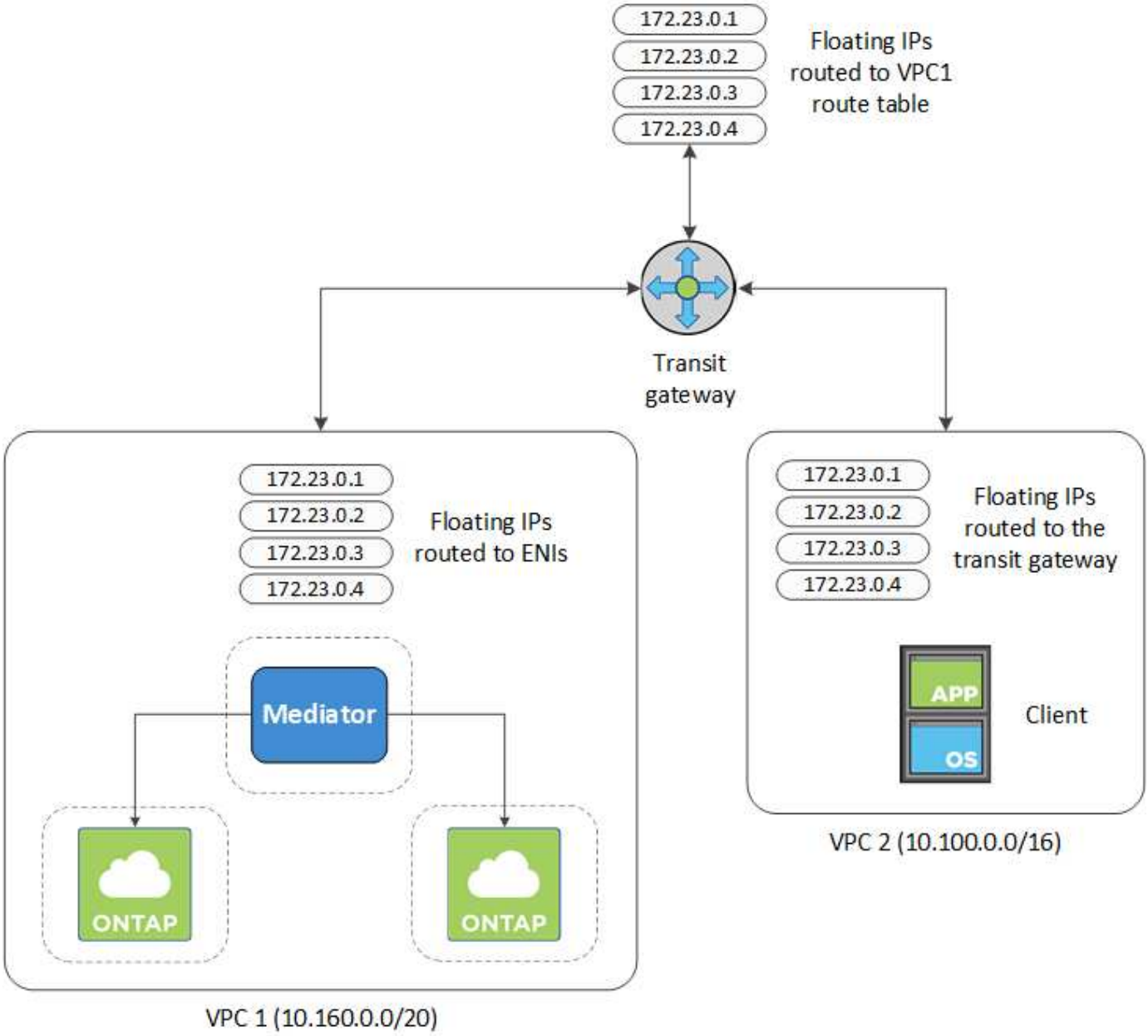
へのアクセスを有効にするために、 AWS 転送ゲートウェイを設定します HA ペアの 1 つ "フローティング IP アドレス" HA ペアが存在する VPC の外部から

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。

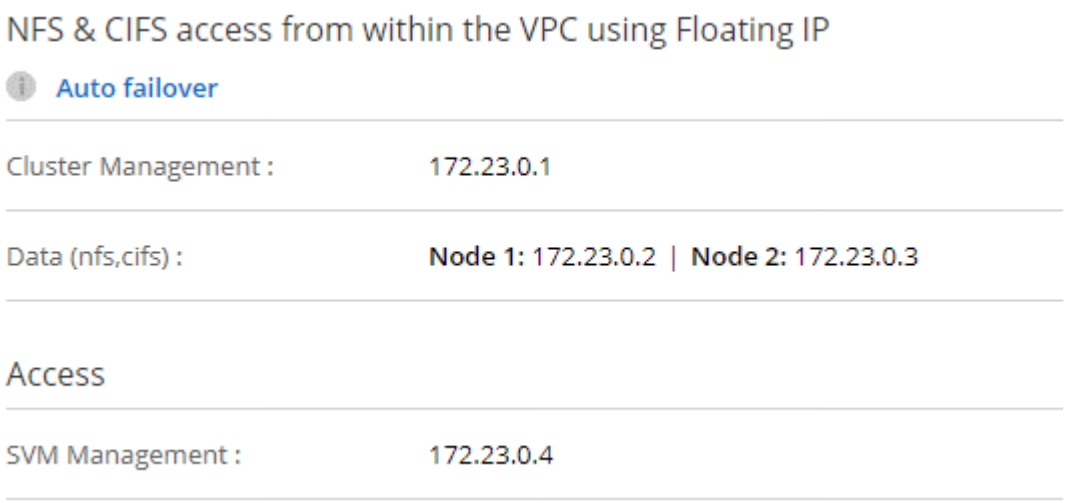


以下に、同様の構成を設定する手順を示します。

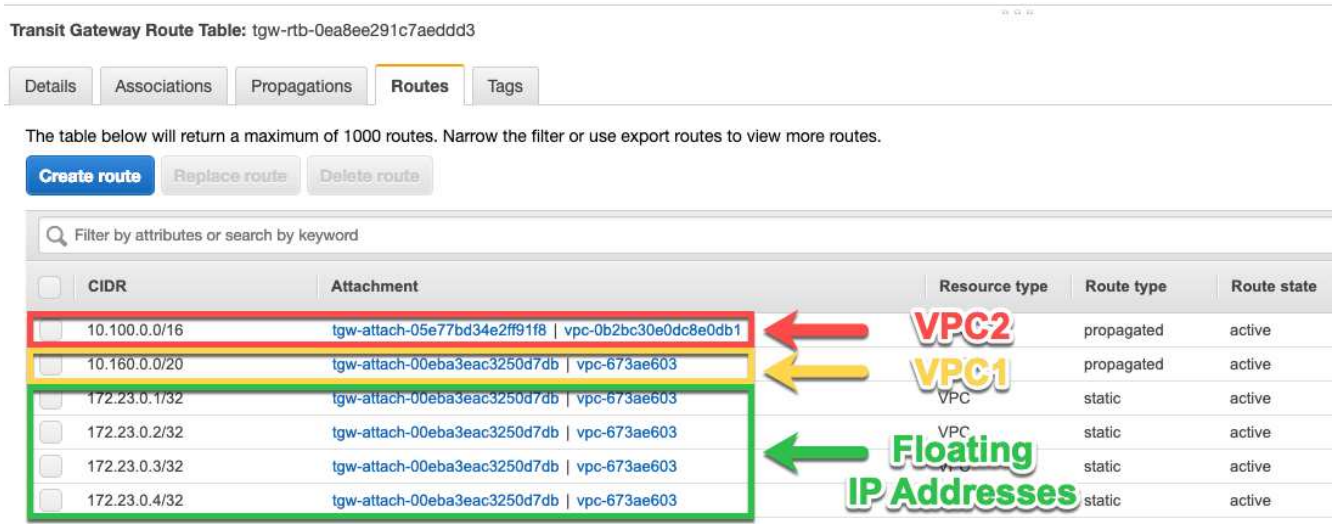
手順

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. VPC とトランジットゲートウェイルートテーブルを関連付ける。
   a. *VPC サービスで、 *Transit Gateway Route Tables * をクリックします。
   b. ルートテーブルを選択します。
   c. [*Associations] をクリックし、 [Create associations] を選択します。
   d. 関連付ける添付ファイル（ VPC ）を選択し、 * 関連付けの作成 * をクリックします。
3. 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、BlueXPの[作業環境情報]ページにあります。次に例を示します。



   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。

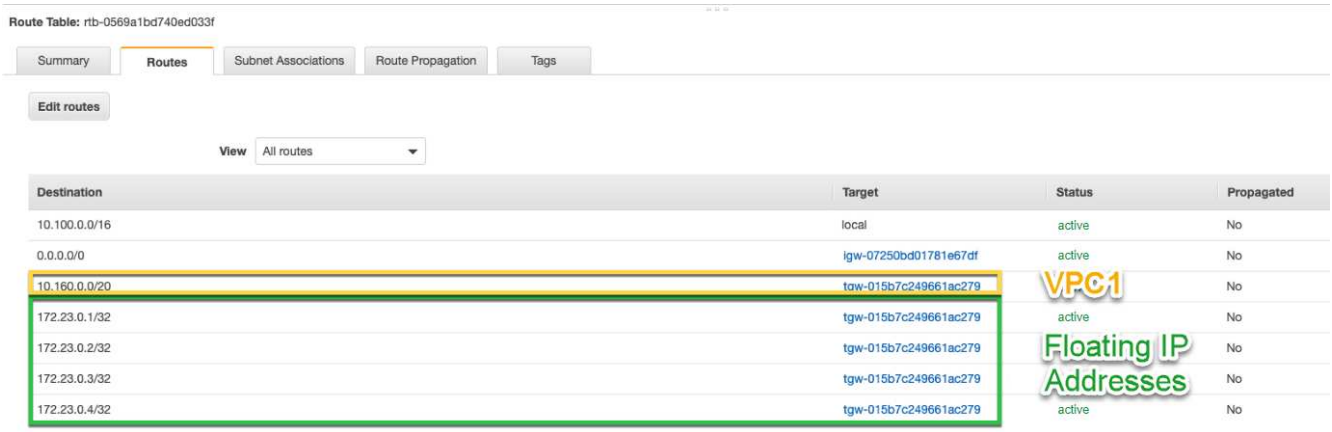


4. フローティング IP アドレスにアクセスする必要がある VPC のルーティングテーブルを変更します。

   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。

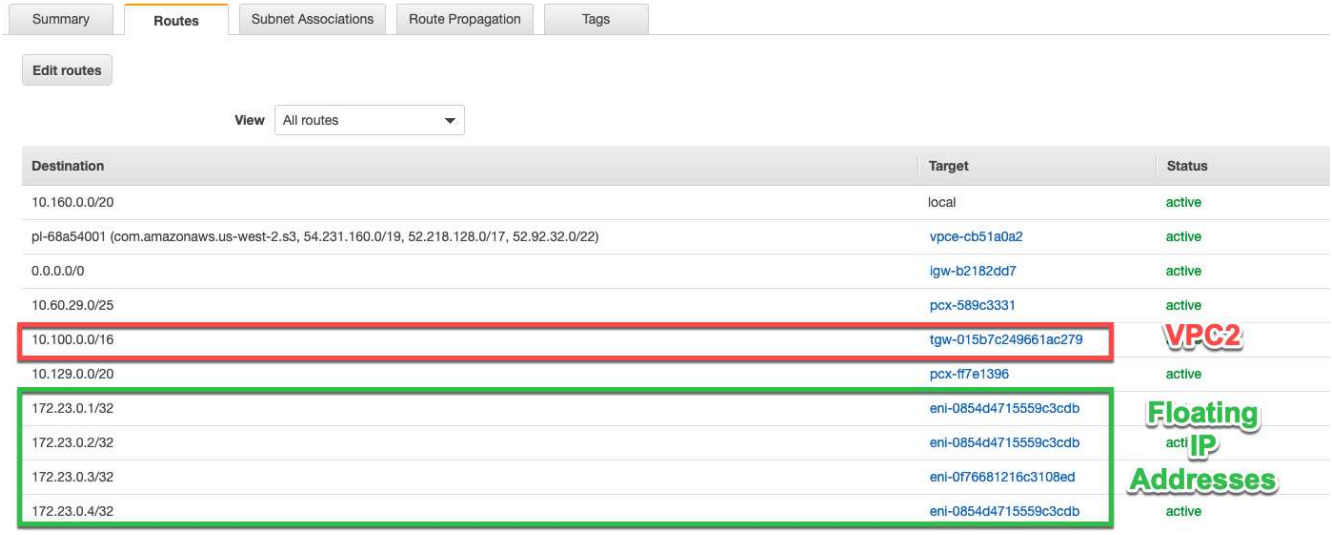
      次の図は、 VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。



5. 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。

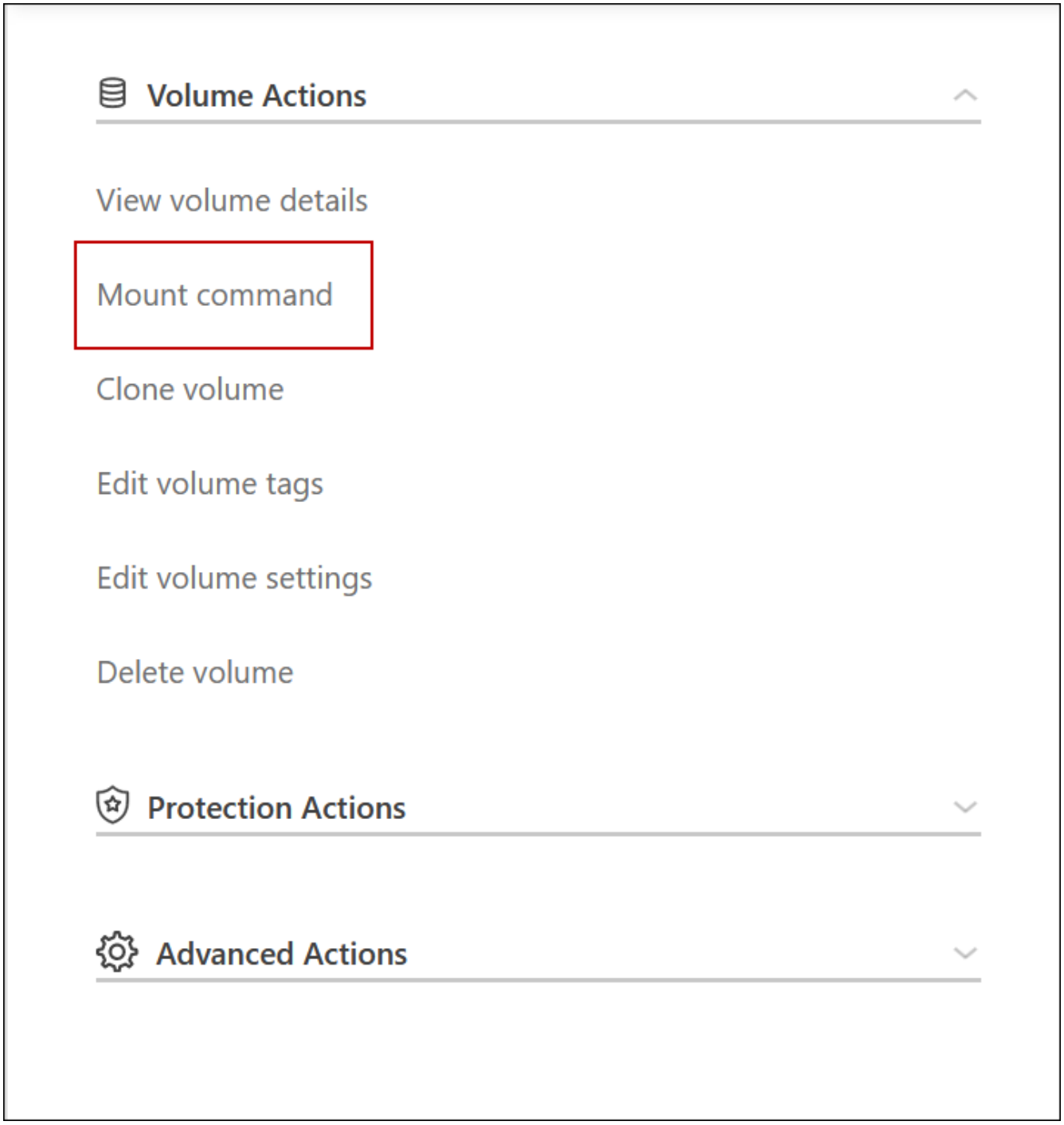
   VPC 間のルーティングが完了するため、この手順は重要です。

   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。BlueXPでは、HAペアを展開すると、フローティングIPがルートテーブルに自動的に追加されました。



6. 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。

   BlueXPで正しいIPアドレスを確認するには、BlueXPの[Manage Volumes]パネルにある*[Mount Command]*オプションを使用します。



7. NFS ボリュームをマウントする場合は、クライアント VPC のサブネットと一致するようにエクスポートポリシーを設定します。

   "ボリュームを編集する方法について説明します"。

   - 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"

HAペアを共有サブネットに導入します

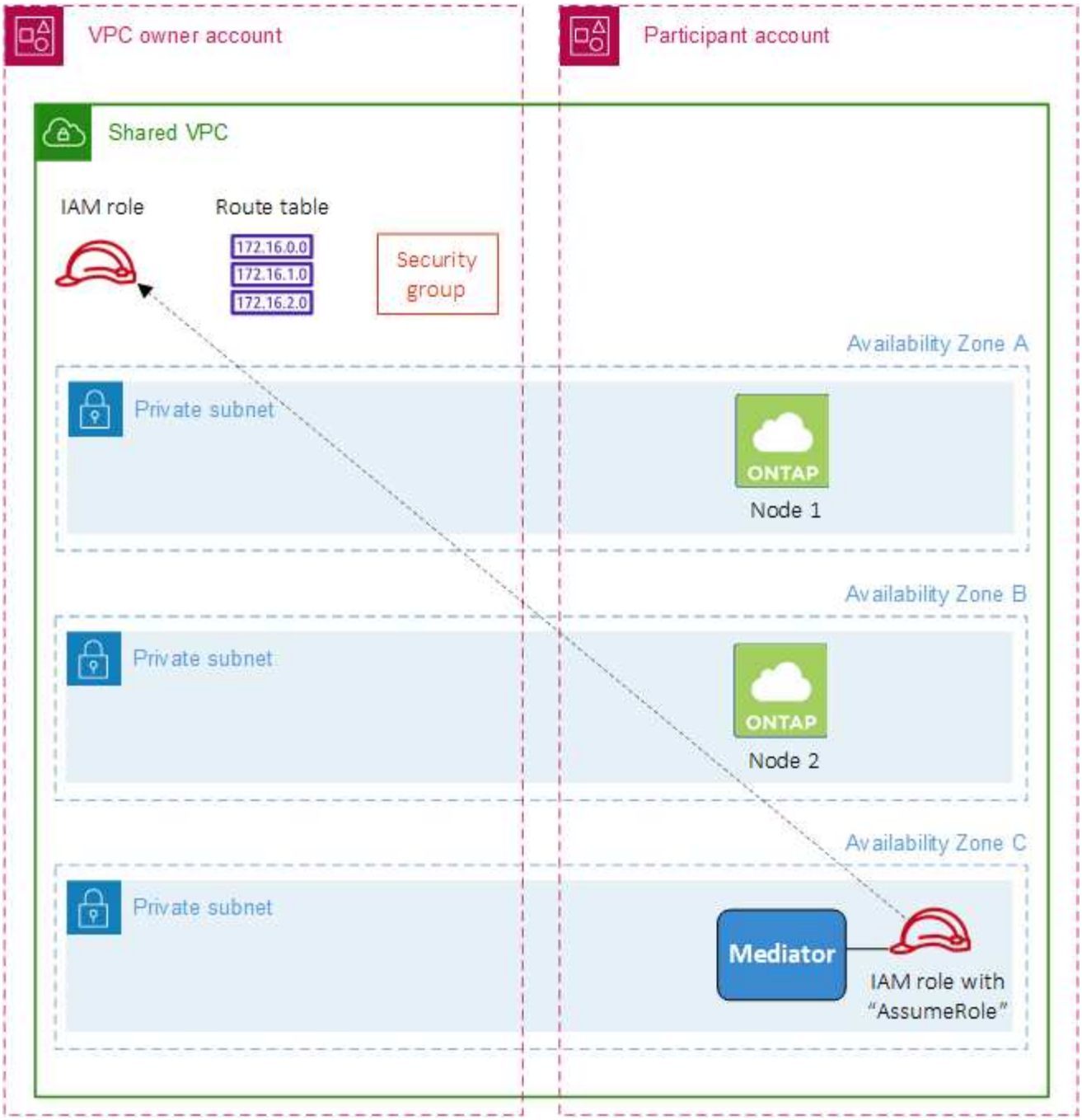
9.11.1リリース以降では、VPCを共有するAWSでCloud Volumes ONTAP HAペアがサポートされます。VPC共有を使用すると、他のAWSアカウントとサブネットを共有できます。この構成を使用するには、AWS環境をセットアップし、APIを使用してHAペアを導入する必要があります。

を使用 "vPC共有"Cloud Volumes ONTAP HA構成は、次の2つのアカウントに分散されます。

- ネットワークを所有するVPC所有者アカウント（VPC、サブネット、ルーティングテーブル、Cloud Volumes ONTAP セキュリティグループ）
- EC2インスタンスが共有サブネット（2つのHAノードとメディエーターを含む）に導入されている参加者アカウント

複数のアベイラビリティゾーンにまたがって導入されているCloud Volumes ONTAP HA構成の場合は、HAメディエーターからVPC所有者アカウントのルーティングテーブルに書き込むための特定の権限が必要です。メディエーターで想定できるIAMロールを設定して、これらの権限を指定する必要があります。

次の図は、この導入に関連するコンポーネントを示しています。



以下の手順で説明するように、サブネットを参加者アカウントと共有し、VPC所有者アカウント内にIAMロールとセキュリティグループを作成する必要があります。

Cloud Volumes ONTAP 作業環境を作成すると、自動的にIAMロールが作成され、メディエーターに関連付けられます。このロールは、VPC所有者アカウントで作成したIAMロールを前提としており、HAペアに関連付けられているルーティングテーブルを変更します。

手順

1. VPC所有者アカウントのサブネットを参加者アカウントと共有します。

   この手順は、HAペアを共有サブネットに導入するために必要です。

   "AWSドキュメント：サブネットを共有"

2. VPC所有者アカウントで、Cloud Volumes ONTAP のセキュリティグループを作成します。

   "Cloud Volumes ONTAP のセキュリティグループルールを参照してください"。HAメディエーターのセキュリティグループを作成する必要はありません。BlueXPはそのような機能を提供します。

3. VPC所有者アカウントで、次の権限を含むIAMロールを作成します。

```
Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
```

4. BlueXP APIを使用して'新しいCloud Volumes ONTAP 作業環境を作成します

   次のフィールドを指定する必要があります。

   - "securityGroupId"

     「securityGroupId」フィールドには、VPC所有者アカウントで作成したセキュリティグループを指定する必要があります（上記の手順2を参照）。

   - "haParams"オブジェクトの"amereRoleArn"を想定します

     「仮定ロールアーn」フィールドには、VPC所有者アカウントで作成したIAMロールのARNを含める必要があります（上記の手順3を参照）。

     例：

```
"haParams": {
     "assumeRoleArn":
"arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}
```

+
"Cloud Volumes ONTAP APIについて説明します"

AWS のセキュリティグループルール

BlueXPでは、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を含むAWSセキュリティグループが作成されます。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 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。

インバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVPC *：インバウンドトラフィックのソースは0.0.0.0/0のIP範囲です。

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	8時80分	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	コネクタへの接続と、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	————	NFS のリモートプロシージャコール
TCP	一三九	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年	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	10、000	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	————	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年	NFS サーバデーモン

プロトコル	ポート	目的
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

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	一三七	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	一三八	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	一三九	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	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 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	UDP	一三七	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	一三八	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	一三九	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	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
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	8時80分	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128だ	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
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 ）
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）
構成のバックアップ	HTTP	8時80分	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
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

サービス	プロトコル	ポート	ソース	宛先	目的
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	一六二	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	一六二	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

HAメディエーターの事前定義されたセキュリティグループには、次のインバウンドルールが含まれています。

プロトコル	ポート	ソース	目的
TCP	3000	コネクタのCIDR	コネクタからの 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	8時80分	AWS EC2インスタンスのコネクタの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	ec2.amazonaws.com	ストレージのフェイルオーバーを支援します
UDP	53.	ec2.amazonaws.com	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構成の内部セキュリティグループに関するルール

Cloud Volumes ONTAP HA構成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。このセキュリティグループを使用すると、HAノード間、メディエーターとノード間の通信が可能になります。

BlueXPでは常にこのセキュリティグループが作成されます。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

コネクタのルール

"コネクタのセキュリティグループルールを表示します"

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。BlueXPやCloud Volumes

ONTAP と同じAWSアカウントにすることも、別のAWSアカウントに含めることもできます。

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

2. BlueXPに「a_key user__」権限を提供するIAMロールを追加して、各CMKのキーポリシーを変更します。

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

   "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。

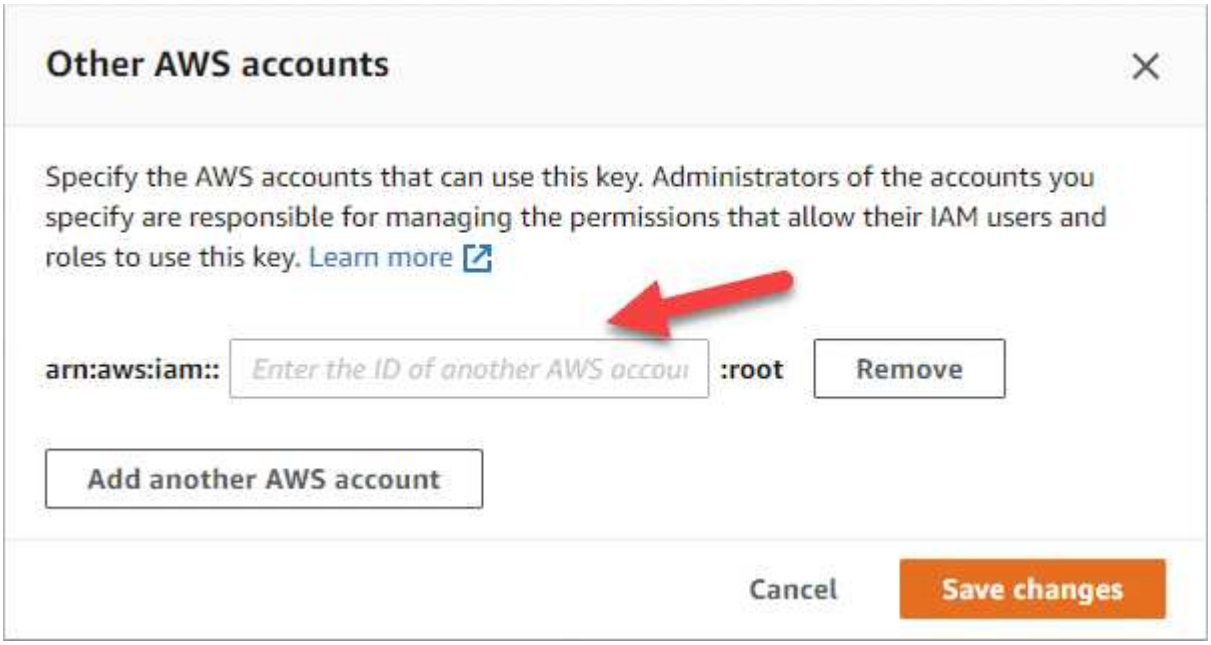
   b. キーを選択します。

   c. General configuration * ペインで、キーの ARN をコピーします。

      Cloud Volumes ONTAP システムを作成するときは、BlueXPにARNを提供する必要があります。

   d. [* Other AWS accounts （その他の**AWS**アカウント）]ペインで、BlueXP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、これはBlueXPが存在するアカウントです。BlueXPがAWSにインストールされていない場合は、BlueXPにAWSアクセスキーを提供したアカウントになります。



e. 次に、BlueXP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. このポリシーを、BlueXPに対する権限を提供するIAMロールまたはIAMユーザに関連付けます。

次のポリシーは、BlueXP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 のマニュアル：他のアカウントのユーザに KMS キーの使用を許可する"。

4. お客様が管理する CMK を使用している場合は、 Cloud Volumes ONTAP IAM ロールを a_key user_権限として追加して、 CMK のキーポリシーを変更します。

   この手順は、 Cloud Volumes ONTAP でデータの階層化を有効にし、 S3 バケットに格納されているデータを暗号化する場合に必要です。

   作業環境の作成時に IAM ロールが作成されるため、このステップの _ 導入後 _ Cloud Volumes ONTAP を実行する必要があります。（もちろん、既存の Cloud Volumes ONTAP IAM ロールを使用することもできるため、この手順を前に実行することもできます）。

   "AWS のドキュメント：「キーの編集"

Cloud Volumes ONTAP 用のIAMロールを設定します

必要な権限を持つIAMロールを各Cloud Volumes ONTAP ノードに関連付ける必要があります。HAメディエーターについても同様です。BlueXPでIAMロールを作成するのが最も簡単ですが、自分の役割を使用することもできます。

このタスクはオプションです。Cloud Volumes ONTAP 作業環境を作成する場合、デフォルトでは、BlueXPでIAMロールを作成することができます。ビジネスのセキュリティポリシーでIAMロールの作成が手動で求められる場合は、次の手順を実行します。

AWS Commercialクラウド サービス 環境でIAMロールを独自に割り当てる必要があります。"C2SにCloud Volumes ONTAP を導入する方法を学習します"。

手順

1. AWS IAMコンソールに移動します。
2. 次の権限を含むIAMポリシーを作成します。

   - Cloud Volumes ONTAP ノードのベースポリシー

標準領域

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }, {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::fabric-pool-*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（US）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-us-gov:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

C2S環境

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

- Cloud Volumes ONTAP ノードのバックアップポリシー

  Cloud Volumes ONTAP システムでBlueXPのバックアップとリカバリを使用する場合は、ノードのIAMロールに次の2つ目のポリシーを含める必要があります。

標準領域

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

GovCloud（US）リージョン

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-us-gov:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

C2S環境

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:RestoreObject",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws-iso:s3:::netapp-backup*/*",
            "Effect": "Allow"
        }
    ]
}
```

- HA メディエータ

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
                "sts:AssumeRole"
                "ec2:DescribeSubnets"
            ],
            "Resource": "*"
        }
    ]
}
```

3. IAMロールを作成し、作成したポリシーを関連付けます。

結果

新しいCloud Volumes ONTAP 作業環境を作成するときに選択できるIAMロールを設定できました。

詳細情報

- "AWSのドキュメント：「IAMポリシーの作成"
- "AWSのドキュメント：「IAMロールの作成"

AWSでCloud Volumes ONTAP のライセンスを設定

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

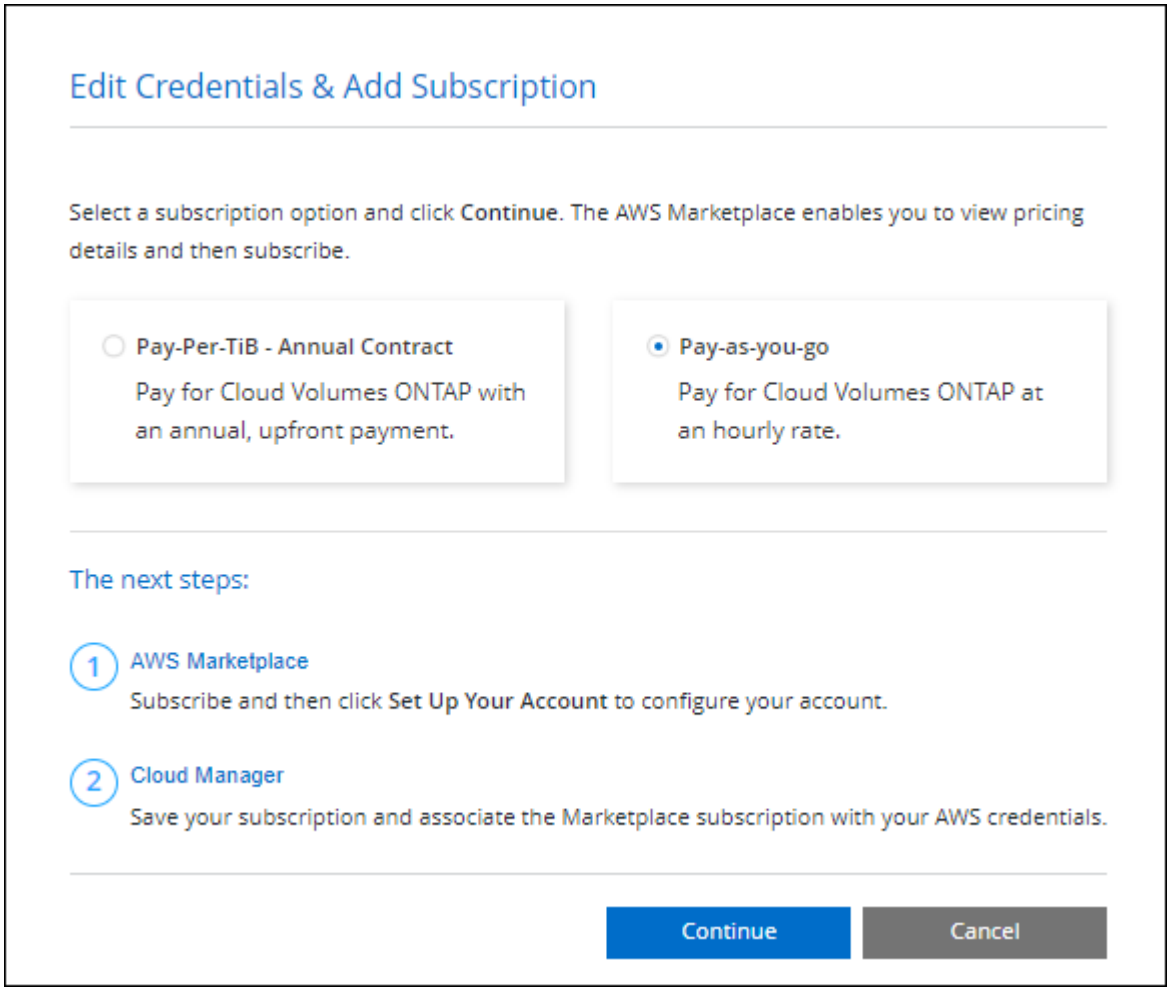
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

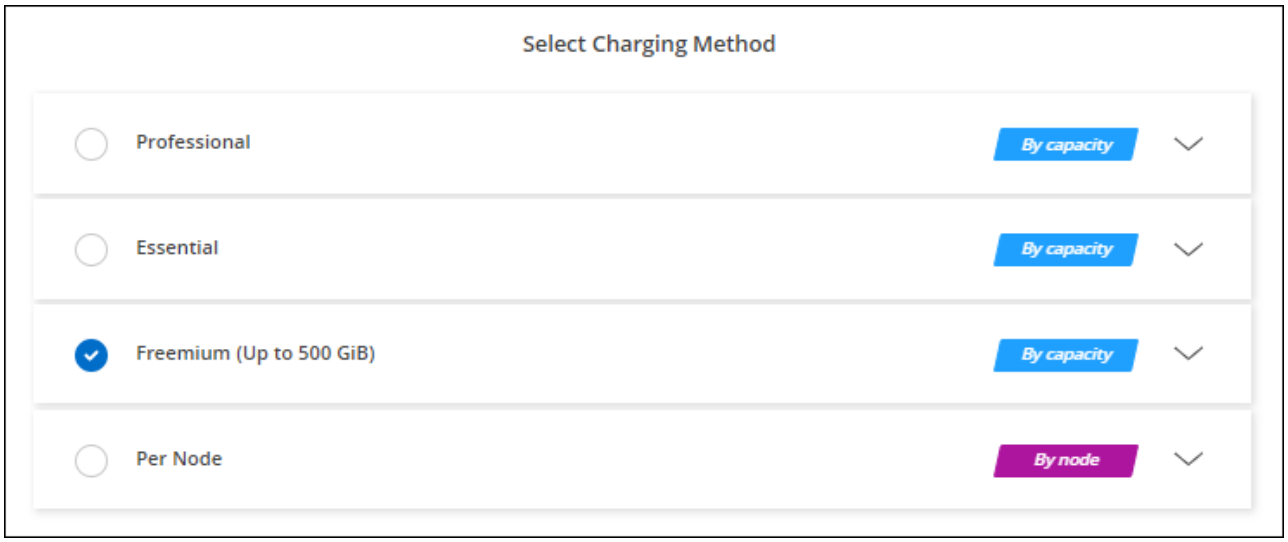
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- AWS Marketplaceで提供する従量課金制（PAYGO）の1時間単位のサブスクリプション
- AWS Marketplaceからの年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

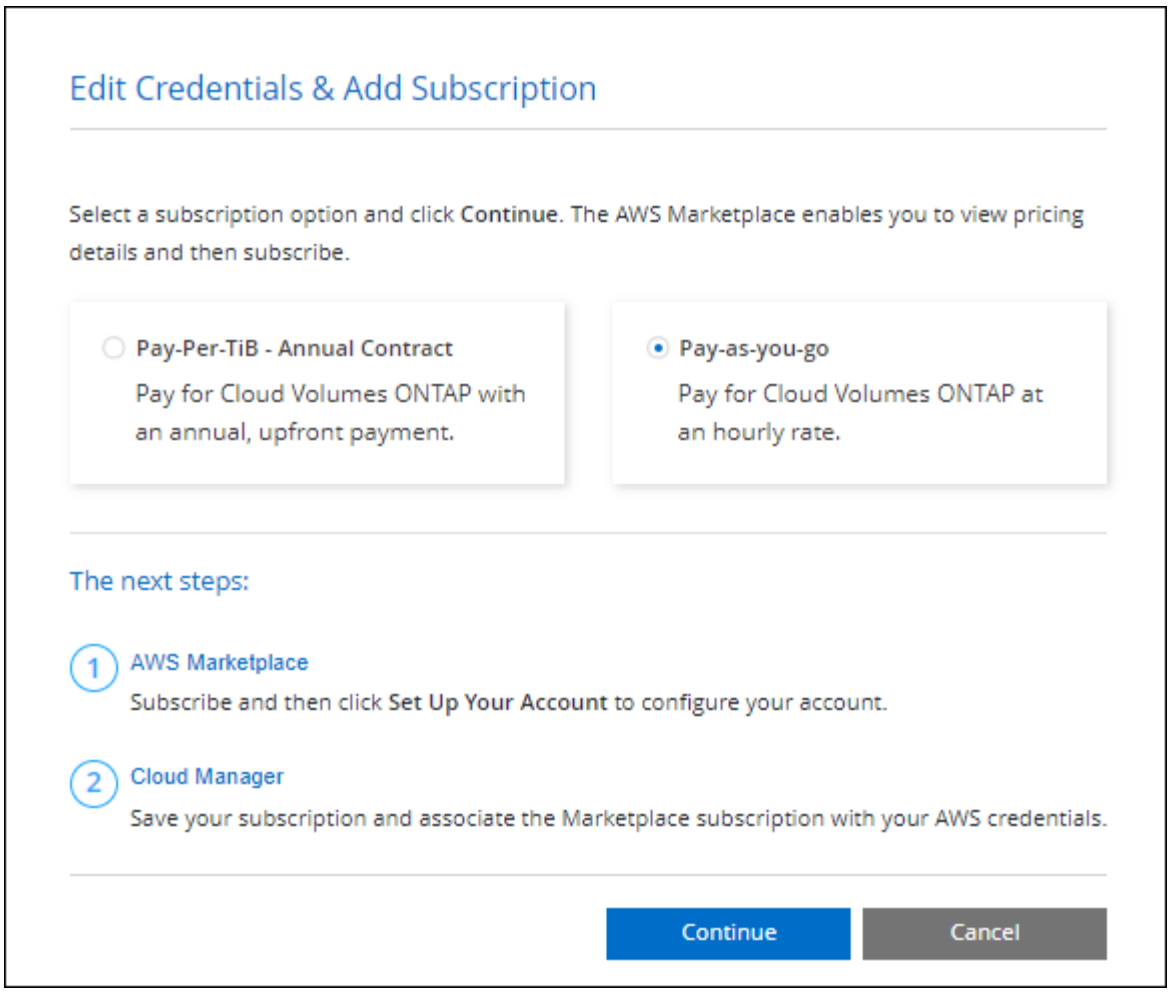
   BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

   Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

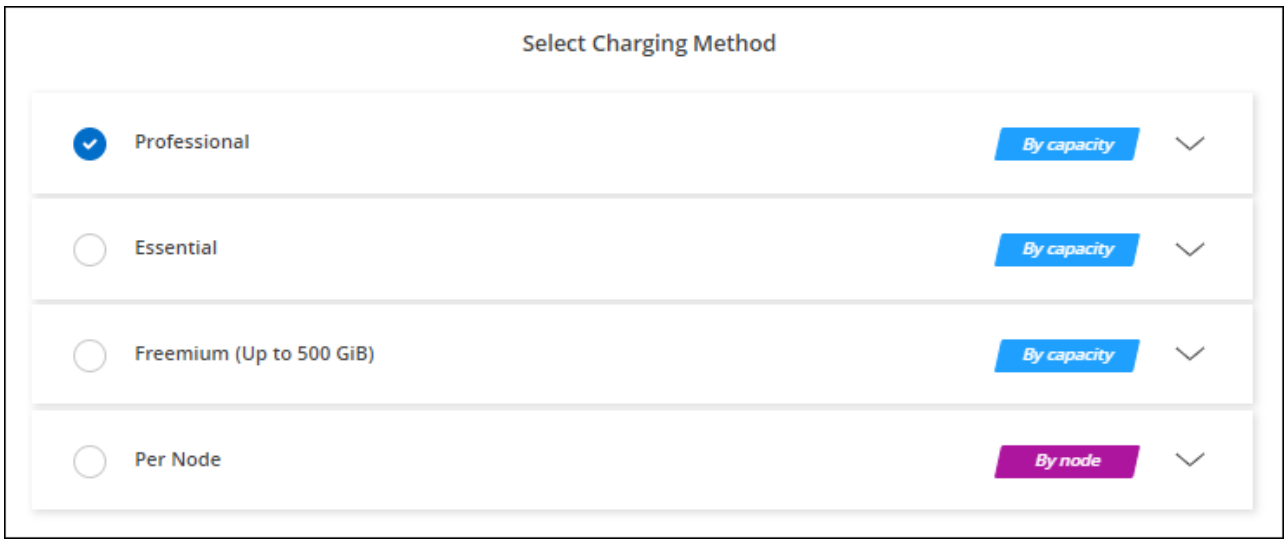
3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。



a. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

PAYGOサブスクリプション

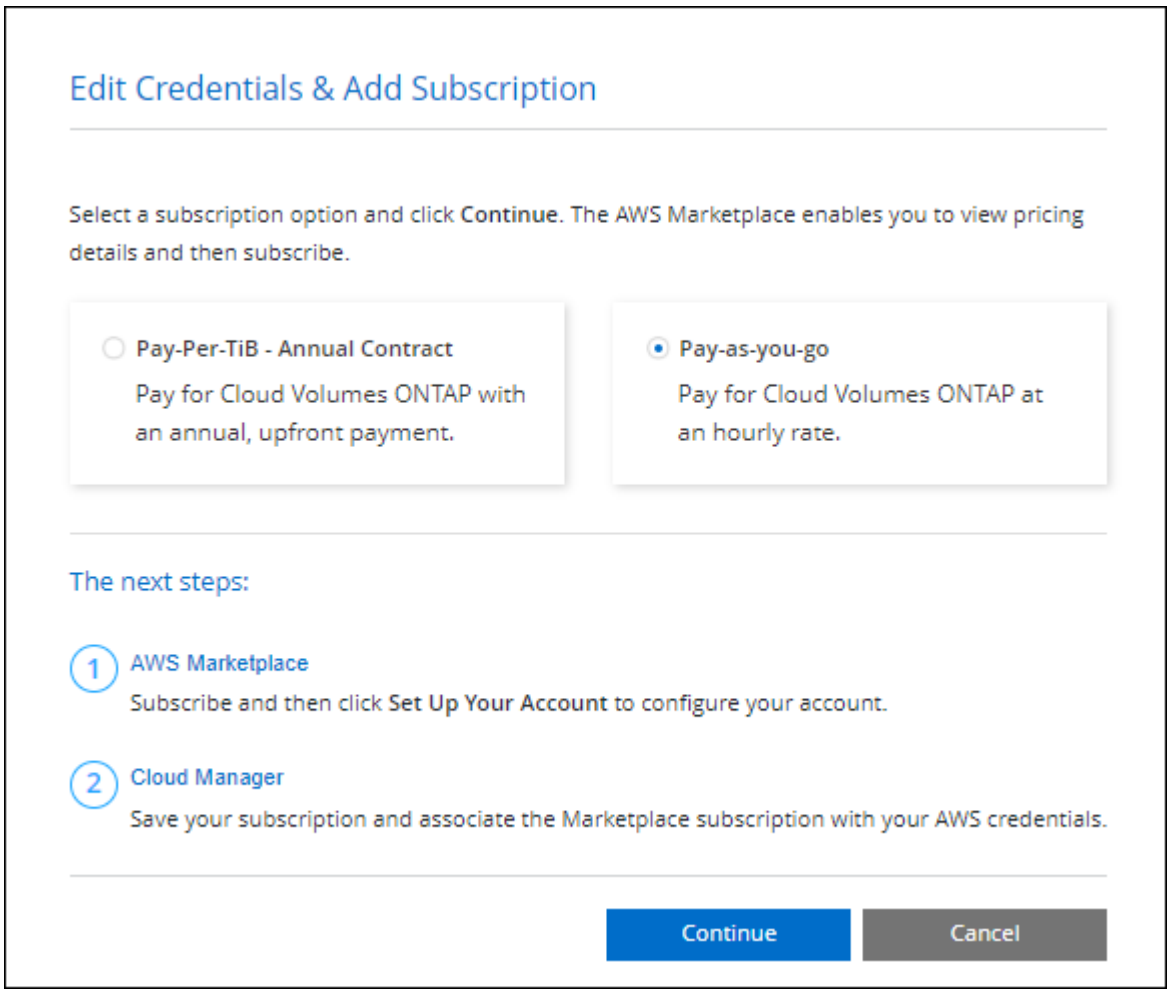
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生し

ます。

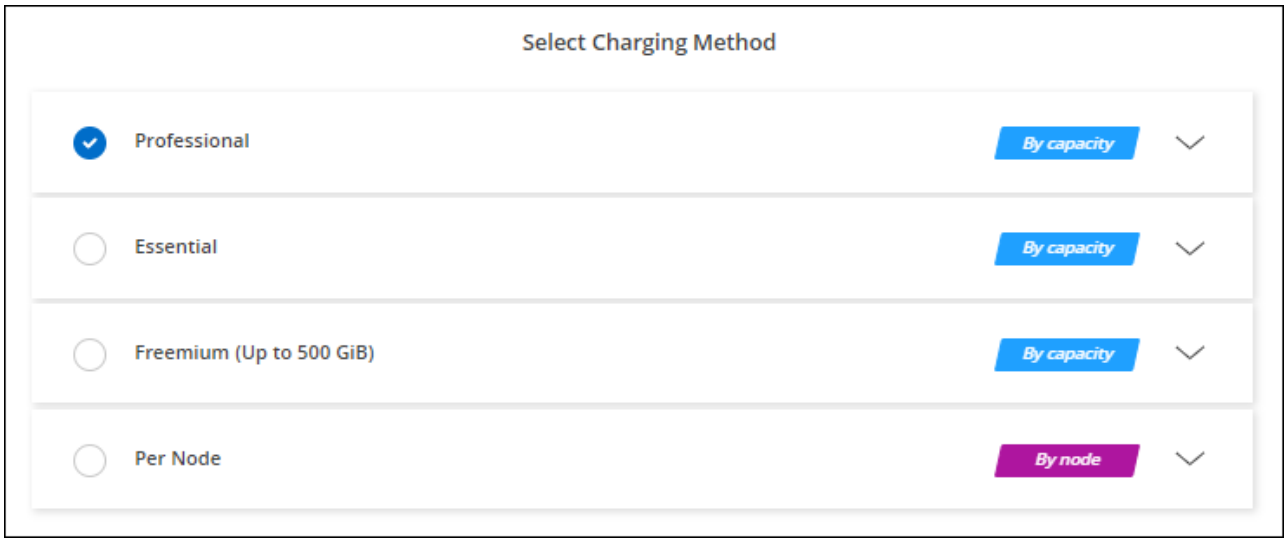
Cloud Volumes ONTAP 作業環境を作成すると、AWS Marketplaceで提供されている契約に登録するよう求めるメッセージが表示されます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで従量課金制サービスに登録します。



   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

AWSアカウントに関連付けられたAWS Marketplaceのサブスクリプションを管理するには、[設定]>[クレデンシャル]ページを使用します。 "AWSのアカウントとサブスクリプションの管理方法について説明します"

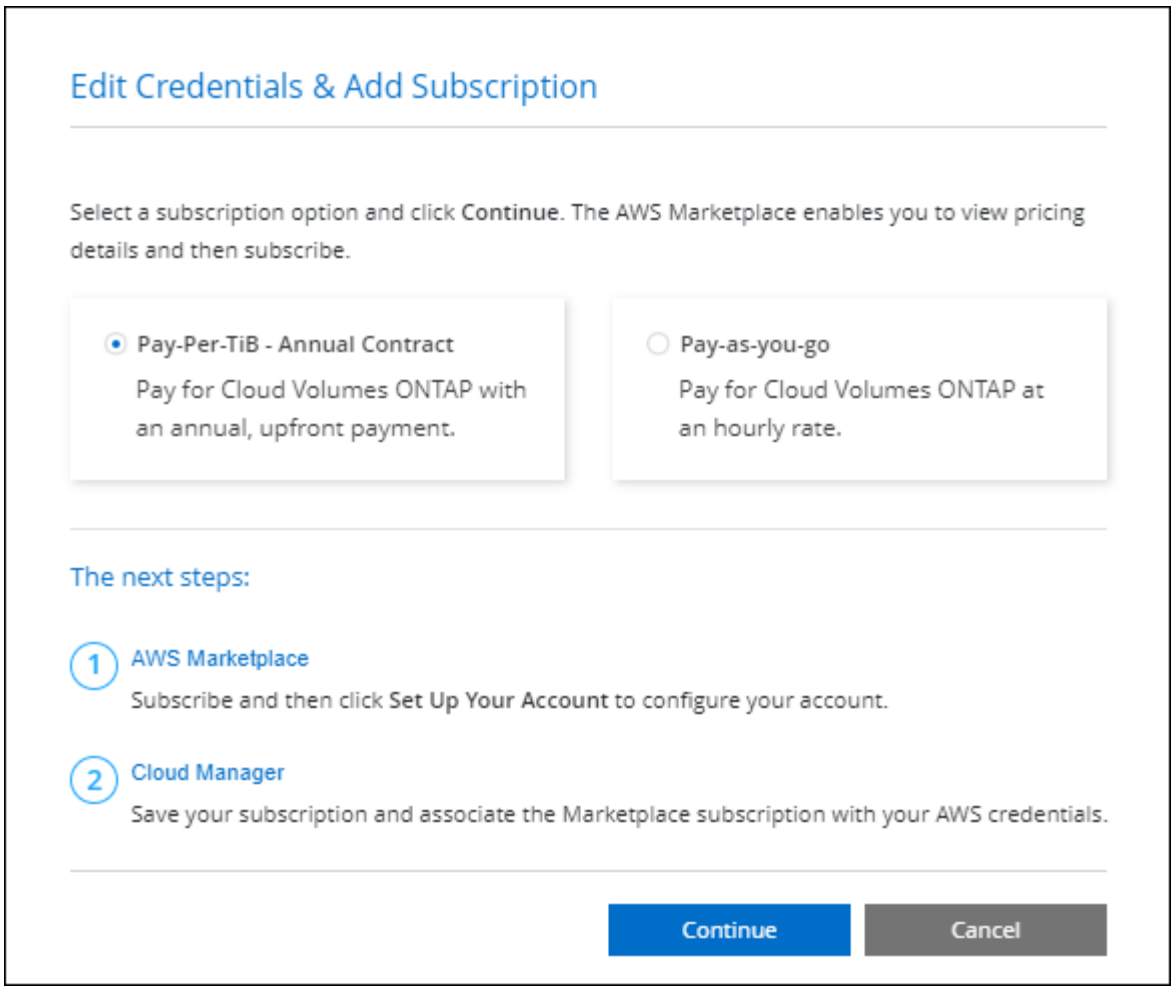
年間契約

クラウドプロバイダのマーケットプレイスから年間契約を購入することで、年間料金を支払うことができます。

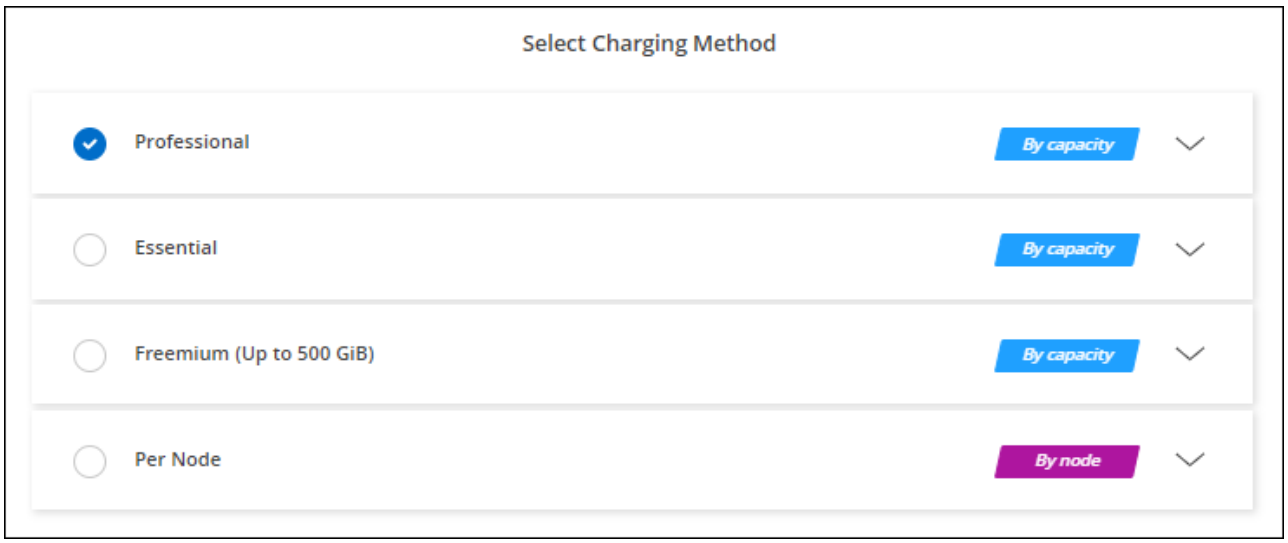
1時間単位のサブスクリプションと同様に、AWS Marketplaceで提供される年間契約にサブスクライブするよう求められます。

手順

1. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]>[サブスクリプションの追加]をクリックし、プロンプトに従ってAWS Marketplaceで年間契約をサブスクライブします。



b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

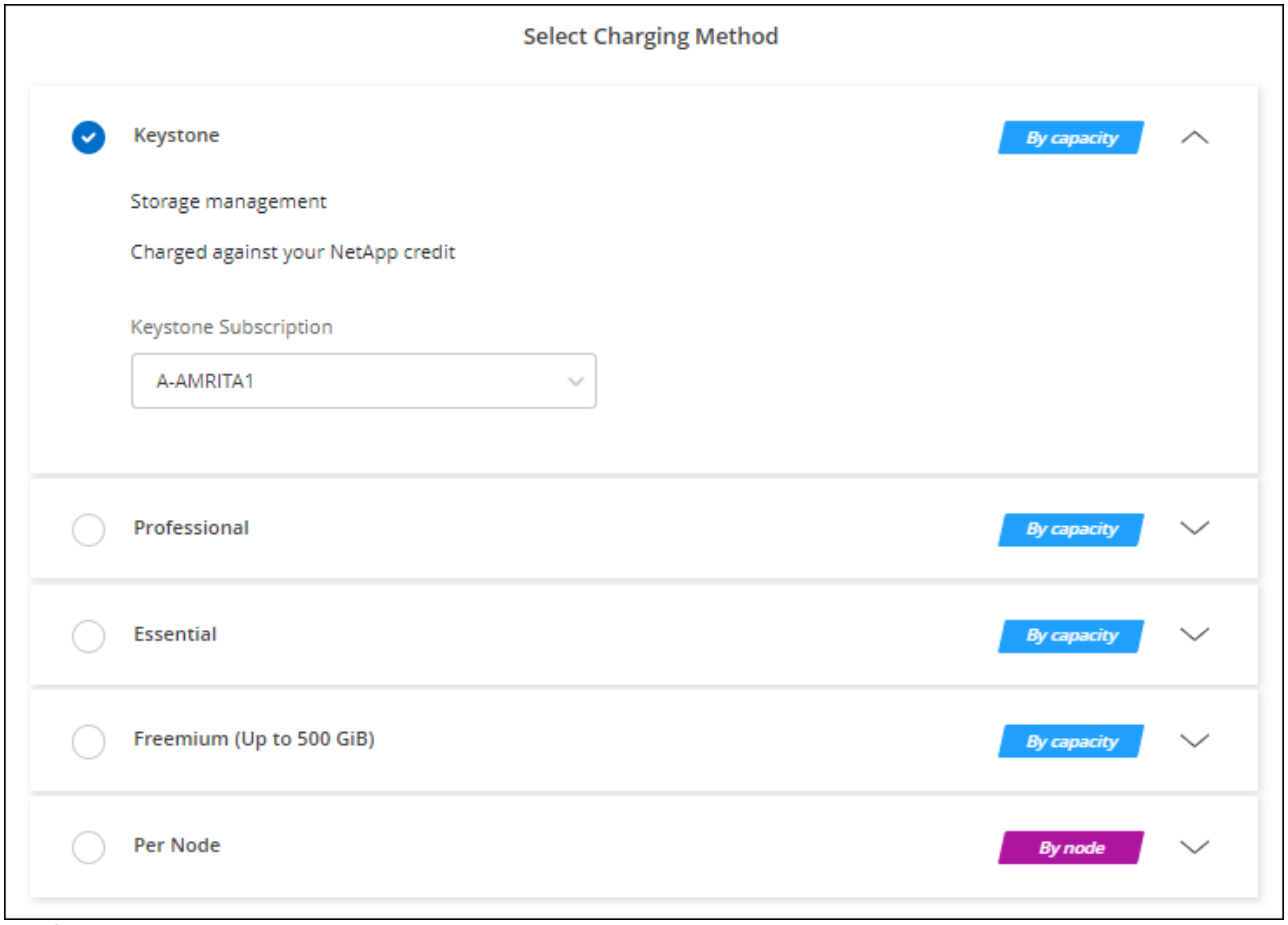
Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。

"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"ステップバイステップの手順を確認して、AWSでCloud Volumes ONTAP を起動してください"。

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。

始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
- 使用する構成についての理解。

  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"。
- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

  "ライセンスの設定方法について説明します"。
- CIFS 構成用の DNS と Active Directory

  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"。

AWS でのシングルノード Cloud Volumes ONTAP システムの起動

AWSでCloud Volumes ONTAP を起動する場合は、BlueXPで新しい作業環境を作成する必要があります

このタスクについて

作業環境を作成した直後に、指定されたVPCでテストインスタンスを起動して接続を検証します。成功すると、すぐにインスタンスが終了し、Cloud Volumes ONTAP システムの導入が開始されます。BlueXPが接続を検証できない場合は'作業環境の作成に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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. * 場所を選択 * ：「 * Amazon Web Services * 」と「 * Cloud Volumes ONTAP シングルノード * 」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. * 詳細とクレデンシャル * ：必要に応じて、 AWS のクレデンシャルと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。

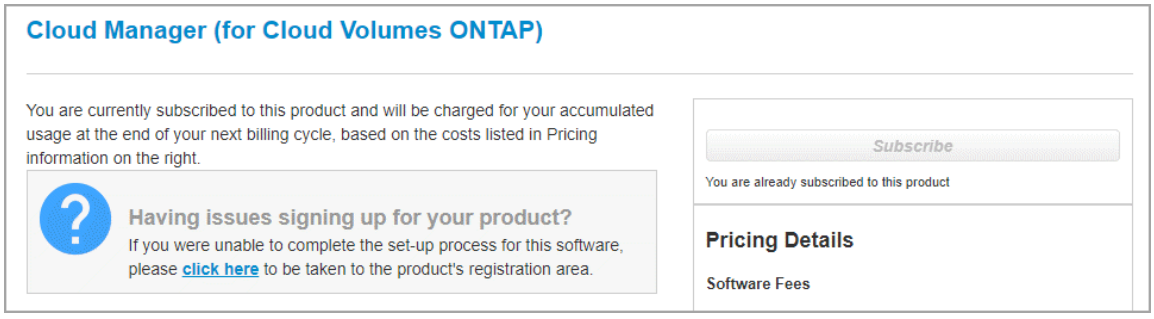
フィールド	説明
作業環境名	BlueXPでは、作業環境名を使用してCloud Volumes ONTAP システムとAmazon EC2インスタンスの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。

フィールド	説明
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。BlueXPは、Cloud Volumes ONTAP インスタンスとそのインスタンスに関連付けられている各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"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	このシステムを導入するアカウントに関連付けられている AWS クレデンシャルを選択します。この Cloud Volumes ONTAP システムで使用する AWS Marketplace サブスクリプションを関連付けることもできます。 Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。 "BlueXPにAWSクレデンシャルを追加する方法について説明します"。

次のビデオでは、従量課金制の Marketplace サブスクリプションを AWS クレデンシャルに関連付ける方法を紹介します。

► https://docs.netapp.com/ja-jp/test//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すると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。次のメッセージが表示されたら、[Click here *（ここをクリック）]リンクをクリックしてBlueXP Webサイトにアクセスし、プロセスを完了します。



6. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"

◦ "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. * 場所と接続 * ：に記録したネットワーク情報を入力します "AWS ワークシート"。

   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
vPC	AWS Outpost を使用している場合は、 Outpost VPC を選択して、その Outpost に単一のノードの Cloud Volumes ONTAP システムを導入できます。エクスペリエンスは、 AWS に存在する他の VPC と同じです。
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースは、選択したVPCのサブネット範囲と、コネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースは0.0.0.0/0のIP範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * 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"。

9. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。

   ◦ "Cloud Volumes ONTAP のライセンスオプションについて説明します"。

   ◦ "ライセンスの設定方法について説明します"。

10. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

    デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

11. 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、*構成の変更*をクリックして独自の構成を選択します。

    いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

12. **IAM**の役割: BlueXPが役割を作成できるようにするには、既定のオプションをそのまま使用することをお勧めします。

    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 ノードのポリシーの要件"。

13. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンスタイプとインスタンステナンシーを選択します。

    > 選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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。

14. 基盤となるストレージリソース：ディスクタイプを選択し、基盤となるストレージを構成して、データの階層化を有効にするかどうかを選択します。

    次の点に注意してください。

    - ディスクタイプは最初のボリューム（およびアグリゲート）用です。以降のボリューム（およびアグリゲート）には別のディスクタイプを選択できます。
    - GP3またはio1ディスクを選択した場合、BlueXPはAWSのElastic Volumes機能を使用して、必要に応じて、基盤となるストレージディスク容量を自動的に増やします。初期容量はストレージのニーズに基づいて選択し、Cloud Volumes ONTAP の導入後に変更することができます。 "Elastic VolumesのAWSサポートの詳細については、こちらをご覧ください"。
    - gp2ディスクまたはst1ディスクを選択する場合、シンプルなプロビジョニングオプションを使用する場合、初期アグリゲートおよびBlueXPで作成される追加のアグリゲートのすべてのディスクサイズを選択できます。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。
    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

      "データ階層化の仕組みをご確認ください"。

15. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 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。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレード

は、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

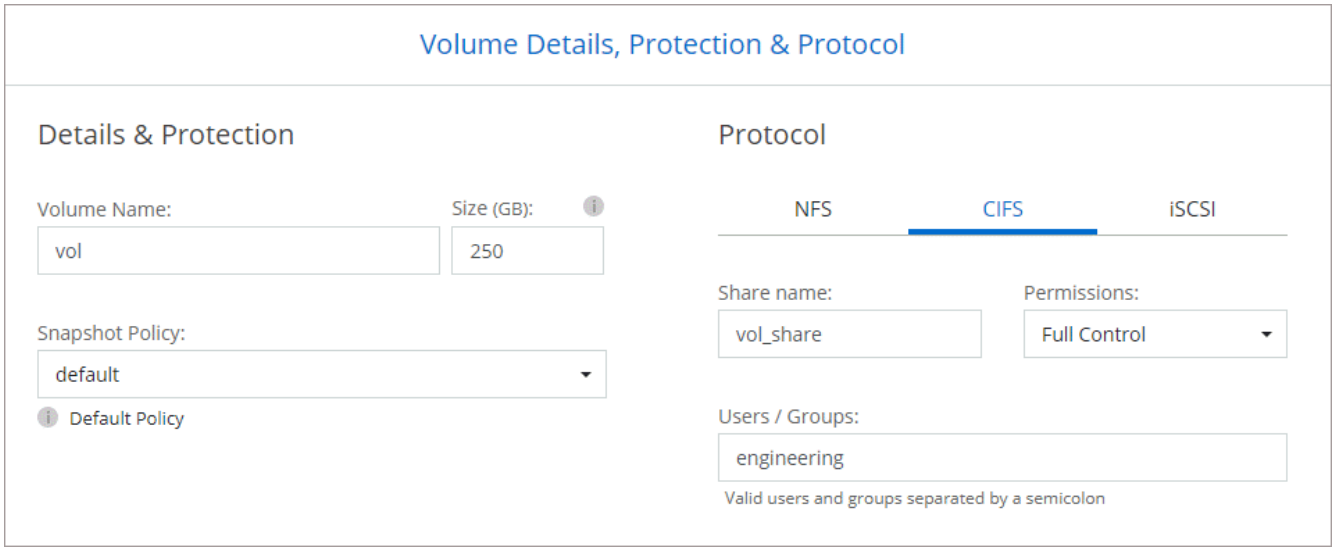
16. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

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、BlueXP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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



17. * 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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

18. * 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、ボリューム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"。

19. * 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、BlueXPが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 Volumes ONTAP インスタンスが起動します。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

AWSでCloud Volumes ONTAP HAペアを起動するには、BlueXPでHA作業環境を作成する必要があります。

制限事項

現時点では、 AWS アウトポストで HA ペアがサポートされていません。

このタスクについて

作業環境を作成した直後に、指定されたVPCでテストインスタンスを起動して接続を検証します。成功すると、すぐにインスタンスが終了し、Cloud Volumes ONTAP システムの導入が開始されます。BlueXPが接続を検証できない場合は'作業環境の作成に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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
3. 場所を選択：「* Amazon Web Services 」と「 Cloud Volumes ONTAP HA *」を選択します。
4. * 詳細とクレデンシャル * ：必要に応じて、 AWS のクレデンシャルと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。

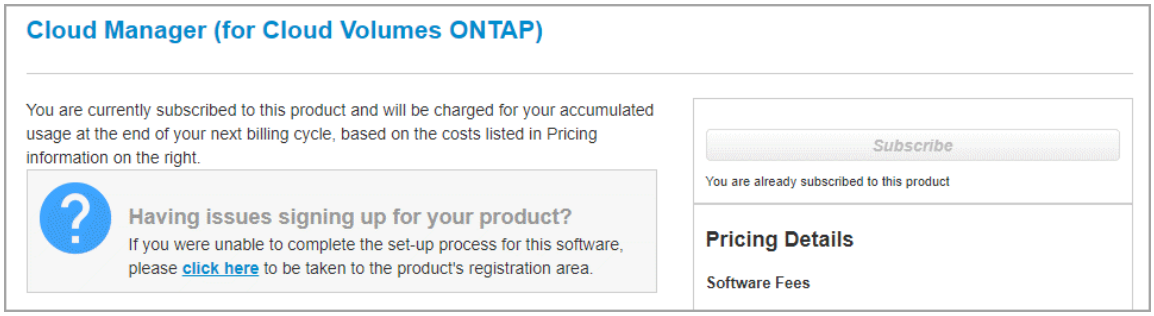
   このページの一部のフィールドは、説明のために用意されています。次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	BlueXPでは、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。BlueXPは、Cloud Volumes ONTAP インスタンスとそのインスタンスに関連付けられている各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"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する AWS クレデンシャルと Marketplace サブスクリプションを選択します。 Add Subscription * をクリックして、選択したクレデンシャルを新しい AWS Marketplace サブスクリプションに関連付けます。サブスクリプションは、年間契約の場合と、 Cloud Volumes ONTAP の料金を 1 時間ごとに支払う場合があります。 NetApp （ BYOL ）からライセンスを直接購入した場合、 AWS サブスクリプションは必要ありません。 "BlueXPにAWSクレデンシャルを追加する方法について説明します"。

次のビデオでは、従量課金制の Marketplace サブスクリプションを AWS クレデンシャルに関連付ける方法を紹介します。

► https://docs.netapp.com/ja-jp/test//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すると、次の図に示すように、 AWS Marketplace から後続のユーザに登録済みであることが通知されます。AWS_account_ のサブスクリプションが設定されている間、各 IAM ユーザは、そのサブスクリプションに自分自身を関連付ける必要があります。次のメッセージが表示されたら、[Click here *（ここをクリック）]リンクをクリックしてBlueXP Webサイトにアクセスし、プロセスを完了します。



5. * 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。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. *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"。

7. 場所と接続（単一AZ）または*リージョンとVPC *（複数のAZ）：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
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースは、選択したVPCのサブネット範囲と、コネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースは0.0.0.0/0のIP範囲になります。
既存のセキュリティグループを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * 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。

9. * 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"。

10. * 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"。

11. * 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"。

12. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。

    - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
    - "ライセンスの設定方法について説明します"。

13. * Cloud Volumes ONTAP 構成 * （ AWS Marketplace の年間契約のみ）：デフォルトの構成を確認して「 * Continue * 」をクリックするか、「 * 構成の変更 * 」をクリックして独自の構成を選択します。

    デフォルトの設定を使用している場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

14. * 構成済みパッケージ * （時間単位または BYOL のみ）： 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、 * 構成の変更 * をクリックして独自の構成を選択します。

    いずれかのパッケージを選択した場合、ボリュームを指定し、構成を確認および承認するだけで済みます。

15. **IAM**の役割: BlueXPが役割を作成できるようにするには、既定のオプションをそのまま使用することをお勧めします。

    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"。

16. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンスタイプとインスタンステナンシーを選択します。

選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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。

17. 基盤となるストレージリソース：ディスクタイプを選択し、基盤となるストレージを構成して、データの階層化を有効にするかどうかを選択します。

    次の点に注意してください。

    - ディスクタイプは最初のボリューム（およびアグリゲート）用です。以降のボリューム（およびアグリゲート）には別のディスクタイプを選択できます。
    - GP3またはio1ディスクを選択した場合、BlueXPはAWSのElastic Volumes機能を使用して、必要に応じて、基盤となるストレージディスク容量を自動的に増やします。初期容量はストレージのニーズに基づいて選択し、Cloud Volumes ONTAP の導入後に変更することができます。 "Elastic VolumesのAWSサポートの詳細については、こちらをご覧ください"。
    - gp2ディスクまたはst1ディスクを選択する場合、シンプルなプロビジョニングオプションを使用する場合、初期アグリゲートおよびBlueXPで作成される追加のアグリゲートのすべてのディスクサイズを選択できます。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。
    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

      "データ階層化の仕組みをご確認ください"。

18. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 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。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

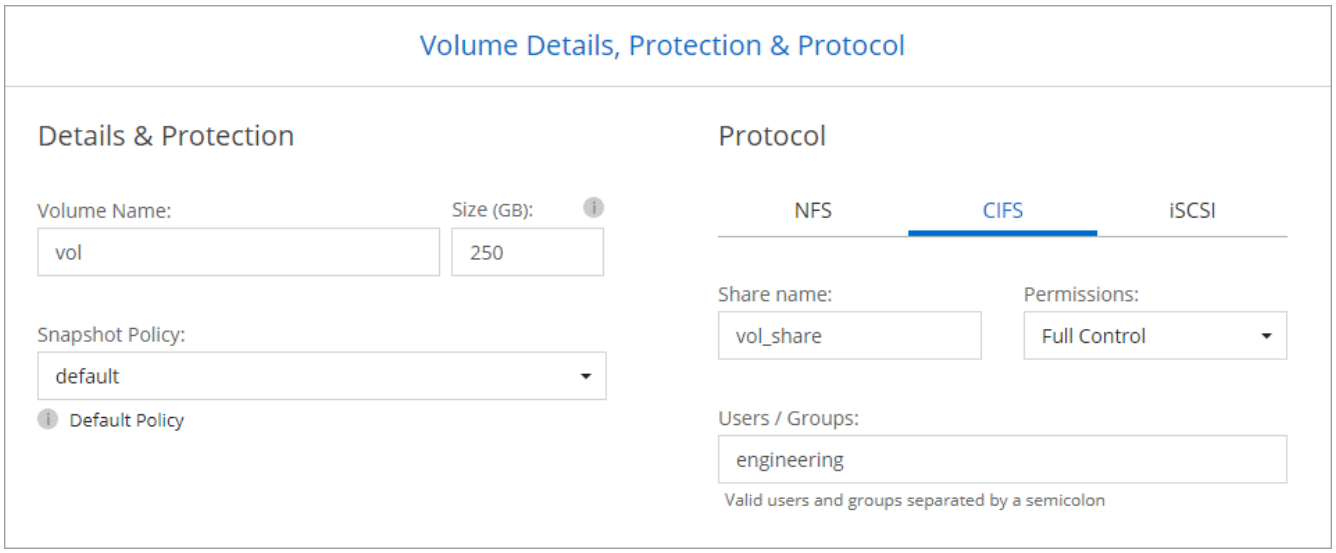
19. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    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、BlueXP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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



20. * 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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

21. * 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、ボリューム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 "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

22. * 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、BlueXPが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 Volumes ONTAP HAペアが起動します。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。

AWS C2S で Cloud Volumes ONTAP を使用する方法を確認します 環境

標準の AWS リージョンと同様に、で Cloud Manager を使用できます "AWS Commercial クラウドサービス（ C2S ）" Cloud Volumes ONTAP を導入する環境。クラウドストレージにエンタープライズクラスの機能を提供します。AWS C2S は米国に固有の閉じたリージョンですIntelligence Community 。このページの手順は、 AWS C2S リージョンユーザにのみ該当します。

C2Sでサポートされているバージョン

- Cloud Volumes ONTAP 9.8がサポートされています
- コネクタのバージョン3.9.4がサポートされています

  Connectorは、AWSでCloud Volumes ONTAP を導入して管理するために必要なソフトウェアです。Connector インスタンスにインストールされているソフトウェアから Cloud Manager にログインします。Cloud ManagerのSaaS Webサイトは、C2S環境ではサポートされていません。

> Cloud Managerの名前はBlueXPに変更されましたが、コネクタのバージョン3.9.4に含まれているユーザインターフェイスはまだCloud Managerと呼ばれるため、C2SではCloud Managerとして引き続き参照しています。

C2S でサポートされている機能

C2S 環境の Cloud Manager から使用可能な機能は次のとおりです。

- Cloud Volumes ONTAP
- データレプリケーション
- 監査のスケジュール

Cloud Volumes ONTAP の場合は、シングルノードシステムまたは HA ペアを作成できます。どちらのライセンスオプションも使用できます。従量課金制とお客様所有のライセンス（ BYOL ）です。

S3 へのデータ階層化は、 C2S の Cloud Volumes ONTAP でもサポートされています。

制限

- ネットアップのどのクラウドサービスも Cloud Manager からは使用できません。
- C2S 環境ではインターネットにアクセスできないため、次の機能も使用できません。
  - Cloud Manager からのソフトウェアの自動アップグレード
  - NetApp AutoSupport
  - AWS の Cloud Volumes ONTAP リソースのコスト情報
- Freemiumライセンスは、C2S環境ではサポートされていません。

導入の概要

C2S で Cloud Volumes ONTAP を使用するにはいくつかの手順を実行します。

1. AWS環境の準備

   これには、ネットワークの設定、 Cloud Volumes ONTAP への登録、権限の設定、および必要に応じて AWS KMS のセットアップが含まれます。

2. ConnectorのインストールとCloud Managerのセットアップ

   Cloud Manager を使用して Cloud Volumes ONTAP を導入するには、コネクタを作成する必要があります。Connector を使用すると、 Cloud Manager でパブリッククラウド環境内のリソースとプロセス（ Cloud Volumes ONTAP を含む）を管理できます。

   Connector インスタンスにインストールされているソフトウェアから Cloud Manager にログインします。

3. Cloud ManagerからCloud Volumes ONTAP を起動しています

以下に、各手順について説明します。

AWS環境の準備

AWS 環境はいくつかの要件を満たす必要があります。

ネットワークをセットアップします

Cloud Volumes ONTAP 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。

手順

1. コネクタインスタンスと Cloud Volumes ONTAP インスタンスを起動する VPC とサブネットを選択します。
2. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
3. 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。

Cloud Volumes ONTAP に登録します

Cloud Manager から Cloud Volumes ONTAP を導入するには、 Marketplace サブスクリプションが必要です。

手順

1. AWS Intelligence Community Marketplace にアクセスして、 Cloud Volumes ONTAP を検索します。
2. 導入を計画しているサービスを選択します。
3. 条件を確認し、 [**Accept**](同意する) をクリックします。
4. 導入を計画している場合は、他のサービスについても同じ手順を繰り返します。

   Cloud Volumes ONTAP インスタンスを起動するには、 Cloud Manager を使用する必要があります。Cloud Volumes ONTAP インスタンスを EC2 コンソールから起動しないでください。

権限を設定します

AWS Commercialクラウド サービス 環境でアクションを実行するために必要な権限をコネクタとCloud Volumes ONTAP に提供するIAMポリシーとロールを設定する。

次の項目について、 IAM ポリシーと IAM ロールを 1 つずつ用意する必要があります。

- コネクタインスタンス
- Cloud Volumes ONTAP インスタンス
- Cloud Volumes ONTAP HA メディエーターインスタンス （ HA ペアを導入する場合）

手順

1. AWS IAM コンソールに移動し、 * Policies * をクリックします。
2. コネクタインスタンスのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
```

```
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:ListInstanceProfiles",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
```

```
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
```

```
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

3. Cloud Volumes ONTAP のポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": "s3:ListAllMyBuckets",
        "Resource": "arn:aws-iso:s3:::*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }, {
        "Action": [
            "s3:GetObject",
            "s3:PutObject",
            "s3:DeleteObject"
        ],
        "Resource": "arn:aws-iso:s3:::fabric-pool-*",
        "Effect": "Allow"
    }]
}
```

4. Cloud Volumes ONTAP HA ペアを導入する場合は、 HA メディエーターのポリシーを作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

5. 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関連付けます。

   ポリシーと同様に、コネクタ用の IAM ロールが 1 つ、 Cloud Volumes ONTAP ノード用の IAM ロールが 1 つ、 HA メディエーター用の IAM ロールが 1 つ（ HA ペアを導入する場合）必要です。

   コネクタインスタンスを起動するときに、コネクタ IAM ロールを選択する必要があります。

   Cloud Volumes ONTAP の IAM ロールと HA メディエーターは、 Cloud Manager から Cloud Volumes ONTAP の作業環境を作成するときに選択できます。

AWS KMS を設定します

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、 AWS Key Management Service の要件を満たしていることを確認します。

手順

1. アクティブな Customer Master Key （ CMK ；カスタマーマスターキー）がアカウントまたは別の AWS アカウントに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。

2. Cloud Volumes ONTAP を導入するアカウントとは別の AWS アカウントに CMK を配置する場合は、そのキーの ARN を取得する必要があります。

   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。

3. コネクタインスタンスのIAMロールをCMKのキーユーザのリストに追加します。

   これにより、 Cloud Manager には、 Cloud Volumes ONTAP で CMK を使用する権限が与えられます。

Connectorのインストールと**Cloud Manager**のセットアップ

AWS で Cloud Volumes ONTAP システムを起動するには、まず AWS Marketplace から Connector インスタンスを起動してから、ログインして Cloud Manager をセットアップする必要があります。

手順

1. Privacy Enhanced Mail （ PEM ） Base-64 でエンコードされた X.509 形式の認証局（ CA ）が署名したルート証明書を取得する証明書を入手するには、組織のポリシーと手順を参照してください。

   セットアッププロセス中に証明書をアップロードする必要があります。Cloud Manager は、 HTTPS 経由で AWS に要求を送信する際に信頼された証明書を使用します。

2. コネクタインスタンスを起動します。
   a. AWS Intelligence Community Marketplace の Cloud Manager のページに移動します。
   b. Custom Launch タブで、 EC2 コンソールからインスタンスを起動するオプションを選択します。
   c. プロンプトに従って、インスタンスを設定します。

      インスタンスを設定する際には、次の点に注意してください。

      - t3.xlarge をお勧めします。
      - AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
      - デフォルトのストレージオプションはそのままにしておく必要があります。
      - コネクタに必要な接続方法は、 SSH 、 HTTP 、 HTTPS です。
3. コネクタインスタンスに接続されているホストから Cloud Manager をセットアップします。
   a. Web ブラウザを開き、と入力します https://ipaddress _ipaddress_は、コネクタをインストールしたLinuxホストのIPアドレスです。
   b. AWS サービスに接続するためのプロキシサーバを指定します。
   c. 手順 1 で取得した証明書をアップロードします。
   d. セットアップウィザードの手順に従って、 Cloud Manager をセットアップします。
      - * System Details * ： Cloud Manager インスタンスの名前を入力し、会社名を入力します。
      - * ユーザの作成 * ： Cloud Manager の管理に使用する管理者ユーザを作成します。
      - * レビュー * ：詳細を確認し、エンドユーザーライセンス契約を承認します。
   e. CA 署名証明書のインストールを完了するには、 EC2 コンソールからコネクタインスタンスを再起動します。
4. コネクタが再起動したら、セットアップウィザードで作成した管理者ユーザアカウントを使用してログインします。

Cloud Managerから**Cloud Volumes ONTAP** を起動しています

Cloud Manager で新しい作業環境を作成することで、 AWS Commercial クラウドサービス環境で Cloud Volumes ONTAP インスタンスを起動できます。

必要なもの

- ライセンスを購入した場合は、ネットアップから受け取ったライセンスファイルが必要です。ライセンスファイルは JSON 形式の .NLF ファイルです。
- HA メディエーターへのキーベースの SSH 認証を有効にするには、キーペアが必要です。

手順

1. 作業環境ページで、 * 作業環境の追加 * をクリックします。
2. 作成（ Create ）で、 Cloud Volumes ONTAP または Cloud Volumes ONTAP HA を選択します。
3. ウィザードの手順に従って、 Cloud Volumes ONTAP システムを起動します。

   ウィザードを完了する際には、次の点に注意してください。

   - 複数のアベイラビリティゾーンに Cloud Volumes ONTAP HA を導入する場合は、公開時点で AWS Commercial クラウドサービス環境で使用可能な AZ は 2 つだけだったため、次のように構成を導入します。
     - ノード 1 ：アベイラビリティゾーン A
     - ノード 2 ：アベイラビリティゾーン B
     - メディエーター：アベイラビリティゾーン A または B
   - 生成されたセキュリティグループを使用するには、デフォルトのオプションをそのままにしておく必要があります。

     事前定義されたセキュリティグループには、 Cloud Volumes ONTAP が正常に動作するために必要なルールが含まれています。独自の要件がある場合は、下のセキュリティグループのセクションを参照してください。

   - AWS 環境の準備の際に作成した IAM ロールを選択する必要があります。
   - 基盤となる AWS ディスクタイプは Cloud Volumes ONTAP の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。

   - AWSディスクのパフォーマンスはディスクサイズと連動します。

     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。EBS のパフォーマンスの詳細については、 AWS のドキュメントを参照してください。

   - ディスクサイズは、システム上のすべてのディスクのデフォルトサイズです。

     あとでサイズを変更する必要がある場合は、 Advanced allocation オプションを使用して、特定のサイズのディスクを使用するアグリゲートを作成できます。

   - Storage Efficiency 機能を使用すると、ストレージ利用率を高めて、必要なストレージの総容量を減らすことができます。

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。

セキュリティグループのルール

Cloud Manager で作成されるセキュリティグループには、 Cloud Manager と Cloud Volumes ONTAP がクラウドで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。テスト目的または独自のセキュリティグループを使用する場合は、ポートを参照してください。

コネクタのセキュリティグループ

コネクタのセキュリティグループには、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。

インバウンドルール

プロトコル	ポート	目的
SSH	22.	コネクタホストへの SSH アクセスを提供します
HTTP	8時80分	クライアント Web ブラウザからローカルへの HTTP アクセスを提供します ユーザインターフェイス
HTTPS	443	クライアントWebブラウザからローカルユーザインターフェイスへのHTTPSアクセスを提供します

アウトバウンドルール

コネクタの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

Cloud Volumes ONTAP のセキュリティグループ

Cloud Volumes ONTAP ノードのセキュリティグループには、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。

インバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVPC *：インバウンドトラフィックのソースは0.0.0.0/0のIP範囲です。

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

プロトコル	ポート	目的
HTTP	8時80分	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	———	NFS のリモートプロシージャコール
TCP	一三九	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年	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	10、000	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	———	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年	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

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

HA メディエーターの外部セキュリティグループ

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ソースは、コネクタが存在する VPC からのトラフィックです。

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	コネクタからの RESTful API アクセス

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

HA メディエーターの内部セキュリティグループ

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

Microsoft Azure で利用を開始しましょう

Azure での Cloud Volumes ONTAP のクイックスタート

いくつかの手順で、 Cloud Volumes ONTAP for Azure を使い始めましょう。

コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "Azure でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"

構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。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。 "詳細はこちら。"。

ネットワークをセットアップします

1. VNet とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートすることを確認します。
2. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

   インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

"ネットワーク要件の詳細については、こちらをご覧ください"。

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

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからコネクタを作成しています"
- "Azure Marketplace からコネクタを作成する"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPが権限を持って実行できること"

AzureでCloud Volumes ONTAP 構成を計画

Azure で 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、または独自の設定を作成できます。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。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP は、ほとんどの Microsoft Azure リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

サポートされている**VM**タイプを選択してください

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数の VM タイプがサポートされます。

"Azure で Cloud Volumes ONTAP がサポートされている構成"

ストレージの制限を確認

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。

"Azure での Cloud Volumes ONTAP のストレージの制限"

Azureでシステムのサイズを設定します

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"

シングルノードシステムの**Azure**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。

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。）

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：「 What disk types are available in Azure ？」"。

Azureの**HA**ペア構成のディスクタイプ

HAシステムでは、Premium SSD Shared Managed Disksを使用して、I/O負荷の高いワークロードのパフォーマンスを高コストで実現します。9.12.1リリースより前に作成されたHA配置では、Premiumページブロブが使用されます。

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。BlueXPでは、このディスクサイズを最初のアグリゲート、およびシンプルなプロビジョニングオプションを使用したときに作成される追加のアグリゲートに使用します。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 TiB のディスクを選択すると、 500 GiB 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"

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

"Azure で、 Cloud Volumes ONTAP システムデータのデフォルトディスクを表示します"。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

ネットワーク情報を収集

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）	

書き込み速度を選択します

BlueXPでは、Cloud Volumes ONTAP 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。 "書き込み速度の詳細については、こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

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。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または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。

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 の要件

Azure では、次のネットワーク要件を満たしている必要があります。

アウトバウンドインターネットアクセス

Cloud Volumes ONTAP ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

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

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で_OUTBOUND接続を許可する必要もあります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

IP アドレス

BlueXPは、必要な数のプライベートIPアドレスを自動的にAzureのCloud Volumes ONTAP に割り当てます。ネットワークに利用可能な十分な数のプライベートIPアドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。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。

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

シングルノードシステムの IP アドレス

BlueXPは'1つのノードシステムに5つまたは6つのIPアドレスを割り当てます

- クラスタ管理IP
- ノード管理IP
- SnapMirror用のクラスタ間IP

- NFS / CIFS IP
- iSCSI IP

> iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- SVMの管理（オプション-デフォルトでは設定されていません）

HA ペアの **IP** アドレス

BlueXPでは、導入時に1ノードあたり4 NICにIPアドレスが割り当てられています。

BlueXPでは、HAペアに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には作成されません。

- NIC0*
- ノード管理IP
- クラスタ間IP
- iSCSI IP

> iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- NIC1*
- クラスタネットワークIP
- NIC2 *
- クラスタインターコネクトIP（HA IC）

NIC3

- Pageblob NIC IP (ディスクアクセス)

> NIC3は、ページBLOBストレージを使用するHA環境にのみ適用できます。

上記のIPアドレスは、フェイルオーバーイベントの際に移行されません。

また、4つのフロントエンドIP（FIPS）がフェイルオーバーイベント時に移行するように設定されています。これらのフロントエンドIPはロードバランサに存在します。

- クラスタ管理IP
- nodeAデータIP（NFS / CIFS）
- nodeBデータIP（NFS / CIFS）
- SVM管理IP

Azure サービスへのセキュアな接続

BlueXPでは、Cloud Volumes ONTAP とAzureページBLOBストレージアカウント間の接続用にAzure Private Linkがデフォルトで有効になっています。

ほとんどの場合、必要な操作は何もありません。BlueXPはAzure Private Linkを管理します。ただし、 Azure プライベート DNS を使用している場合は、構成ファイルを編集する必要があります。また、Azureのコネクタの場所に関する要件も把握しておく必要があります。

ビジネスニーズに応じて、プライベートリンク接続を無効にすることもできます。リンクを無効にすると、Cloud Volumes ONTAP はサービスエンドポイントを使用するように設定されます。

"Azureプライベートリンクまたはサービスエンドポイントでの Cloud Volumes ONTAP を使用する方法の詳細については、こちらをご覧ください"。

他の ONTAP システムへの接続

Azure内のCloud Volumes ONTAP システムと他のネットワーク内のONTAP システム間でデータをレプリケートするには、企業ネットワークなど、Azure VNetとその他のネットワーク間に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"。

HA インターコネクトのポート

Cloud Volumes ONTAP HA ペアには HA インターコネクトが含まれています。 HA インターコネクトを使用すると、各ノードはパートナーが機能しているかどうかを継続的に確認し、パートナーの不揮発性メモリのログデータをミラーリングできます。HA インターコネクトは、通信に TCP ポート 10006 を使用します。

デフォルトでは、 HA インターコネクト LIF 間の通信は開いており、このポートにはセキュリティグループのルールはありません。ただし、 HA インターコネクト LIF の間にファイアウォールを作成する場合は、 HA ペアが適切に動作するように、ポート 10006 の TCP トラフィックが開いていることを確認する必要があります。

Azure リソースグループには HA ペアが 1 つしかありません

Azure に導入する Cloud Volumes ONTAP HA ペアごとに、 _dedicated_resource グループを使用する必要があります。リソースグループでサポートされる HA ペアは 1 つだけです。

Azureリソースグループに2つ目のCloud Volumes ONTAP HAペアを導入しようとすると、接続の問題が発生します。

セキュリティグループのルール

BlueXPでは、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を含むAzureセキュリティグループが作成されます。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 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。

コネクタに関する情報をお探しですか？ "コネクタのセキュリティグループルールを表示します"

シングルノードシステムのインバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VNet**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVNet *：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。

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	8時80分 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	ーーー TCP	Any から Any	NFS のリモートプロシージャコール
1003 Inbound_111_UDP	ーーー UDP	Any から Any	NFS のリモートプロシージャコール
1004 Inbound_139	一三九 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
2006 年 10 月 Inbound_161-162_UDP	161-162 UDP	Any から Any	簡易ネットワーク管理プロトコル
1007 INBOUND _ 443	443年 TCP	Any から Any	コネクタへの接続と、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 の場合	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年 TCP	Any から Any	NFS サーバデーモン

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
一 〇 一三 Inbound_2049 _UDP	2049年 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
1015 INBOUND _4045-4046_tcp のようになりました	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 です	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	10、000 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
65、000 AllowVnetInBound のことです	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 の 2 つの機能があります	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

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VNet**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVNet *：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。

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です INBOUND _ 443	443年 任意のプロトコル	Any から Any	コネクタへの接続と、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です INBOUND _111_TCP	ーーー 任意のプロトコル	Any から Any	NFS のリモートプロシージャコール
一 〇 二 INBOUND _2049 _TCP	2049年 任意のプロトコル	Any から Any	NFS サーバデーモン
ーーー inbound_ssh	22. 任意のプロトコル	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
一二一 Inbound_53	53. 任意のプロトコル	Any から Any	DNS と CIFS
65、000 AllowVnetInBound のことです	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 の 2 つの機能があります	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

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
	一三七	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	一三八	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
	一三九	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 および UDP	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 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	一三七	UDP	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	一三八	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
	一三九	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 および UDP	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 ）

サービス	ポート	プロトコル	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	8時80分	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128だ	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
構成のバックアップ	HTTP	8時80分	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
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
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
	一六二	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
	一六二	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

コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "Azureのセキュリティグループルール"

Azure でお客様が管理するキーを使用するように Cloud Volumes ONTAP を設定します

データは、を使用して Azure の Cloud Volumes ONTAP で自動的に暗号化されます "Azure Storage Service Encryption の略" Microsoft が管理するキーを使用する場合：ただし、このページの手順に従って独自の暗号化キーを使用することもできます。

データ暗号化の概要

Cloud Volumes ONTAP データは、を使用して Azure で自動的に暗号化されます "Azure Storage Service Encryption の略"。デフォルトの実装では、 Microsoft が管理するキーが使用されます。セットアップは必要ありません。

Cloud Volumes ONTAP で顧客管理キーを使用する場合は、次の手順を実行する必要があります。

1. Azure で、キーヴォールトを作成し、そのヴォールトでキーを生成します
2. BlueXPから'APIを使用して'キーを使用するCloud Volumes ONTAP 作業環境を作成します

キーローテーション

キーの新しいバージョンを作成すると、 Cloud Volumes ONTAP では自動的に最新のキーバージョンが使用されます。

データの暗号化方法

お客様が管理するキーを使用するように設定された Cloud Volumes ONTAP 作業環境を作成すると、 Cloud Volumes ONTAP データは次のように暗号化されます。

Azure HAの複数のアベイラビリティゾーン

- Cloud Volumes ONTAP 用のすべてのAzureストレージアカウントは、お客様が管理するキーを使用して暗号化されます。^1
- ルート、ブート、NVRAM、コア、データディスクの場合、BlueXPはディスク暗号化セットを使用します。これにより、管理対象ディスクで暗号化キーを管理できます。
- 新しいデータディスクでも同じディスク暗号化セットが使用されます。

Azure HAシングルアベイラビリティゾーン

- Cloud Volumes ONTAP 用のすべてのAzureストレージアカウントは、お客様が管理するキーを使用して暗号化されます。^1
- 新しいストレージアカウント（ディスクやアグリゲートを追加する場合など）も同じキーを使用します。^ 1^
- ONTAP 9.10.1P3以降では、NVRAMおよびコアディスクの場合、BlueXPはを使用します "ディスク暗号化セット"を使用して、管理対象ディスクで暗号化キーを管理できます。下位バージョンでは、顧客管理キーの代わりにMicrosoft管理キーが使用されます。

シングルノード

- Cloud Volumes ONTAP 用のすべての Azure ストレージアカウントは、お客様が管理するキーを使用して暗号化されます。^1 ^
- ルートディスク、ブートディスク、データディスクの場合、BlueXPはを使用します "ディスク暗号化セット"を使用して、管理対象ディスクで暗号化キーを管理できます。

- 新しいデータディスクでも同じディスク暗号化セットが使用されます。
- ONTAP 9.9.2.1P7から、NVRAMおよびコアディスクに対して、BlueXPはディスク暗号化セットを使用します。これにより、管理対象ディスクで暗号化キーを管理できるようになります。下位バージョンでは、顧客管理キーの代わりにMicrosoft管理キーが使用されます。

脚注

1. 作成時にストレージアカウントを暗号化する場合は、CVO作成要求でリソースのIDを作成して指定する必要があります。これは、すべてのタイプの導入に当てはまります。提供しない場合でもストレージアカウントは暗号化されますが、BlueXPはまずMicrosoftが管理するキー暗号化を使用してストレージアカウントを作成し、次にストレージアカウントを更新してお客様が管理するキーを使用するようにします。

ユーザーが割り当てた管理**ID**を作成します

ユーザーが割り当てた管理IDと呼ばれるリソースを作成することもできます。これにより、Cloud Volumes ONTAP作業環境の作成時にストレージアカウントを暗号化できます。キーボールトを作成してキーを生成する前に、このリソースを作成することをお勧めします。

リソースのIDは次のとおりです。 `userassignedidentity`。

手順

1. Azureで、Azureサービスに移動し、* Managed Identities *を選択します。
2. [作成（ Create ）] をクリックします。
3. 次の詳細を入力します。
   - サブスクリプション:サブスクリプションを選択します。コネクタサブスクリプションと同じサブスクリプションを選択することをお勧めします。
   - リソースグループ：既存のリソースグループを使用するか、新しいリソースグループを作成します。
   - リージョン：必要に応じて、コネクタと同じリージョンを選択します。
   - 名前:リソースの名前を入力します。
4. 必要に応じて、タグを追加します。
5. [作成（ Create ）] をクリックします。

キーボールトを作成し、キーを生成します

キーヴォールトは、 Cloud Volumes ONTAP システムを作成するときと同じ Azure サブスクリプションとリージョンに配置する必要があります。

あなたの場合 ユーザーが割り当てた管理IDを作成しました、キーヴォールトの作成時に、キーヴォールトのアクセスポリシーも作成する必要があります。

手順

1. "Azure サブスクリプションでキーヴォールトを作成します"。

   キーヴォールトの次の要件に注意してください。

   - キーヴォールトは、 Cloud Volumes ONTAP システムと同じリージョンに配置する必要があります。
   - 次のオプションを有効にする必要があります。

- * Soft -delete * （このオプションはデフォルトで有効ですが、 DISABLE_NOT BE 無効にする必要があります）
- * パージ保護 *
- * Azure Disk Encryption for Volume Encryption *（シングルノードシステムの場合、または複数のゾーンのHAペアの場合）

◦ ユーザが割り当てた管理IDを作成した場合は、次のオプションを有効にする必要があります。

- バックアップアクセスポリシー

2. バックアップアクセスポリシーを選択した場合は、[作成]をクリックしてキーバックアップのアクセスポリシーを作成します。そうでない場合は、手順3に進みます。
   a. 次の権限を選択します。
      - 取得
      - リスト
      - 復号化します
      - 暗号化
      - キーのラップを解除します
      - ラップキー
      - 検証
      - サインだ
   b. ユーザーが割り当てた管理ID（リソース）をプリンシパルとして選択します。
   c. アクセスポリシーを確認して作成します。
3. "キーボールトでキーを生成します"。

   キーに関する次の要件に注意してください。

   ◦ キータイプは * rsa * である必要があります。
   ◦ 推奨される RSA キー・サイズは **2048** ですが、それ以外のサイズもサポートされます。

暗号化キーを使用する作業環境を作成します

キーヴォールトを作成して暗号化キーを生成したら、そのキーを使用するように設定した新しい Cloud Volumes ONTAP システムを作成できます。これらの手順は、BlueXP APIを使用してサポートされています。

必要な権限

シングルノードのCloud Volumes ONTAP システムで顧客管理キーを使用する場合は、BlueXP Connectorに次の権限があることを確認します。

```
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.Compute/diskEncryptionSets/delete"
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"権限の最新のリストを表示します"

手順

1. 次のBlueXP API呼び出しを使用して、Azureサブスクリプション内の主要なボルトのリストを取得します。

   HA ペアの場合： `GET /azure/ha/metadata/vaults`

   シングルノードの場合： `GET /azure/vsa/metadata/vaults`

   - name * および * resourcegroup * をメモします。次の手順でこれらの値を指定する必要があります。

   "この API 呼び出しの詳細を確認してください"。

2. 次のBlueXP API呼び出しを使用して、ボルト内のキーのリストを取得します。

   HA ペアの場合： `GET /azure/ha/metadata/keys-vault`

   シングルノードの場合： `GET /azure/vsa/metadata/keys-vault`

   - keyName * をメモします。次のステップで、その値（ボルト名とともに）を指定する必要があります。

   "この API 呼び出しの詳細を確認してください"。

3. 次のBlueXP API呼び出しを使用してCloud Volumes ONTAP システムを作成します

   a. HA ペアの場合：

      `POST /azure/ha/working-environments`

      要求の本文には次のフィールドを含める必要があります。

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

      を含めます `"userAssignedIdentity": " userAssignedIdentityId"` フィールド：ストレージアカウントの暗号化に使用するリソースを作成した場合。

"この API 呼び出しの詳細を確認してください"。

b. シングルノードシステムの場合：

```
POST /azure/vsa/working-environments
```

要求の本文には次のフィールドを含める必要があります。

```
"azureEncryptionParameters": {
                "key": "keyName",
                "vaultName": "vaultName"
}
```

を含めます "userAssignedIdentity": " userAssignedIdentityId" フィールド：ストレージアカウントの暗号化に使用するリソースを作成した場合。

"この API 呼び出しの詳細を確認してください"。

結果

新しい Cloud Volumes ONTAP システムで、お客様が管理するキーを使用してデータを暗号化するように設定しておきます。

AzureでCloud Volumes ONTAP のライセンスをセットアップする

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

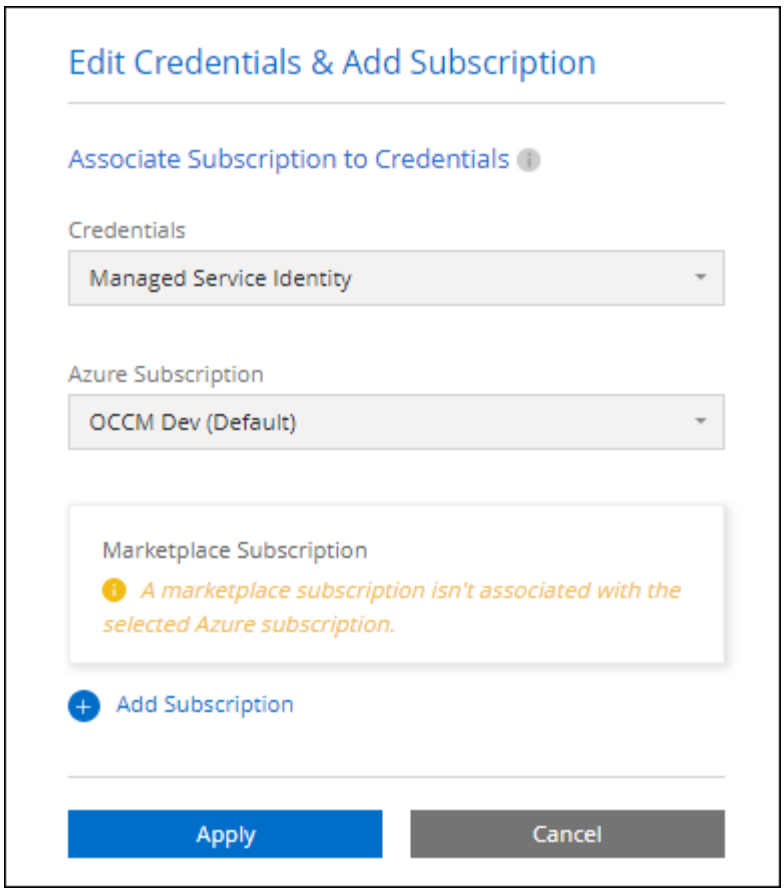
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

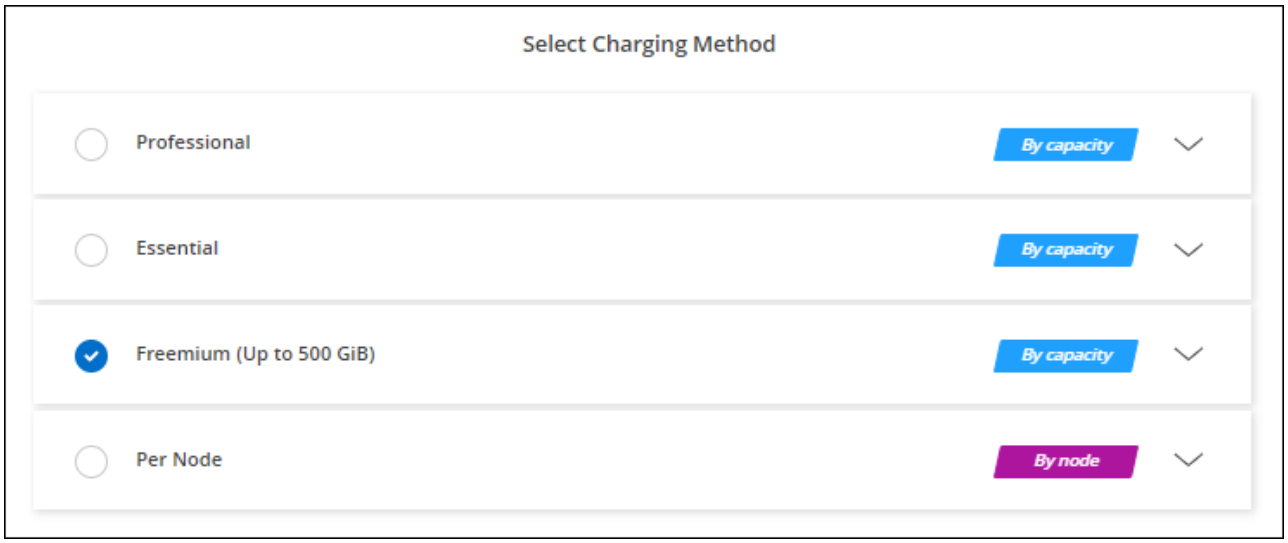
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

      プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- Azure Marketplaceからの従量課金制（PAYGO）単位のサブスクリプション
- 年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

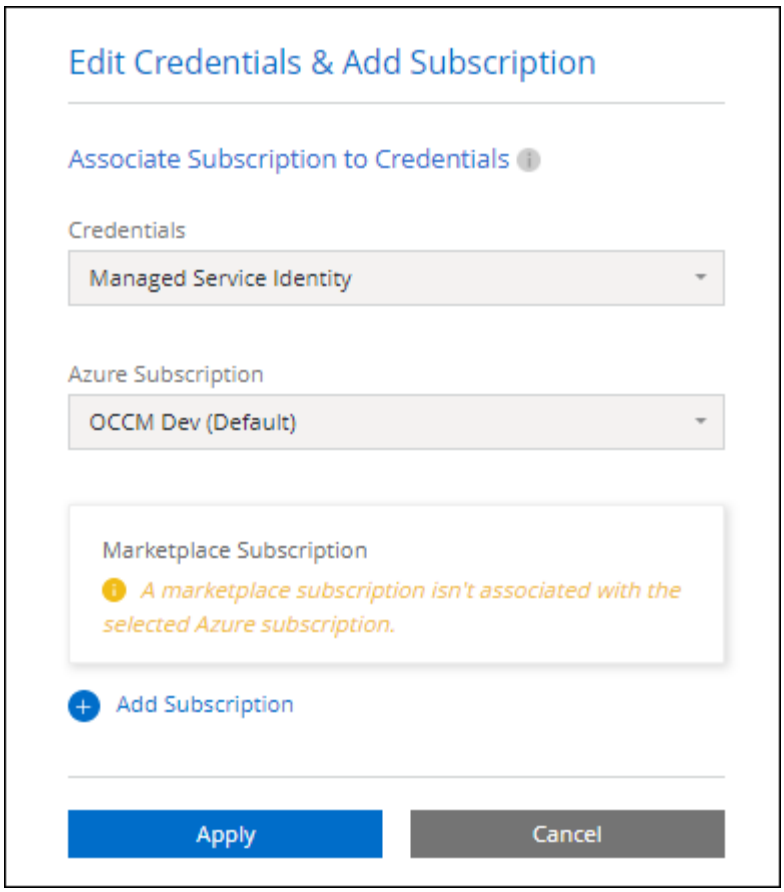
   BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

   Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

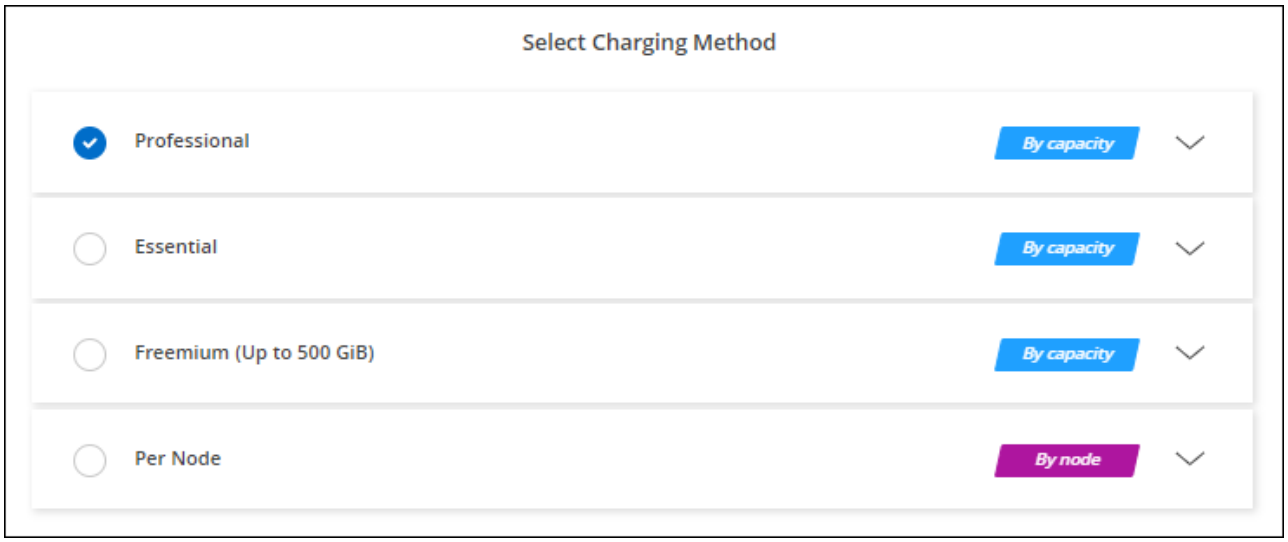
3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。



a. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

PAYGOサブスクリプション

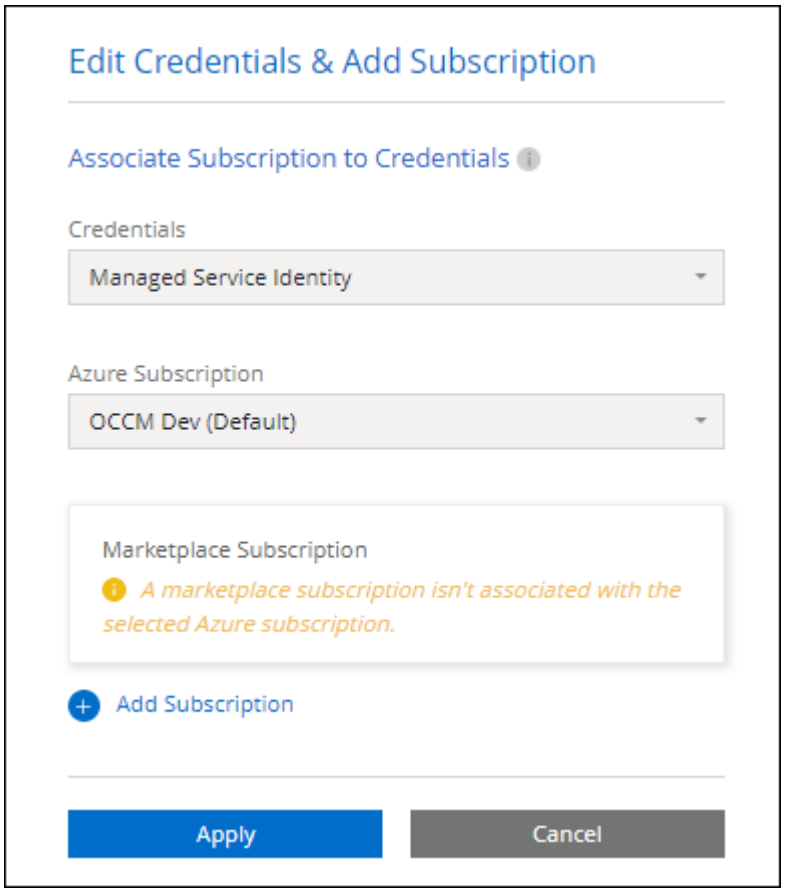
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

Cloud Volumes ONTAP 作業環境を作成すると、Azure Marketplaceで提供されている契約に登録するよう求め

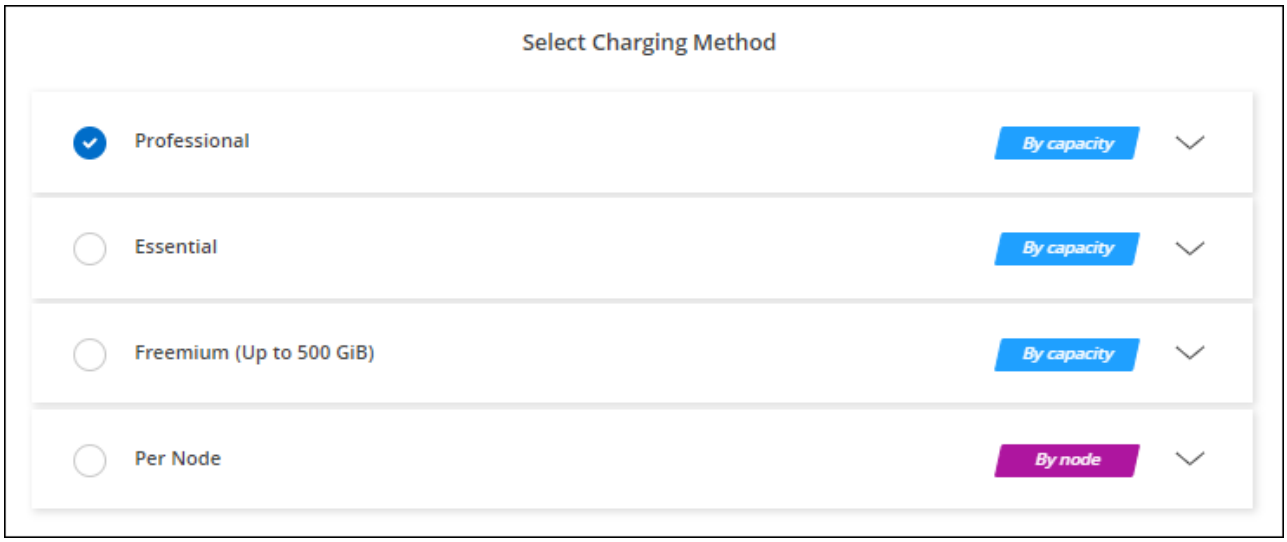
られます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。



   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Azureアカウントに関連付けられたAzure Marketplaceのサブスクリプションを管理するには、[設定]>[クレデンシャル]ページを使用します。 "Azureのアカウントとサブスクリプションの管理方法について説明します"

年間契約

年間契約を購入することで、Cloud Volumes ONTAP の年間料金をお支払いいただけます。

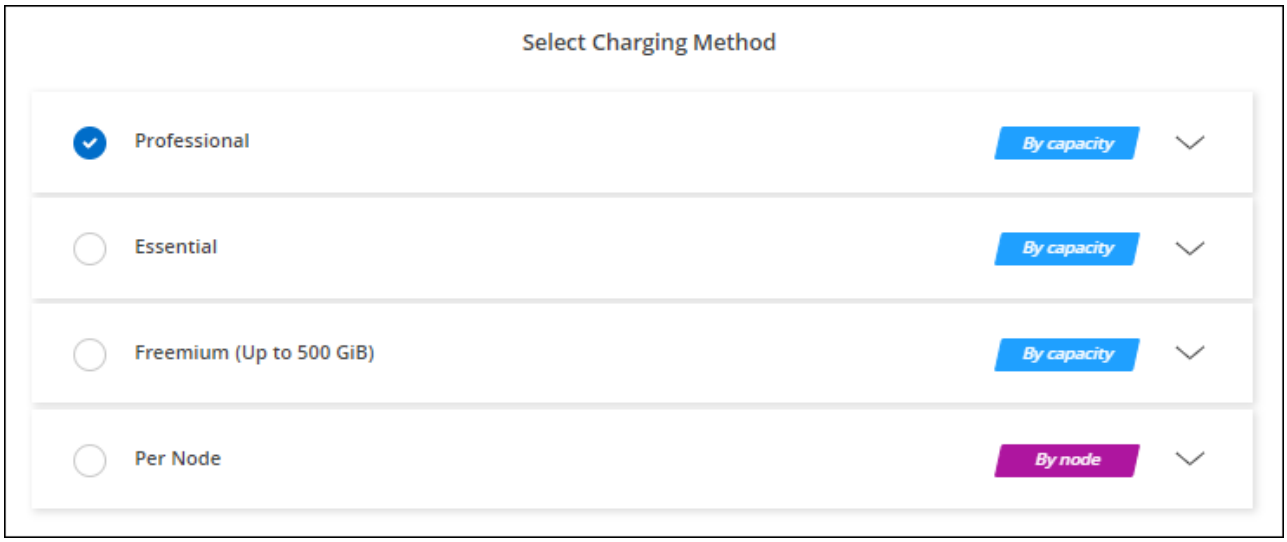
手順

1. 年間契約を購入するには、ネットアップの営業担当者にお問い合わせください。

   この契約は、Azure Marketplaceで_private_offerとして提供されます。

   ネットアップがお客様とプライベートオファーを共有したあとは、Azure Marketplaceでの作業環境の作成時にサブスクリプションするときに、年間プランを選択できます。

2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]>[サブスクリプションの追加]>[続行*]をクリックします。
   b. Azureポータルで、Azureアカウントと共有している年間プランを選択し、* Subscribe *をクリックします。
   c. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



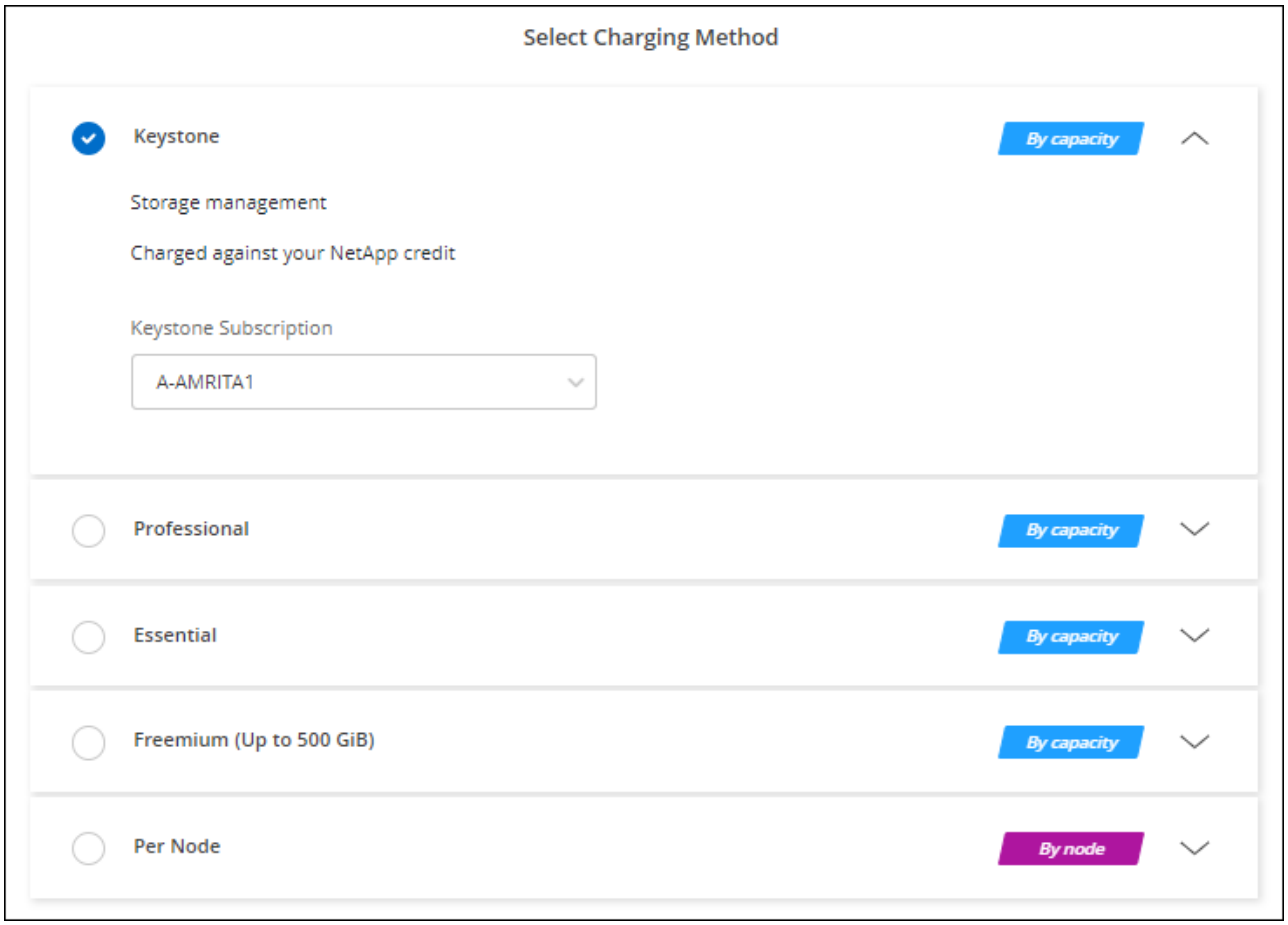
"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。
"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

Azureでハイアベイラビリティモードを有効にします

Microsoft Azureの高可用性モードを有効にして、計画外のフェイルオーバー時間を短縮し、NFSv4でCloud Volumes ONTAP がサポートされるようにする必要があります。

Cloud Volumes ONTAP 9.10.1リリースから、Microsoft Azureで実行されるCloud Volumes ONTAP HAペアの計画外フェイルオーバー時間が短縮され、NFSv4がサポートされるようになりました。これらの機能拡張をCloud Volumes ONTAP で使用できるようにするには、Azureサブスクリプションでハイアベイラビリティ機能を有効にする必要があります。

Azureサブスクリプションでこの機能を有効にする必要がある場合、「Action Required」メッセージにこれらの詳細が表示されます。

次の点に注意してください。

- Cloud Volumes ONTAP HA ペアの高可用性に問題はありません。この Azure 機能は、 ONTAP と連携して動作し、計画外のフェイルオーバーによって発生する NFS プロトコルのアプリケーション停止時間を短縮します。
- この機能を有効にしても、 Cloud Volumes ONTAP HA ペアの処理は中断されません。
- Azure サブスクリプションでこの機能を有効にしても、他の VM で原因の問題は発生しません。

「Owner」権限があるAzureユーザは、Azure CLIからこの機能を有効にできます。

手順

1. "Azure PortalからAzure Cloud Shellにアクセスします"
2. ハイアベイラビリティモード機能を登録します。

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 必要に応じて、機能が登録されたことを確認します。

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLIから次のような結果が返されることを確認します。

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

Azure で Cloud Volumes ONTAP を起動します

BlueXPでCloud Volumes ONTAP 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。

必要なもの

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
- 使用する構成についての理解。

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"。

- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

  "ライセンスの設定方法について説明します"。

このタスクについて

BlueXPは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いくつかのAzureオブジェクトを作成します。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。

> データ損失の可能性があります
>
> Cloud Volumes ONTAP システムごとに新しい専用のリソースグループを使用することを推奨します。
>
> データ損失のリスクがあるため、既存の共有リソースグループに Cloud Volumes ONTAP を導入することは推奨されません。導入に失敗したり削除したりした場合に、共有リソースグループからCloud Volumes ONTAP リソースを削除できますが、Azureユーザが誤って共有リソースグループからCloud Volumes ONTAP リソースを削除する可能性があります。

Azureでのシングルノード**Cloud Volumes ONTAP** システムの起動

AzureでシングルノードのCloud Volumes ONTAP システムを起動する場合は、BlueXPでシングルノードの作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. 場所を選択：「* Microsoft Azure 」および「 Cloud Volumes ONTAP シングルノード*」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. * 詳細とクレデンシャル * ：必要に応じて Azure のクレデンシャルとサブスクリプションを変更し、クラスタ名を指定し、タグを追加し、クレデンシャルを指定することもできます。

   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
作業環境名	BlueXPでは、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が付けられます。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
リソースグループタグ	タグは、 Azure リソースのメタデータです。このフィールドにタグを入力すると、Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。 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"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 "クレデンシャルを追加する方法について説明します"。

次のビデオでは、 Marketplace サブスクリプションを Azure サブスクリプションに関連付ける方法を紹介します。

► https://docs.netapp.com/ja-jp/test//media/video_subscribing_azure.mp4 *(video)*

6. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. 場所：リージョン、アベイラビリティゾーン、VNet、およびサブネットを選択し、チェックボックスを選択してコネクタとターゲットの場所間のネットワーク接続を確認します。

   シングルノードシステムの場合は、 Cloud Volumes ONTAP を導入するアベイラビリティゾーンを選択できます。AZを選択しない場合は、BlueXPによってそのAZが選択されます。

8. 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

   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
リソースグループ	Cloud Volumes ONTAP の新しいリソースグループを作成するか、既存のリソースグループを使用します。Cloud Volumes ONTAP には、新しい専用のリソースグループを使用することを推奨します。既存の共有リソースグループに Cloud Volumes ONTAP を導入することは可能ですが、データ損失のリスクがあるため推奨されません。詳細については、上記の警告を参照してください。 使用している Azure アカウントにが割り当てられている場合 "必要な権限"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。 • 「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のセキュリティグループを選択する場合は、 Cloud Volumes ONTAP の要件を満たす必要があります。 "デフォルトのセキュリティグループを表示します"。

9. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
10. * 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。

11. ライセンス：必要に応じてCloud Volumes ONTAP のバージョンを変更し、仮想マシンのタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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。

12. * Azure MarketplaceからサブスクライブBlueXP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。
13. * 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。

次の点に注意してください。

- 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。
- シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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"。

- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

  "データ階層化の詳細については、こちらをご覧ください。"。

14. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 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。

       このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください "HAペアのライセンスでサポートされる構成"。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

15. * 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。

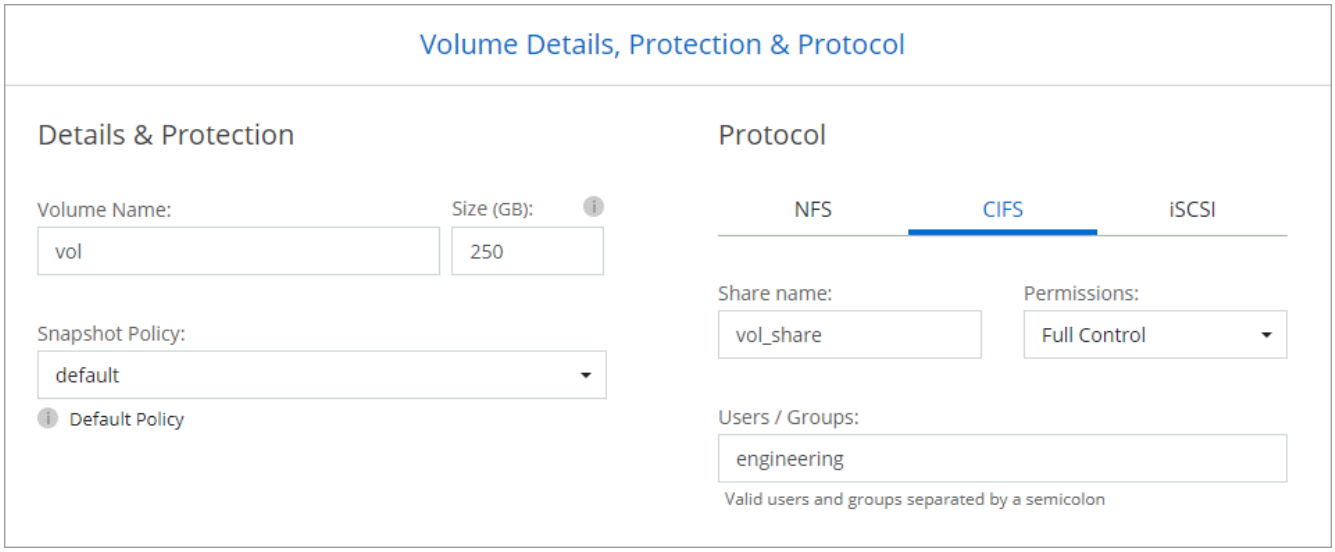
    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    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、BlueXP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。

フィールド	説明
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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



16. * 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。 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。 "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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

17. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    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"。

18. * 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、BlueXPが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

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Azureでの**Cloud Volumes ONTAP HA**ペアの起動

AzureでCloud Volumes ONTAP HAペアを起動するには、BlueXPでHA作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. プロンプトが表示されたら、 "コネクタを作成します"。
4. * 詳細とクレデンシャル * ：必要に応じて Azure のクレデンシャルとサブスクリプションを変更し、クラスタ名を指定し、タグを追加し、クレデンシャルを指定することもできます。

   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
作業環境名	BlueXPでは、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が付けられます。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。
リソースグループタグ	タグは、 Azure リソースのメタデータです。このフィールドにタグを入力すると、Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。 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"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 "クレデンシャルを追加する方法について説明します"。

次のビデオでは、 Marketplace サブスクリプションを Azure サブスクリプションに関連付ける方法を紹介します。

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

5. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "BlueXPの分類の詳細については、こちらをご覧ください"
   - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. * HA導入モデル* ：
   a. 単一アベイラビリティゾーン*または*複数のアベイラビリティゾーン*を選択します。
   b. 場所と接続（単一AZ）および*地域と接続*（複数のAZ）
      - 単一のAZの場合は、リージョン、VNet、およびサブネットを選択します。
      - 複数のAZについて、リージョン、VNet、サブネット、ノード1のゾーン、およびノード2のゾーンを選択します。
   c. [ネットワーク接続を検証しました…]*]チェックボックスを選択します。
7. 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

   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
リソースグループ	Cloud Volumes ONTAP の新しいリソースグループを作成するか、既存のリソースグループを使用します。Cloud Volumes ONTAP には、新しい専用のリソースグループを使用することを推奨します。既存の共有リソースグループに Cloud Volumes ONTAP を導入することは可能ですが、データ損失のリスクがあるため推奨されません。詳細については、上記の警告を参照してください。 Azure に導入する Cloud Volumes ONTAP HA ペアごとに専用のリソースグループを使用する必要があります。リソースグループでサポートされる HA ペアは 1 つだけです。Azureリソースグループに2つ目のCloud Volumes ONTAP HAペアを導入しようとすると、接続の問題が発生します。 使用している Azure アカウントにが割り当てられている場合 "必要な権限"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。

フィールド	説明
セキュリティグループが生成されました	BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。 • 「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のセキュリティグループを選択する場合は、 Cloud Volumes ONTAP の要件を満たす必要があります。 "デフォルトのセキュリティグループを表示します"。

8. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. 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、*構成の変更*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。
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、仮想マシンのタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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. * Azure Marketplaceからサブスクライブ*：BlueXP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。
12. * 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。

    次の点に注意してください。
    - シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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・サイズの選択については、を参照してください "Azureでシステムのサイズを設定します"。
    - ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
    - データの階層化を無効にすると、以降のアグリゲートで有効にすることができます。

"データ階層化の詳細については、こちらをご覧ください。"。

13. *書き込み速度とWORM *：

    a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

       "書き込み速度の詳細については、こちらをご覧ください。"。

    b. 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。

       このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください "HAペアのライセンスでサポートされる構成"。

       Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

14. ストレージと**WORM**へのセキュアな通信：Azureストレージアカウントへの**HTTPS**接続を有効にするかどうかを選択し、必要に応じてWrite Once Read Many（WORM）ストレージをアクティブ化します。

    HTTPS接続は、Cloud Volumes ONTAP 9.7のHAペアからAzureページBLOBストレージアカウントに確立されます。このオプションを有効にすると、書き込みパフォーマンスに影響する可能性があります。作業環境の作成後に設定を変更することはできません。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    データの階層化が有効になっていると、 WORM を有効にできません。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

15. * 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。

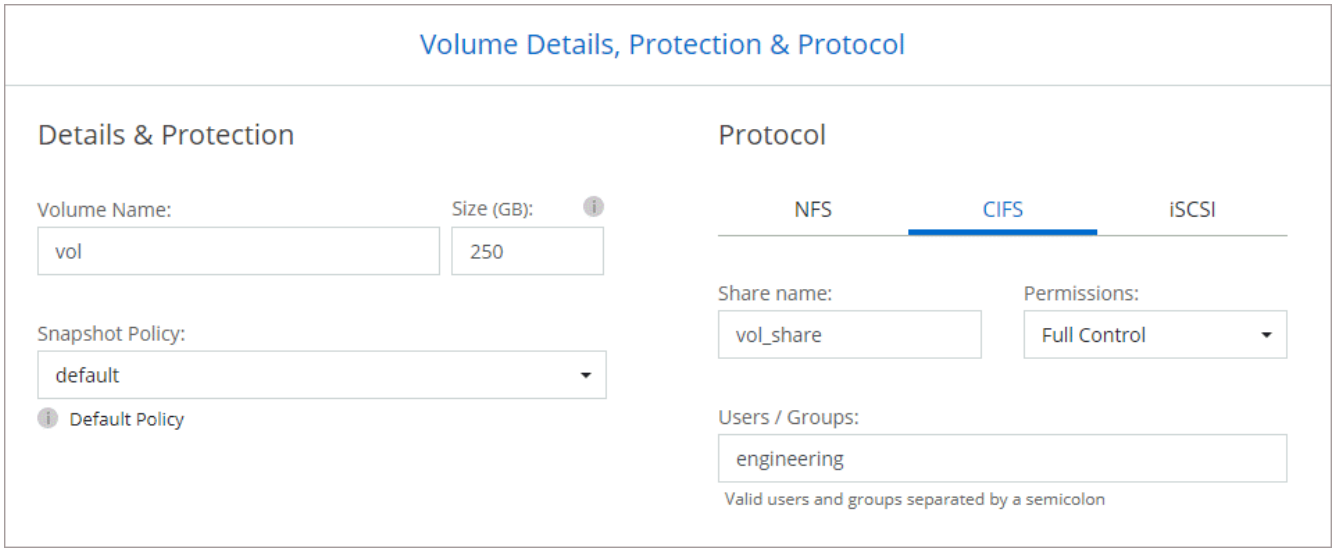
    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    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、BlueXP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。

フィールド	説明
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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



16. * 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。 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。 "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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

17. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

18. * 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、BlueXPが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

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Google Cloud で始めましょう

Google Cloud の Cloud Volumes ONTAP のクイックスタート

Cloud Volumes ONTAP for Google Cloudの使用を開始するには、いくつかの手順を実行します。


コネクタを作成します

を持っていなければ "コネクタ" ただし、アカウント管理者がアカウントを作成する必要があります。 "Google Cloud でコネクタを作成する方法について説明します"

インターネットアクセスを使用できないサブネットにCloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されているBlueXPユーザインターフェイスにアクセスする必要があります。 "インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"


構成を計画

BlueXPでは、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成を作成することもできます。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。

"構成の計画の詳細については、こちらをご覧ください"。


ネットワークをセットアップします

1. VPC とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートしていることを確認します。
2. データの階層化を有効にする場合は、 "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"。
3. HA ペアを導入する場合は、それぞれ独自のサブネットを持つ 4 つの VPC があることを確認します。
4. 共有 VPC を使用する場合は、コネクタサービスアカウントに _Compute Network User_role を指定します。
5. ターゲットVPCからのアウトバウンドのインターネットアクセスをNetApp AutoSupport で有効にします。

インターネットにアクセスできない場所にCloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

"ネットワーク要件の詳細については、こちらをご覧ください"。

4 サービスアカウントを設定します

Cloud Volumes ONTAP には、 2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です "データの階層化" Google Cloud で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こと。2 つ目は、を有効にした場合です "BlueXPのバックアップとリカバリ" ボリュームを低コストのオブジェクトストレージにバックアップできます。

1 つのサービスアカウントを設定して、両方の目的に使用できます。サービスアカウントには * Storage Admin * ロールが必要です。

"詳細な手順を参照してください"。

5 **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、コネクタと Cloud Volumes ONTAP を導入するために必要です。

- Cloud Deployment Manager V2 API
- クラウドロギング API
- Cloud Resource Manager API の略
- Compute Engine API
- ID およびアクセス管理（ IAM ） API

6 **BlueXP**を使用して**Cloud Volumes ONTAP** を起動します

[作業環境の追加] をクリックし、展開するシステムのタイプを選択して、ウィザードの手順を実行します。 "詳細な手順を参照してください"。

関連リンク

- "BlueXPからコネクタを作成しています"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "BlueXPがGoogle Cloud権限で実行する機能"

Google CloudでCloud Volumes ONTAP 構成を計画する

Google Cloud に Cloud Volumes ONTAP を導入する場合は、ワークロードの要件に合わせて事前設定されたシステムを選択するか、または独自の設定を作成できます。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。

Cloud Volumes ONTAP ライセンスを選択します

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

- "Cloud Volumes ONTAP のライセンスオプションについて説明します"
- "ライセンスの設定方法について説明します"

サポートされているリージョンを選択します

Cloud Volumes ONTAP は、ほとんどの Google Cloud リージョンでサポートされています。 "サポートされているリージョンの完全なリストを表示します"。

サポートされているマシンタイプを選択してください

Cloud Volumes ONTAP では、選択したライセンスタイプに応じて、複数のマシンタイプがサポートされます。

"GCP の Cloud Volumes ONTAP でサポートされている構成"

ストレージの制限を確認

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。

"GCP の Cloud Volumes ONTAP でのストレージの制限"

GCPでシステムをサイジングする

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。ディスクタイプは次のいずれかです。

- _ゾーン SSD 永続ディスク _ ： SSD 永続ディスクは、ランダム IOPS が高いワークロードに最適です。

- _ゾーン バランシング永続ディスク _ ：これらの SSD は、 GB あたりの IOPS を下げて、パフォーマンスとコストのバランスを取ります。
- _Zonal 標準パーシステントディスク _ ：標準パーシステントディスクは経済的で、シーケンシャルな読み取り / 書き込み処理に対応できます。

  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。システムの容量をBlueXPで管理できるようになりますが、自分でアグリゲートを作成する場合は、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"

デフォルトのシステムディスクを表示します

ユーザデータ用のストレージに加えて、BlueXPはCloud Volumes ONTAP システムデータ（ブートデータ、ルートデータ、コアデータ、NVRAM）用のクラウドストレージも購入します。計画を立てる場合は、 Cloud Volumes ONTAP を導入する前にこれらの詳細を確認すると役立つ場合があります。

- "Cloud Volumes ONTAP システムデータ用のデフォルトディスクを Google Cloud で表示します"。
- "Google Cloud のドキュメント：リソースクォータ"

  Google Cloud Compute Engine では、リソース使用量にクォータが適用されるため、 Cloud Volumes ONTAP を導入する前に制限に達していないことを確認する必要があります。

コネクタにはシステムディスクも必要です。 "コネクタのデフォルト設定に関する詳細を表示します"。

ネットワーク情報を収集

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。

- シングルノードシステム * のネットワーク情報

GCP情報	あなたの価値
地域	

GCP情報	あなたの価値
ゾーン	
vPC ネットワーク	
サブネット	
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）	

- 複数ゾーン内の HA ペアのネットワーク情報 *

GCP情報	あなたの価値
地域	
ノード 1 のゾーン	
ノード2のゾーン	
メディエーターのゾーン	
vPC-0 およびサブネット	
vPC-1 とサブネット	
vPC-2 およびサブネット	
vPC-3 とサブネット	
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）	

- 単一ゾーン内の HA ペアのネットワーク情報 *

GCP情報	あなたの価値
地域	
ゾーン	
vPC-0 およびサブネット	
vPC-1 とサブネット	
vPC-2 およびサブネット	
vPC-3 とサブネット	
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）	

書き込み速度を選択します

BlueXPを使用すると、Google Cloudのハイアベイラビリティ（HA）ペアを除き、Cloud Volumes ONTAP 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。 "書き込み速度の詳細については、

こちらをご覧ください。"。

ボリュームの使用プロファイルを選択してください

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。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または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。

Google CloudでのCloud Volumes ONTAP 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ネットワークをセットアップします。

HA ペアを導入する場合は、を実行します "Google CloudでのHAペアの仕組みをご確認ください"。

Cloud Volumes ONTAP の要件

Google Cloudでは、次の要件を満たす必要があります。

シングルノードシステムに固有の要件

シングルノードシステムを導入する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つのVPC

シングルノードシステムにはVirtual Private Cloud（VPC；仮想プライベートクラウド）が1つ必要です。

プライベート IP アドレス

BlueXPは、Google Cloudのシングルノードシステムに3つまたは4つのプライベートIPアドレスを割り当てます。

Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップ

し、次のフラグを指定できます。

```
skipSvmManagementLif: true
```

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、Storage VM （ SVM ）管理 LIF が必要です。

HAペアに固有の要件

HAペアを導入する場合は、ネットワークが次の要件を満たしていることを確認します。

1つまたは複数のゾーン

複数のゾーンまたは単一のゾーンに 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。HAペアを作成すると、複数のゾーンまたは単一のゾーンを選択するように求められます。

- 複数のゾーン（推奨）

  3 つのゾーンに HA 構成を導入することで、ゾーン内で障害が発生した場合の継続的なデータ可用性を確保できます。書き込みパフォーマンスは、単一のゾーンを使用する場合に比べてわずかに低くなりますが、最小のパフォーマンスです。

- シングルゾーン

  Cloud Volumes ONTAP HA 構成では、単一のゾーンに導入する場合は分散配置ポリシーを使用します。このポリシーにより、 HA 構成がゾーン内の単一点障害から保護されます。障害の切り分けに別々のゾーンを使用する必要はありません。

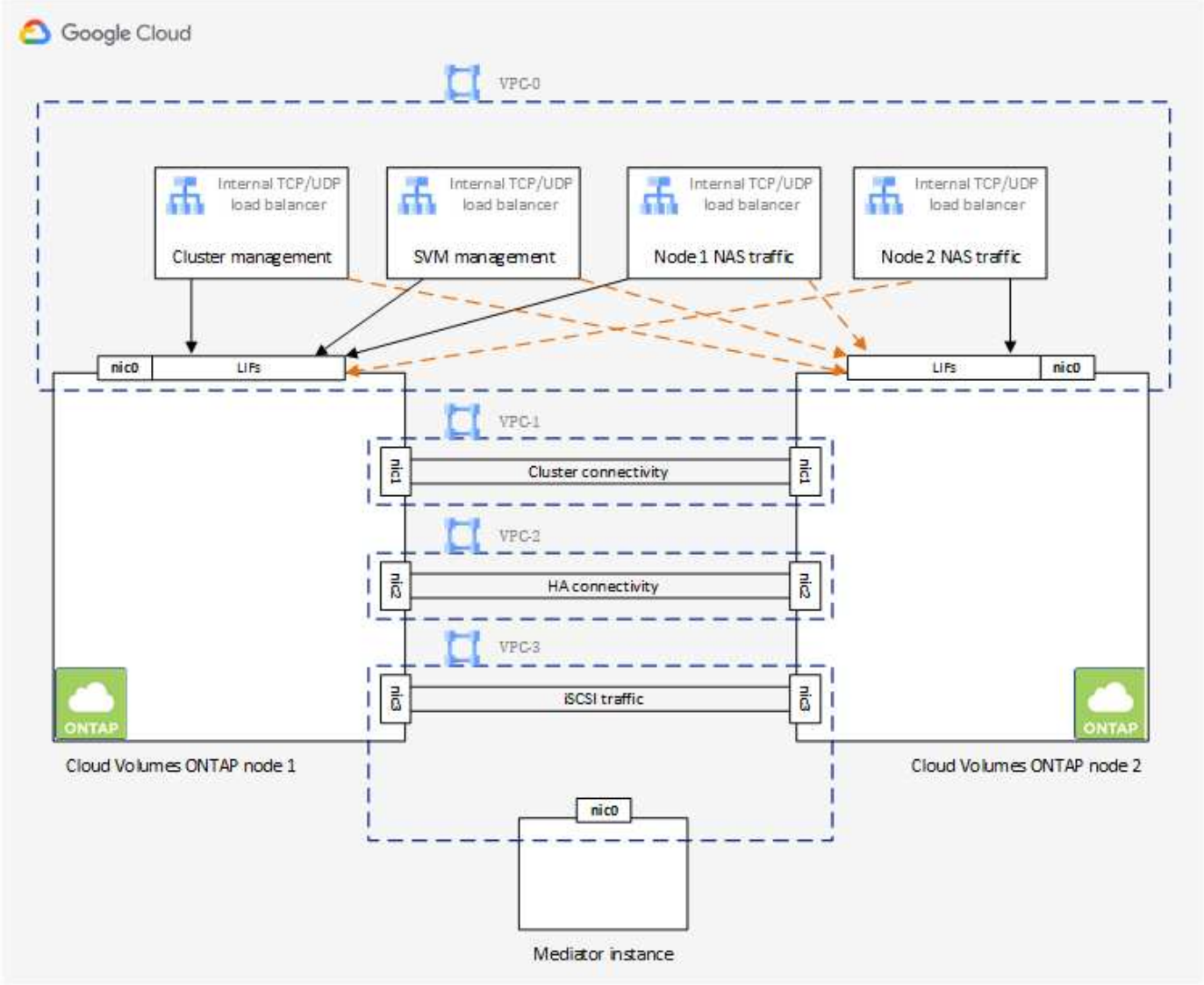
  この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

4つの仮想プライベートクラウド

HA 構成には、 4 つの Virtual Private Cloud （ VPC ；仮想プライベートクラウド）が必要です。Google Cloudでは各ネットワークインターフェイスを別 々 のVPCネットワークに配置する必要があるため、VPCは4つ必要です。

HAペアを作成するときに、4つのVPCを選択するように要求されます。

- vPC-0 ：データおよびノードへのインバウンド接続
- vPC-1 、 VPC -2 、および VPC -3 ：ノードと HA メディエーター間の内部通信



サブネット

VPC ごとにプライベートサブネットが必要です。

コネクタを VPC 0 に配置する場合は、サブネットで Private Google Access を有効にして API にアクセスし、データの階層化を有効にする必要があります。

これらの VPC 内のサブネットには、個別の CIDR 範囲が必要です。CIDR 範囲を重複させることはできません。

プライベート **IP** アドレス

BlueXPは、必要な数のプライベートIPアドレスをGoogle CloudのCloud Volumes ONTAP に自動的に割り当てます。ネットワークに十分なプライベートアドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。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。

- * シングルノード *

BlueXPでは、1つのノードシステムに4つのIPアドレスが割り当てられます。

- ノード管理 LIF
- クラスタ管理 LIF
- iSCSI データ LIF

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

- NAS LIF

  Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップし、次のフラグを指定できます。

```
skipSvmManagementLif: true
```

- * HAペア*
  BlueXPでは、12~13個のIPアドレスをHAペアに割り当てます。
  - ノード管理LIF×2（e0a）
  - クラスタ管理LIF（e0a）×1
  - iSCSI LIF×2（e0a）

> iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

  - NAS LIF（e0a）×1または2
  - クラスタLIF×2（e0b）
  - HAインターコネクトIPアドレス×2（e0c）
  - RSM iSCSI IPアドレス×2（e0d）

    Cloud Volumes ONTAP を API を使用して導入する場合、 Storage VM （ SVM ）管理 LIF の作成をスキップし、次のフラグを指定できます。

```
skipSvmManagementLif: true
```

内部ロードバランサ

BlueXPでは、Cloud Volumes ONTAP HAペアへの着信トラフィックを管理するGoogle Cloud内部ロードバランサ（TCP/UDP）が自動的に4つ作成されます。セットアップは必要ありませんネットワークトラフィックを通知し、セキュリティ上の問題を緩和するだけで、この要件が満たされることがわかりました。

クラスタ管理用のロードバランサで、 1 つは Storage VM （ SVM ）管理用、もう 1 つはノード 1 への NAS トラフィック用、もう 1 つはノード 2 への NAS トラフィック用です。

各ロードバランサの設定は次のとおりです。

- 共有プライベート IP アドレス × 1
- グローバル健全性チェック 1 回

  デフォルトでは、ヘルスチェックで使用されるポートは 63001 、 63002 、および 63003 です。

- 地域 TCP バックエンドサービス × 1
- 1つのリージョナルUDPバックエンドサービス
- 1 つの TCP 転送ルール
- 1つのUDP転送ルール
- グローバルアクセスは無効です

  グローバルアクセスはデフォルトでは無効になっていますが、展開後に有効にすることができます。クロスリージョントラフィックのレイテンシが大幅に高くなるため、この機能は無効にしました。誤ってリージョン間にマウントすることが原因でマイナスの体験が得られないようにしたいと考えていました。このオプションを有効にすることは、ビジネスニーズに固有のものです。

共有 **VPC**

Cloud Volumes ONTAP とコネクタは、 Google Cloud の共有 VPC とスタンドアロンの VPC でサポートされます。

シングルノードシステムの場合は、 VPC は共有 VPC またはスタンドアロン VPC のどちらかになります。

HA ペアの場合は、 4 つの VPC が必要です。これらの各 VPC は、共有またはスタンドアロンのどちらかにすることができます。たとえば、 VPC は VPC を共有化し、 VPC は VPC 1 、 VPC は 2 、 VPC は 3 で構成されることになります。

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、 Connector および Cloud Volumes ONTAP 仮想マシンインスタンスをサービスプロジェクト _ で導入できます。 "Google Cloud のドキュメント：「 Shared VPC Overview"。

"Connector の導入でカバーされている必要な共有 VPC の権限を確認します"

VPC でのパケットミラーリング

"パケットミラーリング" Cloud Volumes ONTAP を導入する Google Cloud VPC で無効にする必要があります。パケットミラーリングがイネーブルの場合、 Cloud Volumes ONTAP は正常に動作しません。

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 へのアウトバウンドのインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

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

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのファイアウォールがポート3128上の_INBOUND接続を許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP ファイアウォールがポート3128で_OUTBOUND接続を許可することも必要です。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

HA ペアを使用している場合、 HA メディエーターではアウトバウンドのインターネットアクセスは必要ありません。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、 "AutoSupport 構成のトラブルシューティングを行います"。

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。BlueXPはファイアウォールルールを作成します。独自のファイアウォールを使用する必要がある場合は、以下のファイアウォールルールを参照してください。

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。これらのルールにより、 Cloud Volumes ONTAP へのデータアクセスが可能になります。 詳細はこちら。。
- VPC -1 、 VPC -2 、および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、 HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。詳細はこちら。。

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 Access 用に設定する必要があります（ HA ペアを使用している場合、これは VPC 0 のサブネットです）。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：「 Configuring Private Google Access"。

BlueXPでデータの階層化を設定するために必要な追加手順については'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

Google Cloud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"。

ファイアウォールルール

BlueXPは、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を

含むGoogle Cloudファイアウォールルールを作成します。テスト目的または独自のファイアウォールルールを使用する場合は、ポートを参照してください。

Cloud Volumes ONTAP 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。HA 構成を導入する場合は、 VPC 0 の Cloud Volumes ONTAP のファイアウォールルールを以下に示します。

HA 構成には、次の 2 組のファイアウォールルールが必要です。

- VPC -0 の HA コンポーネントのルールセット。これらのルールにより、 Cloud Volumes ONTAP へのデータアクセスが可能になります。
- VPC -1 、 VPC -2 、および VPC -3 の HA コンポーネントに関するもう 1 つのルールセット。これらのルールは、 HA コンポーネント間のインバウンド通信とアウトバウンド通信に対してオープンです。 詳細はこちら。。

コネクタに関する情報をお探しですか？ "コネクタのファイアウォールルールを表示します"

インバウンドルール

作業環境を作成する場合、展開時に定義済みファイアウォールポリシーのソースフィルタを選択できます。

- 選択した**VPC**のみ：インバウンドトラフィックのソースフィルタは、Cloud Volumes ONTAP システムのVPCのサブネット範囲、およびコネクタが存在するVPCのサブネット範囲です。これが推奨されるオプションです。
- *すべてのVPC *：インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲です。

独自のファイアウォールポリシーを使用する場合は、Cloud Volumes ONTAP と通信する必要のあるすべてのネットワークを追加し、内部のGoogleロードバランサが正常に機能するように両方のアドレス範囲を追加してください。これらのアドレスは 130.211.0.0/22 および 35.191.0.0/16 です。詳細については、を参照してください "Google Cloud ドキュメント：ロードバランサファイアウォールルール"。

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	8時80分	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	コネクタへの接続と、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	———	NFS のリモートプロシージャコール
TCP	一三九	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

プロトコル	ポート	目的
TCP	2049年	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	10、000	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
TCP	63001-63050	プローブポートをロードバランシングして、どのノードが正常であるかを判断します（ HA ペアの場合のみ必要）
UDP	———	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年	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

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	一三七	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	一三八	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	一三九	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	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 、 iSCSI ）	Active Directory フォレスト	Kerberos V 認証
	UDP	一三七	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS ネームサービス
	UDP	一三八	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	一三九	データ LIF （ NFS 、 CIFS ）	Active Directory フォレスト	NetBIOS サービスセッション
	TCP および UDP	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
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport （デフォルトは HTTPS ）
	HTTP	8時80分	ノード管理 LIF	support.netapp.com	AutoSupport （転送プロトコルが HTTPS から HTTP に変更された場合のみ）
	TCP	3128だ	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介してAutoSupport メッセージを送信する
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）
構成のバックアップ	HTTP	8時80分	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。 "構成バックアップファイルについて説明します"。
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	一六二	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	一六二	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

VPC -1、VPC -2、およびVPC -3のルール

Google Cloudでは、4つのVPC間にHA構成が導入されます。VPC -0 の HA 構成に必要なファイアウォールルール はです Cloud Volumes ONTAP については上記のリストを参照してください。

一方、BlueXPでVPC -1、VPC -2、およびVPC -3のインスタンスに対して作成される定義済みのファイアウォールルールにより、_All_protocolsとポートでの入力通信が可能になります。これらのルールに従って、 HA ノード間の通信が可能になります。

HA ノードから HA メディエーターへの通信は、ポート 3260 （ iSCSI ）を介して行われます。

> Google Cloudの新しいHAペア環境で高速な書き込み速度を有効にするには、VPC-1、VPC-2、およびVPC-3のMaximum Transmission Unit（MTU；最大伝送ユニット）が8、896バイト以上必要です。既存のVPC-1、VPC-2、およびVPC-3を8、896バイトのMTUにアップグレードする場合は、設定プロセス中にこれらのVPCを使用している既存のHAシステムをすべてシャットダウンする必要があります。

コネクタの要件

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "コネクタのネットワーク要件を確認します"
- "Google Cloudのファイアウォールルール"

GCP での VPC サービスコントロールの計画

Google Cloud環境をVPC Service Controlsでロックダウンする場合は、BlueXPとCloud Volumes ONTAP がGoogle Cloud APIとどのように連携するか、またBlueXPとCloud Volumes ONTAP を展開するためのサービス境界を構成する方法について理解しておく必要があります。

vPC サービスコントロールを使用すると、信頼できる境界外の Google 管理サービスへのアクセスを制御し、信頼できない場所からのデータアクセスをブロックし、不正なデータ転送のリスクを軽減できます。 "Google Cloud VPC Service Controls の詳細をご覧ください"。

ネットアップサービスと VPC サービスコントロールの通信方法

BlueXPは、Google Cloud APIと直接通信します。これは、Google Cloudの外部の外部IPアドレス（たとえば、api.services.cloud.netapp.comから）、またはBlueXPコネクタに割り当てられた内部アドレスからGoogle Cloud内でトリガーされます。

コネクタの配置スタイルによっては、サービスの境界に対して特定の例外を設定する必要があります。

イメージ

Cloud Volumes ONTAP とBlueXPはどちらも、ネットアップが管理するGCP内のプロジェクトのイメージを使用します。組織内でホスティングされていない画像の使用をブロックするポリシーがある場合、これはBlueXP ConnectorおよびCloud Volumes ONTAP の展開に影響を与える可能性があります。

手動インストールでもコネクタを手動で導入できますが、 Cloud Volumes ONTAP プロジェクトからイメージを取得する必要があります。Connector と Cloud Volumes ONTAP を導入するには、許可されたリストを指定

する必要があります。

コネクタの配置

コネクタを導入するユーザーは、 projectId_NetApp-cloudmanager_and the project Number_14190056516_ でホストされているイメージを参照できる必要があります。

Cloud Volumes ONTAP の導入

- BlueXPサービスアカウントは、projectId_NetApp-cloudmanager_and the project number_14190056516_ でホストされているイメージをサービスプロジェクトから参照する必要があります。
- デフォルトの Google API サービスエージェントのサービスアカウントは、 projectId_NetApp-cloudmanager_and the project number_14190056516_ サービスプロジェクトからホストされているイメージを参照する必要があります。

VPC サービスコントロールを使用してこれらのイメージをプルするために必要なルールの例を次に示します。

vPC サービスは境界ポリシーを制御します

ポリシーでは、 VPC Service Controls ルールセットの例外が許可されます。ポリシーの詳細については、を参照してください "GCP VPC Service Controls Policy Documentation を参照してください"。

BlueXPで必要なポリシーを設定するには、組織内のVPC Service Controls Perimeterに移動し、次のポリシーを追加します。各フィールドは、 VPC の [Service Controls Policy] ページで指定されたオプションと一致する必要があります。また、 * すべての * ルールが必要であり、 * または * パラメーターをルールセットで使用する必要があります。

入力規則

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Service Project]
    Services =
        Service name: iam.googleapis.com
          Service methods: All actions
        Service name: compute.googleapis.com
          Service methods:All actions
```

または

```
From:
    Identities:
        [User Email Address]
    Source > All sources allowed
To:
    Projects =
        [Host Project]
    Services =
        Service name: compute.googleapis.com
          Service methods: All actions
```

または

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
    Source > All sources allowed
To:
    Projects =
        [Service Project]
        [Host Project]
    Services =
        Service name: compute.googleapis.com
        Service methods: All actions
```

出力ルール

```
From:
    Identities:
        [Service Project Number]@cloudservices.gserviceaccount.com
To:
    Projects =
        14190056516
    Service =
        Service name: compute.googleapis.com
        Service methods: All actions
```

上記のプロジェクト番号は、コネクタと Cloud Volumes ONTAP のイメージを格納するためにネットアップが使用する project_name cloudmanager_used です。

データ階層化とバックアップ用のサービスアカウントを作成します

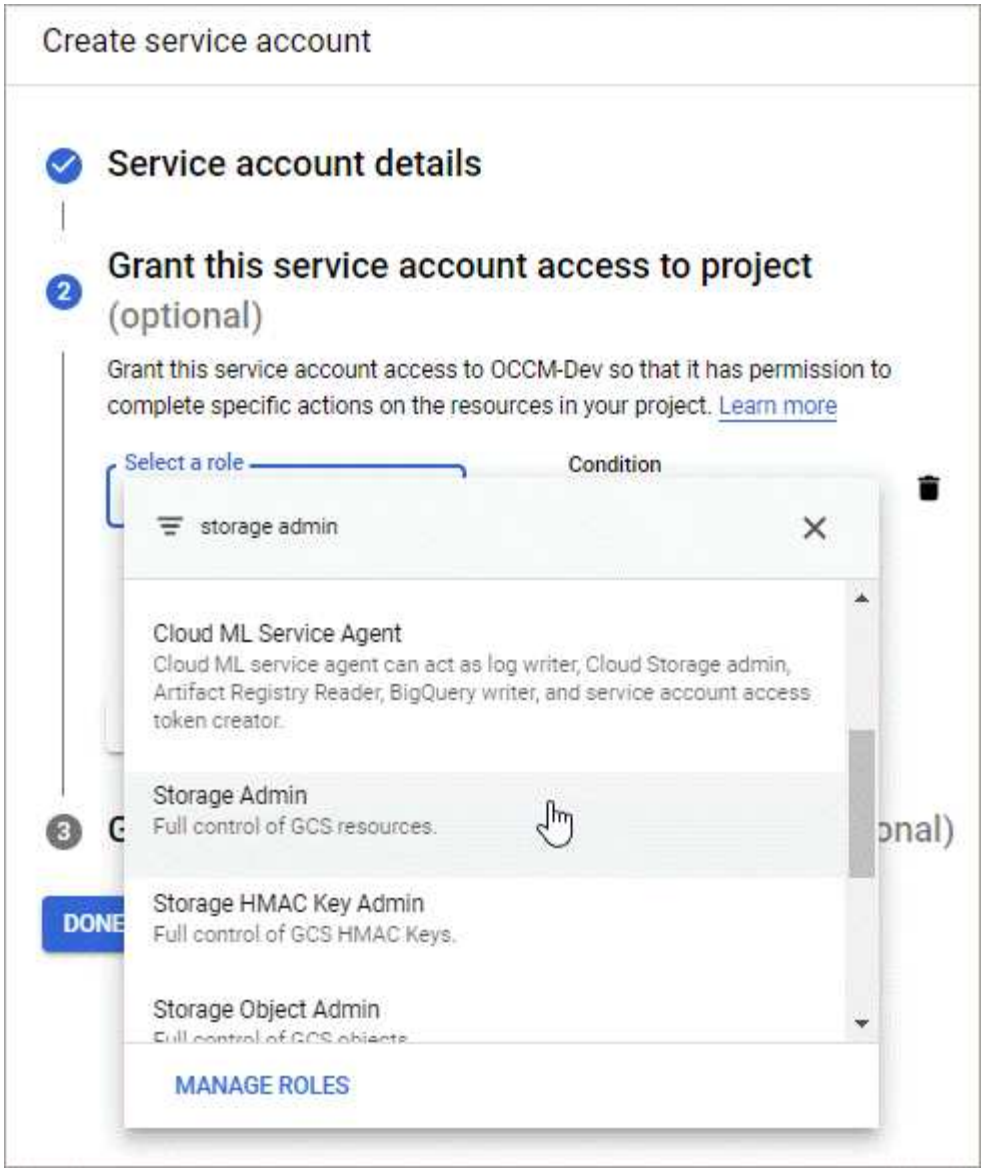
Cloud Volumes ONTAP には、 2 つの目的で Google Cloud サービスアカウントが必要です。1 つ目は、を有効にする場合です "データの階層化" Google Cloud でコールドデータを低コストのオブジェクトストレージに階層化すること。2 つ目は、を有効にした場合です "BlueXPのバックアップとリカバリ" ボリュームを低コストのオブジェクトストレージにバックアップできます。

Cloud Volumes ONTAP では、このサービスアカウントを使用して、階層化データ用のバケットとバックアップ用のバケットにアクセスして管理します。

1 つのサービスアカウントを設定して、両方の目的に使用できます。サービスアカウントには * Storage Admin * ロールが必要です。

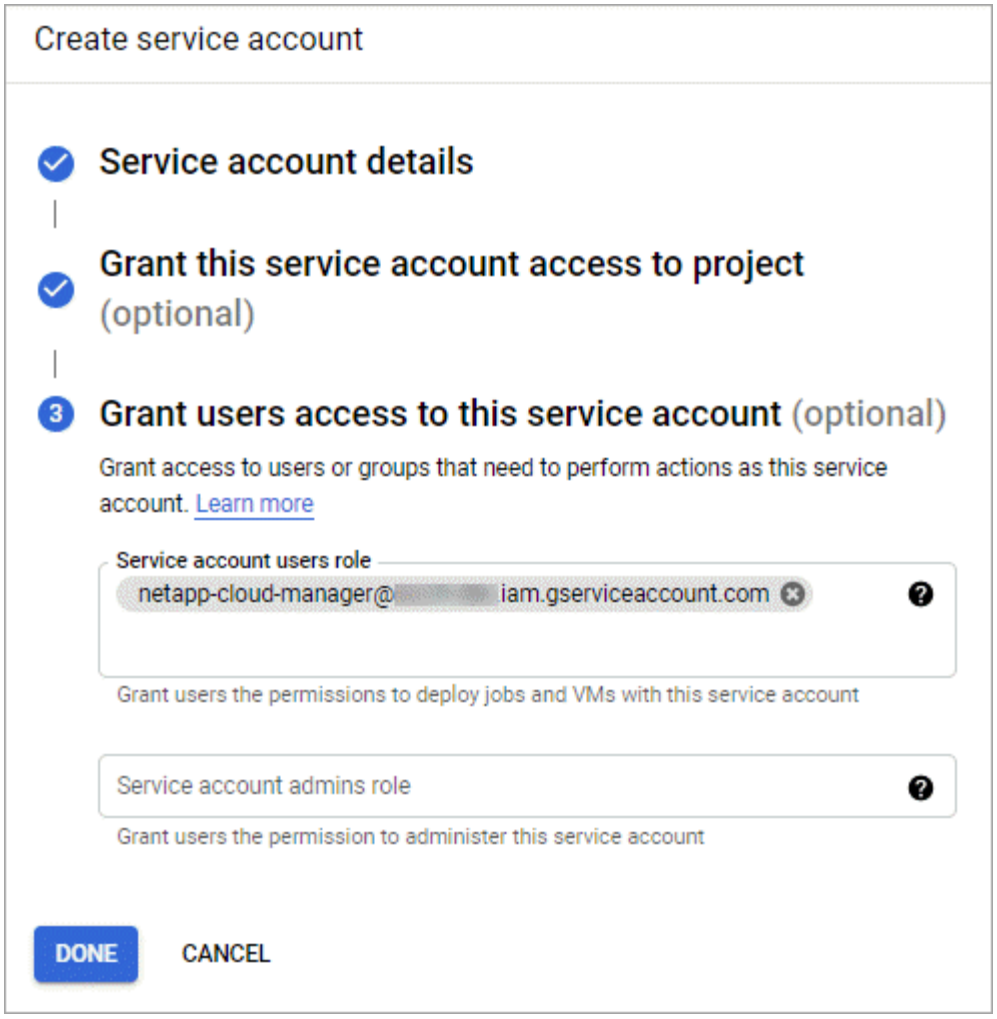
手順

1. Google Cloud コンソールで、 "[サービスアカウント ページに移動します"^]。
2. プロジェクトを選択します。
3. [サービスアカウントの作成] をクリックし、必要な情報を入力します。
    a. * サービスアカウントの詳細 * ：名前と説明を入力します。
    b. * このサービスアカウントにプロジェクトへのアクセスを許可 * ： * ストレージ管理者 * の役割を選択します。



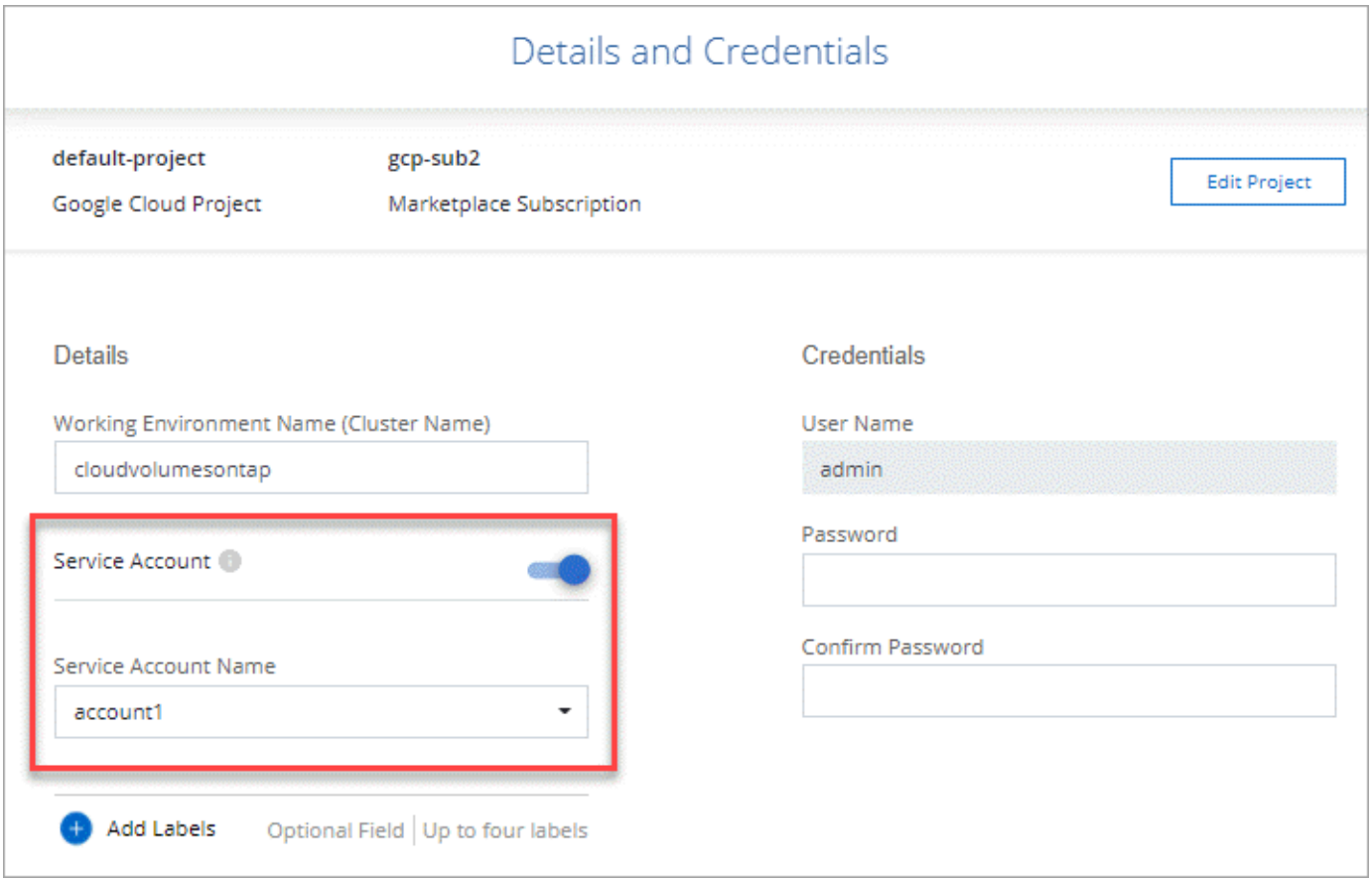
c. * このサービスアカウントへのアクセス権をユーザーに付与 *: Connector サービスアカウントを A_Service アカウント User_ としてこの新しいサービスアカウントに追加します。

この手順はデータ階層化にのみ必要です。BlueXPのバックアップとリカバリには必要ありません。



次の手順

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。



ページのスクリーンショット。"]

お客様が管理する暗号化キーを **Cloud Volumes ONTAP** で使用する

Google Cloud Storageでは、データがディスクに書き込まれる前に常に暗号化されますが、BlueXP APIを使用して、_お客様が管理する暗号化キー_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。

手順

1. キーが格納されているプロジェクトで、BlueXP Connectorサービスアカウントがプロジェクトレベルで正しいアクセス許可を持っていることを確認します。

   権限は、で提供されています "デフォルトでは、Connectorサービスアカウントの権限です"、ただし、Cloud Key Management Serviceに別のプロジェクトを使用する場合は適用できません。

   権限は次のとおりです。

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

2. のサービスアカウントを確認します "Google Compute Engine Service Agent" キーに対する Cloud KMS の

暗号化 / 復号化権限があることを確認します。

サービスアカウントの名前は、「 service-[SERVICE_PROJECT_NUMBER_@compute-system.iam.gserviceaccount.com 」という形式で指定します。

"Google Cloud のドキュメント：「 Using IAM with Cloud KMS - Granting roles on a resource"

3. のgetコマンドを呼び出して、キーの「id」を取得します。 `/gcp/vsa/metadata/gcp-encryption-keys` API呼び出し、またはGCPコンソールのキーで[Copy Resource Name]を選択します。
4. お客様が管理する暗号化キーを使用し、データをオブジェクトストレージに階層化する場合、BlueXPは、永続ディスクの暗号化に使用されるのと同じキーを使用しようとします。キーを使用するには、まず Google Cloud Storage バケットを有効にする必要があります。

   a. 次の手順に従って、 Google Cloud Storage サービスエージェントを検索します "Google Cloud ドキュメント：「 Getting the Cloud Storage service agent"。

   b. 暗号化キーに移動し、 Cloud KMS 暗号化 / 復号化権限を持つ Google Cloud Storage サービスエージェントを割り当てます。

   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：「 Using customer-managed encryption keys"

5. 作業環境を作成するときは、 API 要求で "GcpEncryption" パラメータを使用します。

   ◦ 例 *

```
"gcpEncryptionParameters": {
    "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
  }
```

を参照してください "BlueXP自動化ドキュメント" "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。

Google CloudでCloud Volumes ONTAP のライセンスを設定します

Cloud Volumes ONTAP で使用するライセンスオプションを決定したら、新しい作業環境を作成する際にそのライセンスオプションを選択する前に、いくつかの手順を実行する必要があります。

フリーミアム

プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

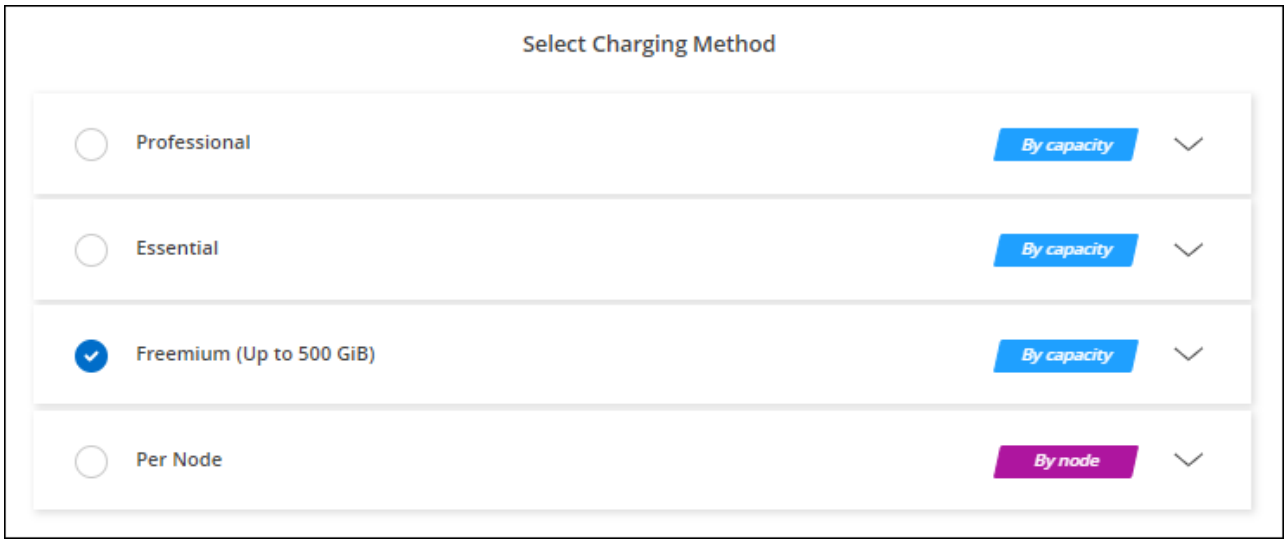
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。

   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロン

プトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

プロビジョニング済み容量が500GiBを超えると、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。

b. BlueXPに戻ったら、充電方法のページにアクセスして「* Freemium *」を選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

容量単位のライセンスです

容量単位のライセンスでは、 TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。容量ベースのライセンスは、パッケージ：Essentialsパッケージまたはプロフェッショナルパッケージの形式で提供されます。

Essentials パッケージと Professional パッケージには、次の消費モデルがあります。

- ネットアップから購入したライセンス（ BYOL ）
- Google Cloud Marketplaceから1時間単位の従量課金制（PAYGO）サブスクリプション
- 年間契約

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

ネットアップからライセンスを購入（BYOL）して前払いし、任意のクラウドプロバイダにCloud Volumes ONTAP システムを導入できます。

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "NetApp Support Site アカウントをBlueXPに追加します"

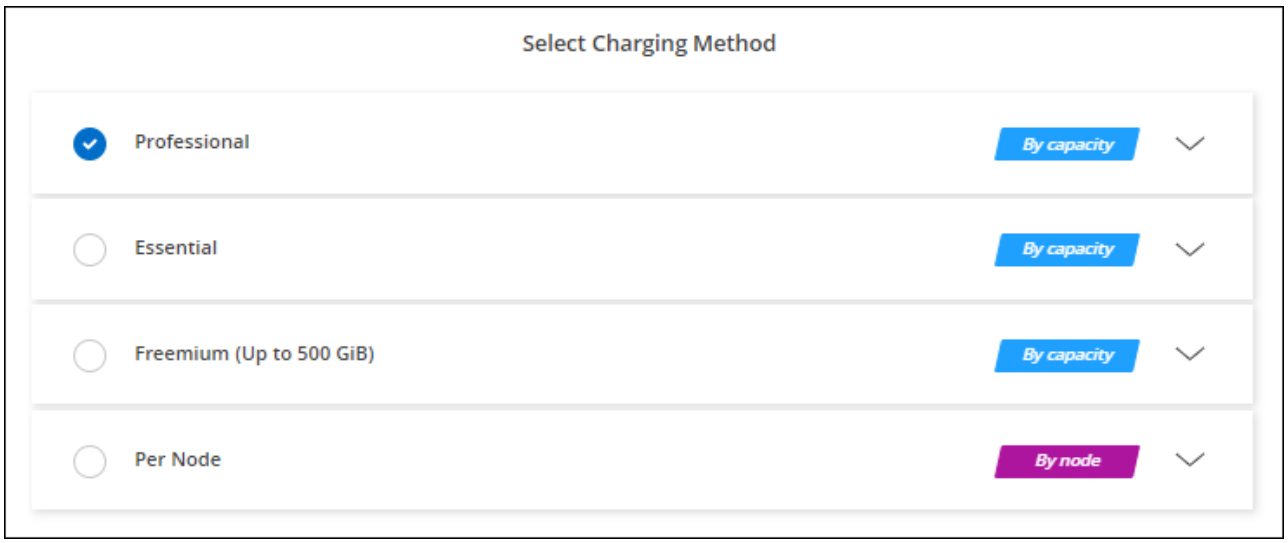
BlueXPは、ネットアップのライセンスサービスを自動的に照会し、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます "ライセンスをBlueXPデジタルウォレットに手動で追加します"。

3. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

      ネットアップから購入したライセンスには、最初に必ず料金が請求されますが、ライセンスで許可された容量を超えた場合や、ライセンスの期間が終了した場合は、マーケットプレイスで1時間ごとに料金が請求されます。

   b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

PAYGOサブスクリプション

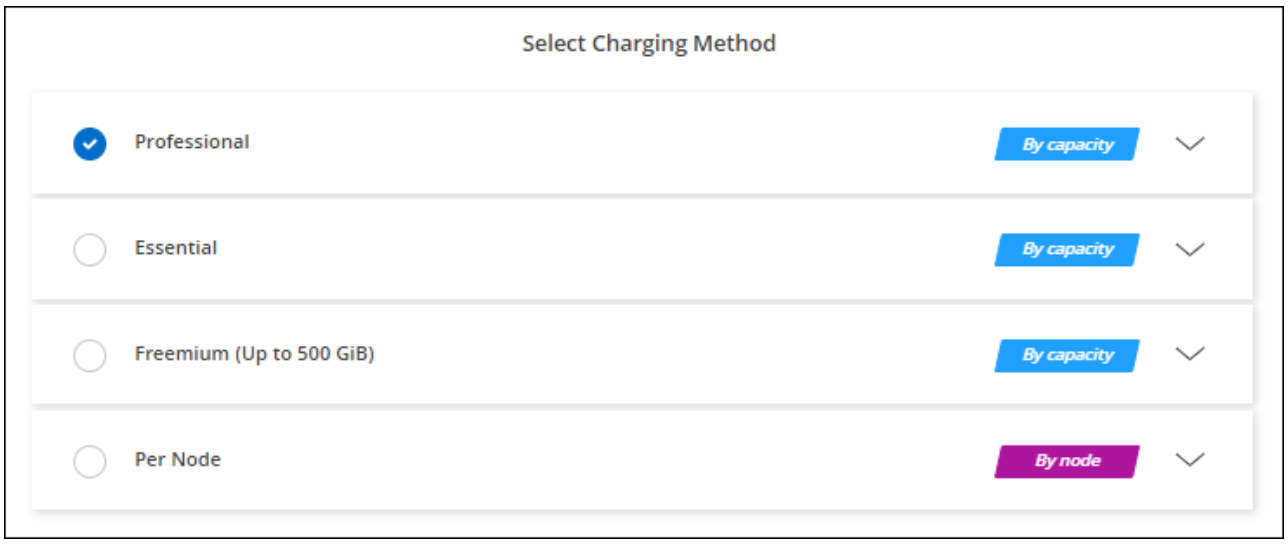
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

Cloud Volumes ONTAP 作業環境を作成すると、Google Cloud Marketplaceで提供されている契約を購読するように求めるメッセージが表示されます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceでの従量課金制サービスに登録します。

b. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

アカウントに関連付けられたGoogle Cloud Marketplaceのサブスクリプションは、[設定]>[クレデンシャル]ページで管理できます。 "Google Cloudのクレデンシャルとサブスクリプションを管理する方法について説明します"

年間契約

年間契約を購入することで、Cloud Volumes ONTAP の年間料金をお支払いいただけます。

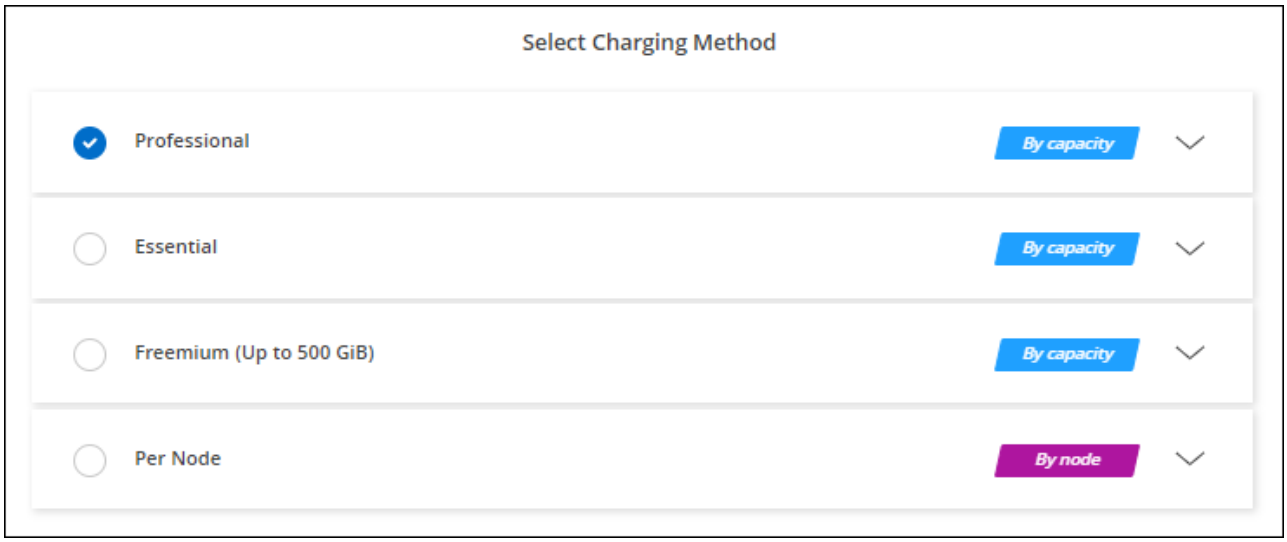
手順

1. 年間契約を購入するには、ネットアップの営業担当者にお問い合わせください。

   この契約は、Google Cloud Marketplaceで_private_offerとして提供されます。

   ネットアップがプライベートオファーを共有した後は、作業環境の作成中にGoogle Cloud Marketplaceから登録するときに、年間プランを選択できます。

2. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
   a. [詳細と資格情報]ページで、[資格情報の編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってGoogle Cloud Marketplaceで年間プランを購読します。
   b. Google Cloudで、アカウントと共有されている年間プランを選択し、[**Subscribe**]をクリックします。
   c. BlueXPに戻ったら、[課金方法]ページにアクセスして容量ベースのパッケージを選択します。



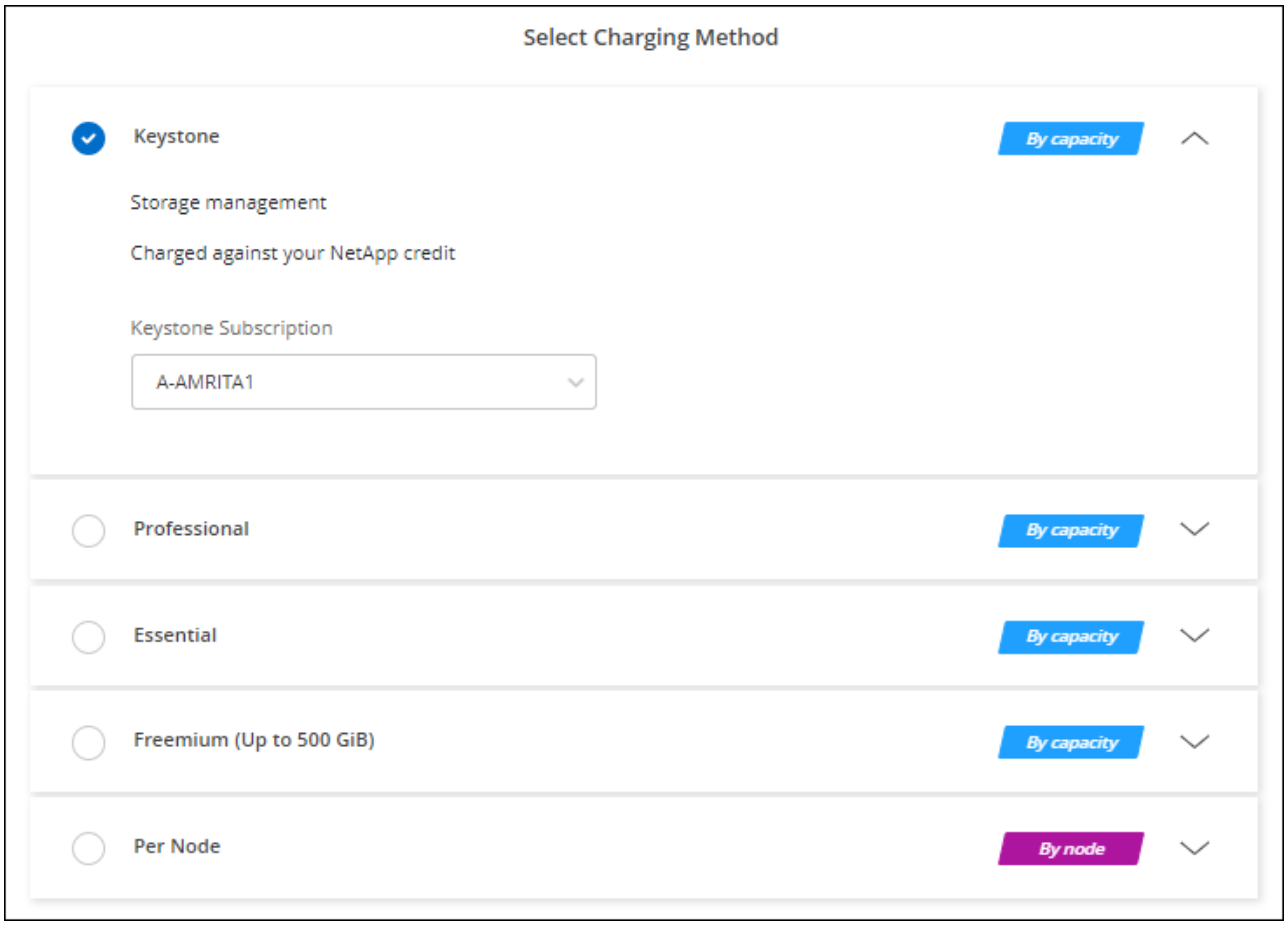
"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。
"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

手順

1. まだサブスクリプションをお持ちでない場合は、 "ネットアップにお問い合わせください"
2. mailto：ng-keystone-success@netapp.com [ネットアップにお問い合わせください]。1つ以上のKeystoneサブスクリプションでBlueXPユーザアカウントを承認する場合。
3. ネットアップがお客様のアカウントを許可したあと、 "Cloud Volumes ONTAP で使用するサブスクリプションをリンクします"。
4. キャンバスページで、*Add Working Environment*をクリックし、BlueXPの手順に従います。
    a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"Google CloudでCloud Volumes ONTAP を起動するための詳細な手順を表示します"。

Google Cloud で Cloud Volumes ONTAP を起動しています

Cloud Volumes ONTAP は、シングルノード構成またはGoogle CloudのHAペアとして起動できます。

始める前に

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
  - を用意しておく必要があります "ワークスペースに関連付けられているコネクタ"。
  - "コネクタをで実行したままにする準備をしておく必要があります 常時"。
  - コネクタに関連付けられているサービスアカウント "必要な権限がある必要があります"
- 使用する構成についての理解。

  構成を選択し、管理者からGoogle Cloud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"。

- Cloud Volumes ONTAP のライセンスを設定するために必要な事項を理解する。

"ライセンスの設定方法について説明します"。

- Google Cloud API はとする必要があります "プロジェクトで有効にします"：
  - Cloud Deployment Manager V2 API
  - クラウドロギング API
  - Cloud Resource Manager API の略
  - Compute Engine API
  - ID およびアクセス管理（ IAM ） API

Google Cloudでのシングルノードシステムの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. [[subscribe] キャンバスページで、 * 作業環境の追加 * をクリックし、プロンプトに従います。
3. * 場所を選択 * ：「 * Google Cloud * 」と「 * Cloud Volumes ONTAP * 」を選択します。
4. プロンプトが表示されたら、 "コネクタを作成します"。
5. 詳細と認証情報：プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

   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
作業環境名	BlueXPは、作業環境名を使用して、Cloud Volumes ONTAP システムとGoogle Cloud 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。
サービスアカウント名	を使用する場合は "データの階層化" または "BlueXPのバックアップとリカバリ" Cloud Volumes ONTAP では、 * サービスアカウント * を有効にして、事前定義されたストレージ管理者ロールが割り当てられたサービスアカウントを選択する必要があります。 "サービスアカウントの作成方法について説明します"。
ラベルを追加します	ラベルは、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。 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"。

フィールド	説明
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXP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。BlueXPロールを持つ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、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud MarketplaceからCloud Volumes ONTAP へのサブスクリプションに関連付けられているGoogle Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。または、の手順に従って、に登録します "MarketplaceサブスクリプションとGoogle Cloudクレデンシャルの関連付け" セクション。

► https://docs.netapp.com/ja-jp/test//media/video_subscribing_gcp.mp4 *(video)*

6. * サービス * ：このシステムで使用するサービスを選択します。BlueXPのバックアップとリカバリを選択するか、BlueXPの階層化を使用するには、ステップ3でサービスアカウントを指定しておく必要があります。

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

7. 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
接続の検証	コールドデータをGoogle Cloud Storageバケットに階層化するには、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"。

フィールド	説明
ファイアウォールポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースフィルタは、選択したVPCのサブネット範囲とコネクタが存在するVPCのサブネット範囲になります。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲になります。
既存のファイアウォールポリシーを使用する	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。リンク：https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/reference-networking-gcp.html#firewall-rules[Learn Cloud Volumes ONTAPのファイアウォールルールについて^]。

8. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 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。
10. ライセンス：必要に応じてCloud Volumes ONTAP バージョンを変更し、マシンタイプを選択します。

    選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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、つまりディスクタイプと各ディスクのサイズを選択します。

    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。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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 "Google Cloudでシステムをサイジングする"。
12. * Flash Cache、書き込み速度、WORM * ：
    a. 必要に応じて、「Flash Cache」*を有効にします。

Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"。

「* High * write speed」オプションを使用すると、高速な書き込み速度と最大伝送ユニット（MTU）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。VPC-1、VPC-2、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

c. 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。

Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"。

a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloud Platformでのデータ階層化*：最初のアグリゲートでデータの階層化を有効にするかどうかを選択し、階層化されたデータのストレージクラスを選択してから、事前に定義されたストレージ管理者ロール（Cloud Volumes ONTAP 9.7以降で必要）を持つサービスアカウントを選択します。または、Google Cloudアカウントを選択します（Cloud Volumes ONTAP 9.6に必要）。

次の点に注意してください。

- Cloud Volumes ONTAP インスタンスでサービスアカウントを設定します。このサービスアカウントは、 Google Cloud Storage バケットへのデータ階層化の権限を提供します。Connectorサービスアカウントを階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXPから選択できません
- Google Cloudアカウントの追加については、を参照してください "9.6でのデータ階層化用にGoogle Cloudアカウントを設定および追加します"。
- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloudコンソールからサービスアカウントを追加する必要があります。

"データ階層化の詳細については、こちらをご覧ください。"。

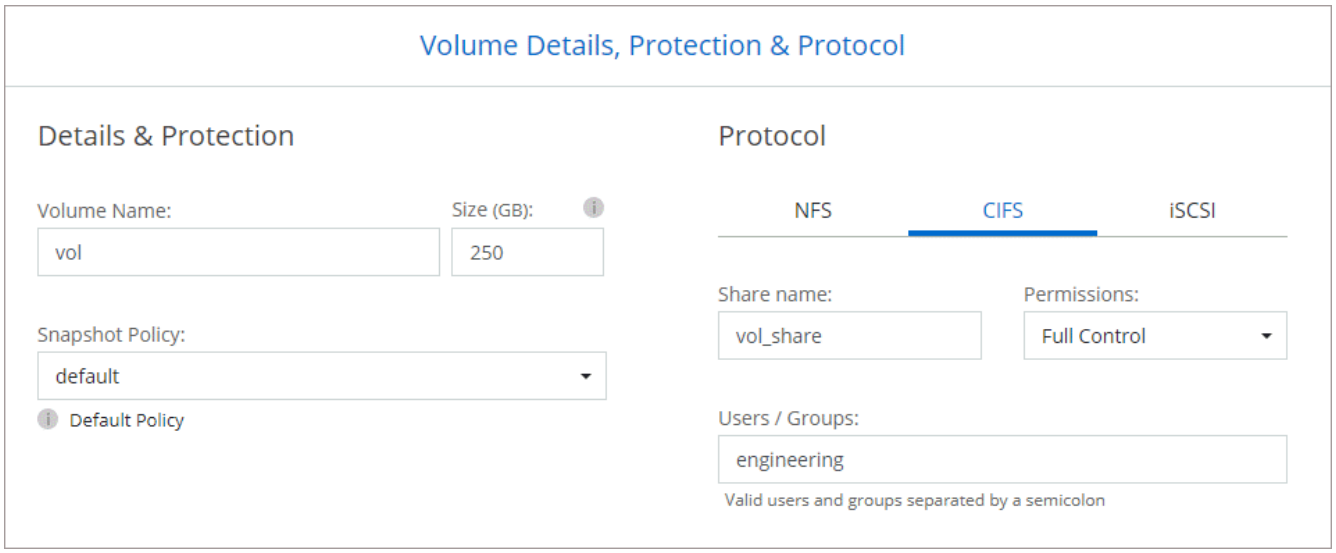
14. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

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、BlueXP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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



15. * 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。 Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。
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。 Google 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=Cloud 」と入力します。 "Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"
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。

フィールド	説明
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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * 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. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    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

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Google CloudでのHAペアの起動

BlueXPで作業環境を作成し、Cloud Volumes ONTAP をGoogle Cloudで起動します。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
3. * 場所を選択 * ：「 * Google Cloud * 」と「 * Cloud Volumes ONTAP HA * 」を選択します。

4. * 詳細と認証情報 * ：プロジェクトを選択し、クラスタ名を指定します。必要に応じてサービスアカウントを選択し、ラベルを追加し、クレデンシャルを指定することもできます。

   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
作業環境名	BlueXPは、作業環境名を使用して、Cloud Volumes ONTAP システムとGoogle Cloud 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。
サービスアカウント名	を使用する場合は "BlueXPの階層化" または "BlueXPのバックアップとリカバリ" サービスを利用するには、 * Service Account * スイッチを有効にし、事前定義された Storage Admin ロールが割り当てられたサービスアカウントを選択する必要があります。
ラベルを追加します	ラベルは、Google Cloudリソースのメタデータです。BlueXPは、システムに関連付けられているCloud Volumes ONTAP システムとGoogle Cloudリソースにラベルを追加します。 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"。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者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。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
プロジェクトを編集します	Cloud Volumes ONTAP を配置するプロジェクトを選択します。既定のプロジェクトは、BlueXPが存在するプロジェクトです。 ドロップダウンリストに他のプロジェクトが表示されない場合は、まだBlueXP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。BlueXPロールを持つ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、BlueXP用に設定したサービスアカウントです。 "このページで説明されているように"。 [サブスクリプションの追加] をクリックして、選択した資格情報をサブスクリプションに関連付けます。 従量課金制のCloud Volumes ONTAP システムを作成するには、Google Cloud MarketplaceからCloud Volumes ONTAP へのサブスクリプションに関連付けられているGoogle Cloudプロジェクトを選択する必要があります。

次のビデオでは、従量課金制のMarketplaceサブスクリプションをGoogle Cloudプロジェクトに関連付ける方法を紹介します。 または、の手順に従って、に登録します "Marketplaceサブスクリプション

とGoogle Cloudクレデンシャルの関連付け" セクション。

► https://docs.netapp.com/ja-jp/test//media/video_subscribing_gcp.mp4 *(video)*

5. * サービス * ：このシステムで使用するサービスを選択します。BlueXPのバックアップとリカバリを選択するか、BlueXP階層化を使用するには、ステップ3でサービスアカウントを指定しておく必要があります。

   WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. *HA 配置モデル *: HA 構成用に複数のゾーン (推奨) または単一ゾーンを選択します。次に、リージョンとゾーンを選択します。

   "HA 導入モデルの詳細については、こちらをご覧ください"。

7. * 接続 * ： HA 構成の場合は 4 つの VPC 、各 VPC のサブネットを選択し、ファイアウォールポリシーを選択します。

   "ネットワーク要件の詳細については、こちらをご覧ください"。

   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
ポリシーが生成されました	BlueXPがファイアウォールポリシーを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。 • 「* Selected VPC Only *」を選択した場合、インバウンドトラフィックのソースフィルタは、選択したVPCのサブネット範囲とコネクタが存在するVPCのサブネット範囲になります。これが推奨されるオプションです。 • どのVPC *も選択した場合、インバウンドトラフィックのソースフィルタは0.0.0.0/0のIP範囲になります。
既存のを使用します	既存のファイアウォールポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAP のファイアウォールルールについて説明します"。

8. * 課金方法と NSS アカウント * ：このシステムで使用する課金オプションを指定し、NetApp Support Site のアカウントを指定します。
   - "Cloud Volumes ONTAP のライセンスオプションについて説明します"。
   - "ライセンスの設定方法について説明します"。
9. * 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。

10. ライセンス：必要に応じてCloud Volumes ONTAP バージョンを変更し、マシンタイプを選択します。

選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。たとえば、 9.6 から 9.7 への更新など、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、つまりディスクタイプと各ディスクのサイズを選択します。

    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。

    シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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 "Google Cloudでシステムをサイジングする"。

12. * Flash Cache、書き込み速度、WORM * ：

    a. 必要に応じて、「Flash Cache」*を有効にします。

    Cloud Volumes ONTAP 9.13.1以降では、n2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64インスタンスタイプで_Flash Cache_が サポートされます。導入後にFlash Cacheを無効にすることはできません。

    b. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

    "書き込み速度の詳細については、こちらをご覧ください。"。

    インスタンスタイプn2-standard-16、n2-standard-32、n2-standard-48、およびn2-standard-64では、* High * write speedオプションを使用して、高速の書き込み速度とより高いMaximum Transmission Unit（MTU；最大伝送ユニット）8、896バイトを使用できます。また、MTUが8、896の場合は、導入環境でVPC-1、VPC-2、およびVPC-3を選択する必要があります。高速の書き込み速度とMTU 8、896は機能に依存し、設定されたインスタンス内で個別に無効にすることはできません。VPC-1、VPC-2、およびVPC-3の詳細については、を参照してください "VPC -1、VPC -2、およびVPC -3のルール"。

    c. 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。

    Cloud Volumes ONTAP 9.7以前のバージョンでデータ階層化が有効になっている場合は、WORMを有効にすることはできません。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

    "WORM ストレージの詳細については、こちらをご覧ください。"。

    a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

13. * Google Cloudでのデータ階層化*：最初のアグリゲートでデータの階層化を有効にするかどうかを選択し、階層化データのストレージクラスを選択してから、定義済みのStorage Adminロールを持つサービスアカウントを選択します。

次の点に注意してください。

- Cloud Volumes ONTAP インスタンスでサービスアカウントを設定します。このサービスアカウントは、 Google Cloud Storage バケットへのデータ階層化の権限を提供します。Connectorサービスアカウントを階層化サービスアカウントのユーザーとして追加してください。追加しないと、BlueXPから選択できません。
- ボリュームを作成または編集するときに、特定のボリューム階層化ポリシーを選択できます。
- データの階層化を無効にすると、以降のアグリゲートで有効にすることができますが、システムの電源をオフにして、Google Cloudコンソールからサービスアカウントを追加する必要があります。

  "データ階層化の詳細については、こちらをご覧ください。"。

14. * 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。

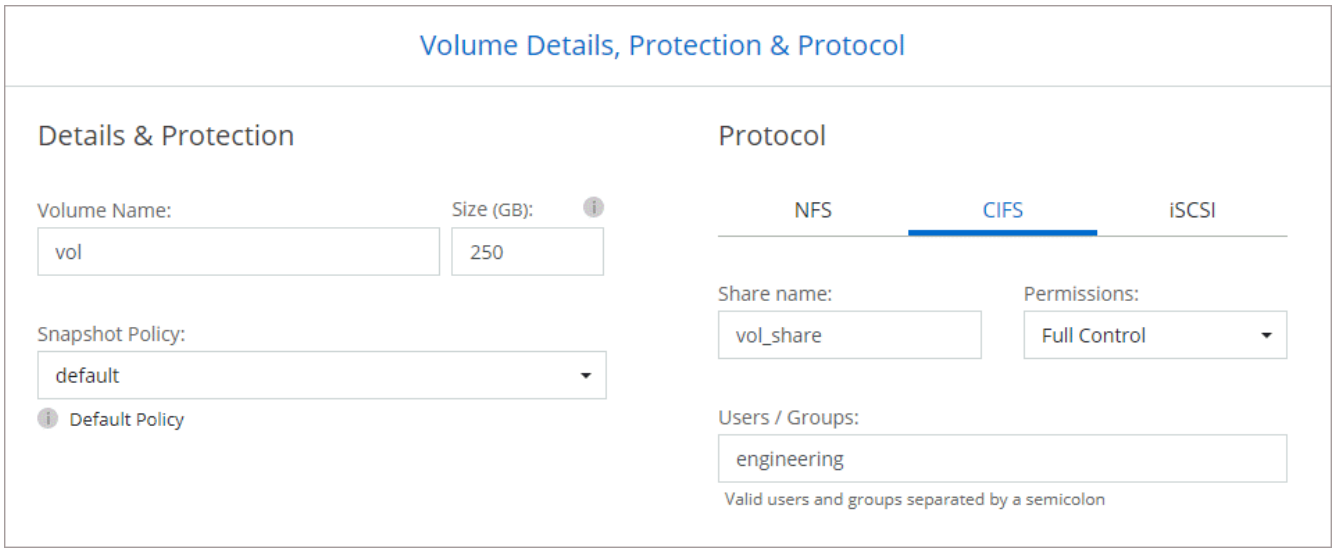
"サポートされるクライアントプロトコルおよびバージョンについて説明します"。

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、BlueXP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。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。

フィールド	説明
イニシエータグループと IQN （ iSCSI のみ）	iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。 イニシエータグループは、 iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。 iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。 iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

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。



15. * 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。 Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。
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 。

フィールド	説明
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。 Google 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=Cloud 」と入力します。 "Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"
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 "BlueXP自動化ドキュメント" を参照してください。 NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

16. * 使用状況プロファイル、ディスクタイプ、階層化ポリシー * ： Storage Efficiency 機能を有効にするかどうかを選択し、必要に応じてボリューム階層化ポリシーを変更します。

    詳細については、を参照してください "ボリュームの使用プロファイルを選択してください" および "データ階層化の概要"。

17. * 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. サポートの詳細とBlueXPが購入するGoogle Cloudのリソースを確認するには、[詳細情報*]をクリックします。
    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

BlueXPがCloud Volumes ONTAP システムを導入しました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。

Google Cloud Platformイメージの検証

Google Cloudの画像検証の概要

Google Cloudのイメージ検証機能は、ネットアップの高度なセキュリティ要件に準拠しています。このタスク用に特別に生成された秘密鍵を使用して、途中でイメージに署名するためのイメージを生成するスクリプトに変更が加えられました。からダウンロードできるGoogle Cloud用の署名済みダイジェストとパブリック証明書を使用して、GCPイメージの整合性を検証できます "NSS" 特定のリリースの場合。

Google Cloudイメージの検証は、Cloud Volumes ONTAP ソフトウェアバージョン9.13.0以降でサポートされています。

Google Cloudで画像をRAW形式に変換します

新しいインスタンスの導入、アップグレード、または既存のイメージで使用されているイメージは、を通じてクライアントと共有されます "NetApp Support Site （NSS）"。署名済みダイジェストと証明書は、NSSポータルからダウンロードできます。ネットアップサポートが共有しているイメージに対応する、適切なリリースのダイジェストと証明書をダウンロードしていることを確認してください。たとえば、9.13.0イメージには、9.13.0署名付きダイジェストとNSSで使用できる証明書があります。

この手順が必要なのはなぜですか？

Google Cloudからの画像は直接ダウンロードできません。署名済みダイジェストと証明書と照合してイメージを検証するには、2つのファイルを比較してイメージをダウンロードするメカニズムが必要です。これを行うには、画像をdisk.raw形式にエクスポート/変換し、結果をGoogle Cloudのストレージバケットに保存する必要があります。disk.rawファイルは、処理中にtarredおよびgzipされます。

ユーザ/サービスアカウントには、次の操作を実行するための権限が必要です。

- Googleストレージバケットへのアクセス
- Google Storageバケットに書き込みます
- クラウドビルドジョブの作成（エクスポートプロセスで使用）
- 目的の画像へのアクセス
- イメージのエクスポートタスクを作成します

イメージを検証するには、disk.raw形式に変換してからダウンロードする必要があります。

Google Cloudのコマンドラインを使用して、**Google Cloud**イメージをエクスポートします

Cloud Storageにイメージをエクスポートする場合は、を使用することを推奨します "gcloud compute images exportコマンド"。このコマンドは、提供されたイメージを取得し、tarredおよびgzipされるdisk.rawファイルに変換します。生成されたファイルは保存先URLに保存され、ダウンロードして検証することができます。

この処理を実行するには、ユーザ/アカウントに目的のバケットへのアクセスと書き込み、イメージのエクスポート、およびクラウドビルド（Googleがイメージのエクスポートに使用）の権限が必要です。

- gcloud *を使用してGoogle Cloudイメージをエクスポートします

をクリックしてスクリプトを表示します

```
$ gcloud compute images export \
    --destination-uri DESTINATION_URI \
    --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
    --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
    --image example-user-20230120115139


## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxx?project=xxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```
[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
```

```
StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."
```

```
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished export in  48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: <serial-output key:'target-size-gb'
value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running
step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-
25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-
export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step
"copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step
"delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk"
(IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-
size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-
size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning
up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished
cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz


# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION
```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to
file://CVO_GCP_Signed_Digest.tar.gz
  Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s

Average throughput: 213.3MiB/s
$ ls -l
total 1565036
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44
CVO_GCP_Signed_Digest.tar.gz
```

圧縮されたファイルを抽出します

```
# Extracting files from the digest
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```

を参照してください "画像のエクスポートに関するGoogle Cloudドキュメント" Google Cloudを使用して画像をエクスポートする方法の詳細については、を参照してください。

画像署名の検証

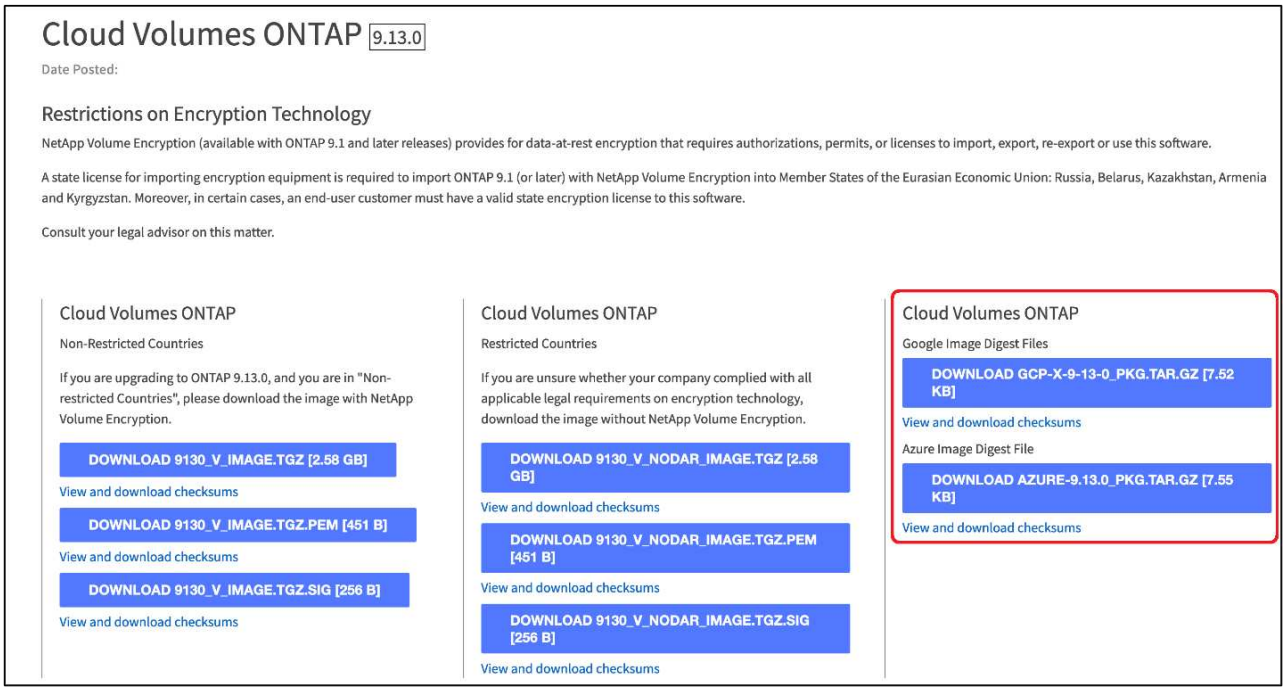
Google Cloudの署名済みイメージを検証します

エクスポートされたGoogle Cloud署名済みイメージを確認するには、NSSからイメージダイジェストファイルをダウンロードして、disk.rawファイルとダイジェストファイルの内容を検証する必要があります。

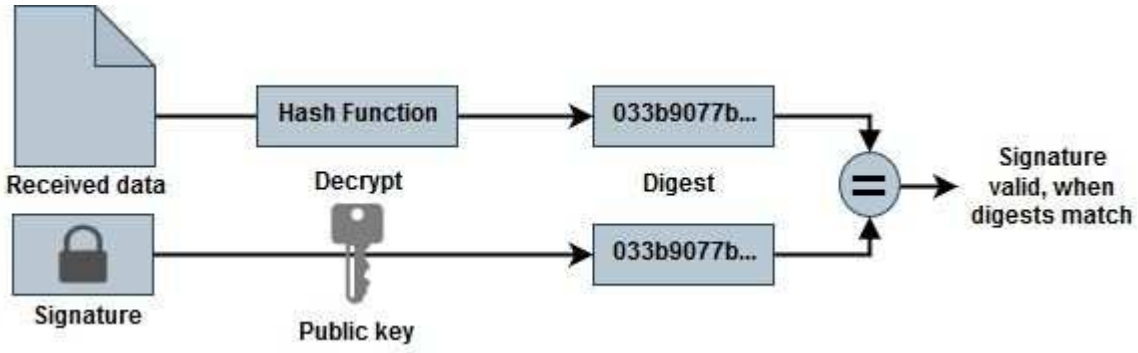
署名済み画像検証ワークフローの概要

以下は、Google Cloudの署名付き画像検証ワークフロープロセスの概要です。

- から "NSS"次のファイルを含むGoogle Cloudアーカイブをダウンロードします。
  - 署名付きダイジェスト（.sig）
  - 公開鍵（.pem）を含む証明書
  - 証明書チェーン（.pem）



- 変換されたdisk.rawファイルをダウンロードします
- 証明書チェーンを使用して証明書を検証します
- 証明書に公開鍵が含まれていることを使用して、署名済みダイジェストを検証します
  - 公開鍵を使用して署名済みダイジェストを復号化し、イメージファイルのダイジェストを抽出します
  - ダウンロードしたdisk.rawファイルのダイジェストを作成します
  - 2つのダイジェストファイルを比較して検証します



OpenSSLを使用した**disk.raw**ファイルおよびダイジェストファイルの内容の検証

Google Cloudでダウンロードしたdisk.rawファイルを、で使用できるダイジェストファイルの内容と照合して確認できます "NSS" OpenSSLを使用しています。

イメージがLinux、Mac OS、およびWindowsマシンと互換性があるかどうかを検証するOpenSSLコマンド。

手順

1. OpenSSLを使用して証明書を確認します。

をクリックしてスクリプトを表示します

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OCSP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OCSP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${ocsp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem  -url ${ocsp_url} -resp_text
-respout resp.der
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
    Produced At: Jan 19 15:14:00 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A
      Issuer Key Hash: CE894F8251AA15A28462CA312361D261FBF8FE78
      Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5
    Cert Status: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

    Signature Algorithm: sha512WithRSAEncryption
         0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
         f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
         af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
         1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
         d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
         cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
         1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
         15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
         8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
         e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
         5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
         b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
         9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
         24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
         5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
         2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
         17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
         d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
         15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
         44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
         cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
         e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
         6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
         77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:
```

```
          e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
          22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
          38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
          fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
          bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
    This Update: Jan 19 15:00:00 2023 GMT
    Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK
```

2. ダウンロードしたdisk.rawファイル、署名、および証明書をディレクトリに配置します。
3. OpenSSLを使用して証明書から公開鍵を抽出します。
4. 抽出した公開鍵を使用して署名を復号化し、ダウンロードしたdisk.rawファイルの内容を確認します。

をクリックしてスクリプトを表示します

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Cloud Volumes ONTAP を使用します

ライセンス管理

容量ベースのライセンスを管理します

BlueXPデジタルウォレットから容量ベースライセンスを管理して、ネットアップアカウントにCloud Volumes ONTAP システム用の十分な容量を確保します。

_ 容量ベースのライセンス _ 容量単位の Cloud Volumes ONTAP に対する支払いが可能。

BlueXPデジタルウォレット_を使用すると、Cloud Volumes ONTAP のライセンスを1つの場所から管理できます。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

BlueXPデジタルウォレットへのライセンスの追加方法

ネットアップの営業担当者からライセンスを購入されると、ネットアップからシリアル番号と追加のライセンス情報を記載したEメールが送信されます。

一方、BlueXPは、ネットアップのライセンスサービスに自動的に問い合わせて、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

BlueXPでライセンスを追加できない場合は、手動でライセンスをデジタルウォレットに追加する必要があります。たとえば、インターネットにアクセスできない場所にConnectorがインストールされている場合は、ライセンスを自分で追加する必要があります。 購入済みライセンスをアカウントに追加する方法について説明します。

アカウントの使用済み容量を表示します

BlueXPのデジタルウォレットには、アカウントの消費容量の合計と、ライセンスパッケージの消費容量が表示されます。この情報は、料金の支払い方法や、容量の追加購入が必要かどうかを把握するのに役立ちます。

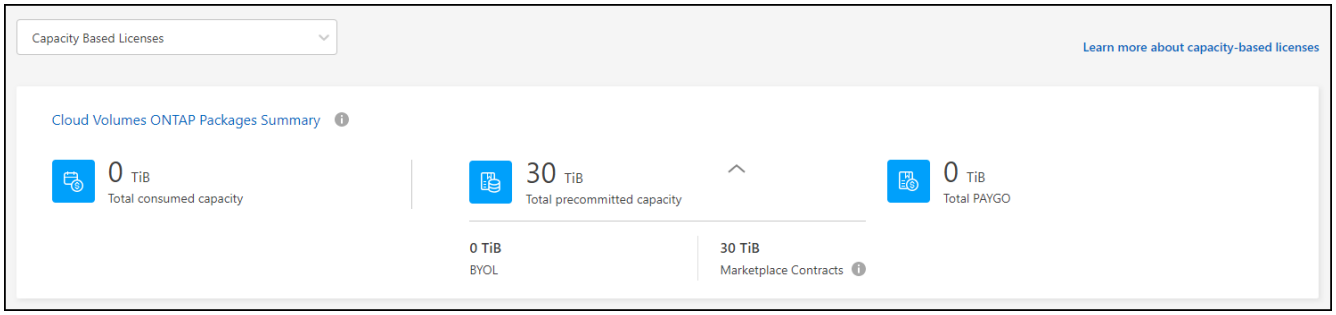
手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. Cloud Volumes ONTAP タブで、 Capacity Based Licenses *を選択したままにします。
3. パッケージの概要を確認します。この概要には、消費容量、事前コミット済み容量の合計、従量課金制の合計容量が表示されます。

    - Total Consumed capacity_は、ネットアップアカウントのすべてのCloud Volumes ONTAP システムのプロビジョニング済み総容量です。充電は、ボリューム内のローカルスペース、使用済みスペース、格納済みスペース、または有効なスペースに関係なく、各ボリュームにプロビジョニングされたサイズに基づいて行われます。
    - _Total precommitted capacity_は、ネットアップから購入したライセンスで許可された容量（BYOLまたはマーケットプレイス契約）の合計です。
    - _従量課金制の合計_は、クラウドマーケットプレイスのサブスクリプションを使用してプロビジョニ

ングされた合計容量です。PAYGOによる課金は、消費容量がライセンスで許可された容量を超えている場合、またはBlueXPデジタルウォレットに使用可能なBYOLライセンスがない場合にのみ使用されます。

BlueXPデジタルウォレットに含まれるCloud Volumes ONTAP パッケージの概要の例を次に示します。



4. ライセンスパッケージごとの使用済み容量を表示します。

   ◦ 消費容量_パッケージのボリュームの容量を表示します。特定のパッケージの詳細を表示するには、ツールチップの上にマウスポインタを置きます。

   Essentialsパッケージに表示される容量を理解するには、充電の仕組みを理解しておく必要があります。 "Essentialsパッケージの充電について説明します"。

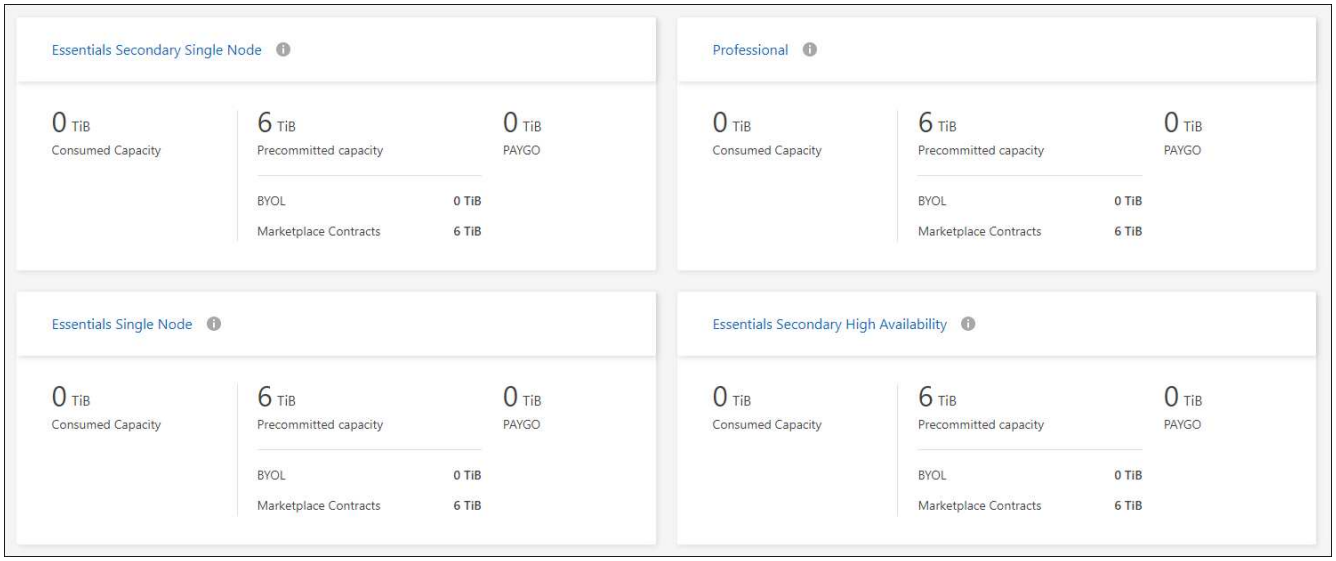
   ◦ _推奨容量_は、ネットアップから購入したライセンス容量（BYOLまたはマーケットプレイス契約）です。

      ▪ _BYOL_このパッケージタイプに対してネットアップから購入したライセンス容量を表示します。

      ▪ _Marketplace契約_このパッケージタイプのマーケットプレイス契約で購入したライセンス容量を表示します。

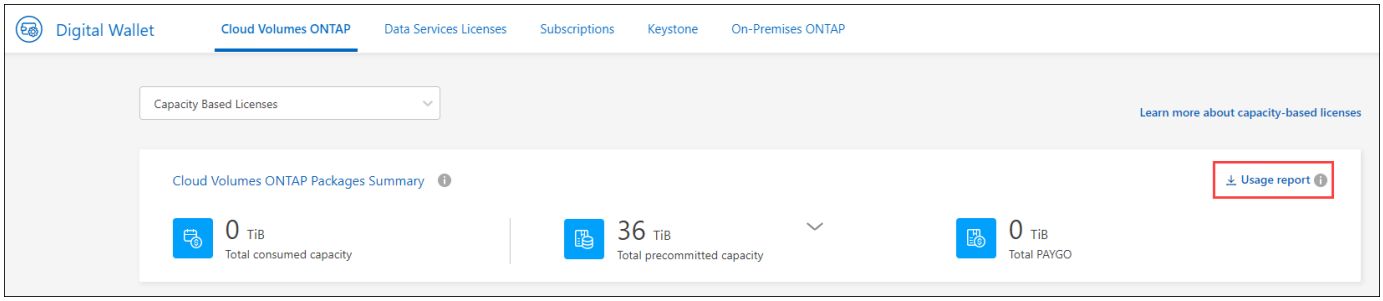
   ◦ _PAYGO_ライセンス消費モデル別の消費容量を表示します。

   次に、複数のライセンスパッケージがあるアカウントの例を示します。



使用状況レポートをダウンロードします

アカウント管理者は、BlueXPのデジタルウォレットから4つの使用状況レポートをダウンロードできます。これらの使用状況レポートには、サブスクリプションの容量の詳細と、Cloud Volumes ONTAP サブスクリプションのリソースに対する課金方法が表示されます。ダウンロード可能なレポートは、特定の時点のデータをキャプチャし、他のユーザーと簡単に共有できます。



以下のレポートをダウンロードできます。容量の値はTiB単位です。

- 使用状況の概要：このレポートには、デジタルウォレットの「Cloud Volumes ONTAP Packages Summary」カードの内容が正確に表示されます。次の情報が含まれています。
  - 合計消費容量
  - 事前コミット済み容量の合計
  - BYOLの合計容量
  - マーケットプレイス契約の合計容量
  - PAYGOの合計容量
- * Cloud Volumes ONTAP パッケージの使用状況*：このレポートには、デジタルウォレット内のパッケージカードに記載されている内容が正確に表示されます。最適化されたI/Oパッケージを除く各パッケージについて、次の情報が含まれています。
  - 合計消費容量
  - 事前コミット済み容量の合計
  - BYOLの合計容量
  - マーケットプレイス契約の合計容量
  - PAYGOの合計容量
- * Storage VMの使用量*：このレポートは、Cloud Volumes ONTAP システムとStorage Virtual Machine（SVM）全体で、課金された容量の内訳を表示します。この情報は、デジタルウォレットのどの画面にも表示されません。次の情報が含まれています。
  - 作業環境のIDと名前（UUIDとして表示）
  - クラウド
  - ネットアップアカウントID
  - 作業環境の設定
  - SVM 名
  - プロビジョニングされた容量

- 充電容量のまとめ
- マーケットプレイスの請求期間
- Cloud Volumes ONTAP パッケージまたは機能
- 課金SaaS Marketplaceサブスクリプション名
- 課金SaaS MarketplaceサブスクリプションID
- ワークロードの種類

- ボリュームの使用量：このレポートは、使用済み容量が作業環境内のボリューム別に内訳で表示されます。この情報は、デジタルウォレットのどの画面にも表示されません。次の情報が含まれています。
  - 作業環境のIDと名前（UUIDとして表示）
  - SVN名
  - ボリューム ID
  - ボリュームタイプ
  - ボリュームのプロビジョニング済み容量

    FlexCloneボリュームは料金が発生しないため、このレポートには含まれていません。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. Cloud Volumes ONTAP タブで、 Capacity Based Licenses を選択したまま Usage report *をクリックします。

   使用状況レポートがダウンロードされます。
3. ダウンロードしたファイルを開き、レポートにアクセスします。

購入済みライセンスをアカウントに追加します

購入したライセンスがBlueXPデジタルウォレットに表示されない場合は、Cloud Volumes ONTAP で使用できる容量を確保するために、ライセンスをBlueXPに追加する必要があります。

必要なもの

- ライセンスファイルまたはライセンスファイルのシリアル番号をBlueXPに提供する必要があります。
- シリアル番号を入力する場合は、最初にが必要です "NetApp Support Site アカウントをBlueXPに追加します"。シリアル番号へのアクセスが許可されているNetApp Support Siteのアカウントです。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [* Cloud Volumes ONTAP （ライセンスの追加）]タブで、[*容量ベースのライセンス]を選択したまま、[*ライセンスの追加]をクリックします。
3. 容量ベースのライセンスのシリアル番号を入力するか、ライセンスファイルをアップロードしてください。

   シリアル番号を入力した場合は、シリアル番号へのアクセス権を持つNetApp Support Siteのアカウントも

選択する必要があります。

4. [ライセンスの追加] をクリックします。

容量ベースのライセンスを更新する

容量を追加購入した場合やライセンスの期間を延長した場合は、デジタルウォレット内のライセンスがBlueXPによって自動的に更新されます。必要なことは何もありません。

ただし、インターネットにアクセスできない場所にBlueXPを導入した場合は、BlueXPでライセンスを手動で更新する必要があります。

必要なもの

ライセンスファイル（ HA ペアがある場合は *files* ）。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [ライセンスの更新*（Cloud Volumes ONTAP ）]タブで、ライセンスの横にあるアクションメニューをクリックし、[ライセンスの更新（Update License *）]を選択します。
3. ライセンスファイルをアップロードします。
4. [ライセンスのアップロード] をクリックします。

充電方法を変更します

容量ベースのライセンスを使用するCloud Volumes ONTAP システムの充電方法を変更できます。たとえば、Essentialsパッケージを含むCloud Volumes ONTAP システムを導入した場合、ビジネスニーズの変化に応じて、そのシステムをProfessionalパッケージに変更できます。

制限事項

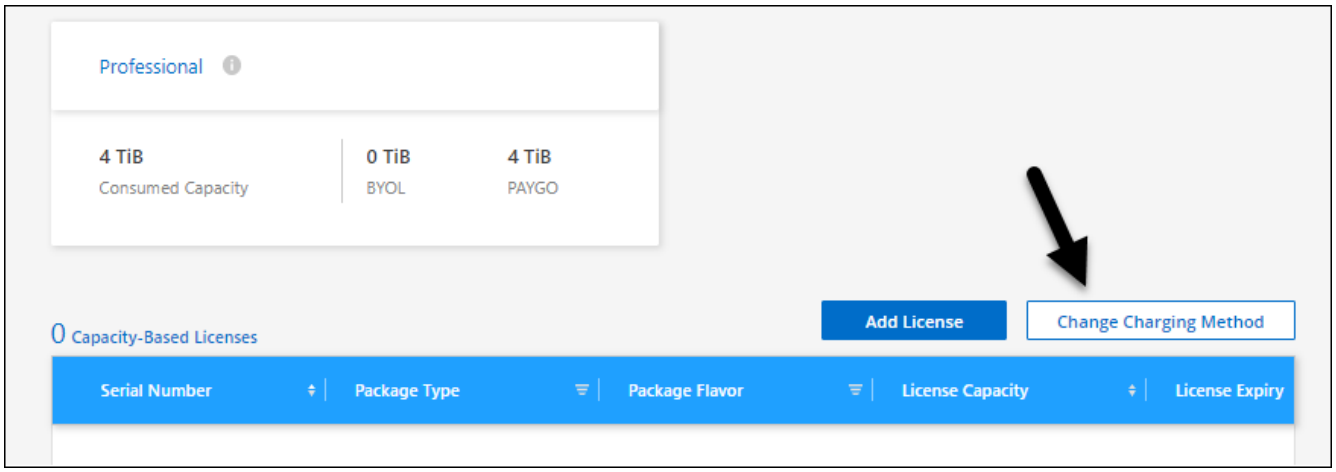
Edge Cacheライセンスとの間での変更はサポートされていません。

重要事項

クラウドプロバイダの市場からプライベートオファーまたは契約を結んでいる場合、契約に含まれていない課金方式に変更すると、BYOL（ネットアップからライセンスを購入した場合）またはPAYGOに対して課金されます。

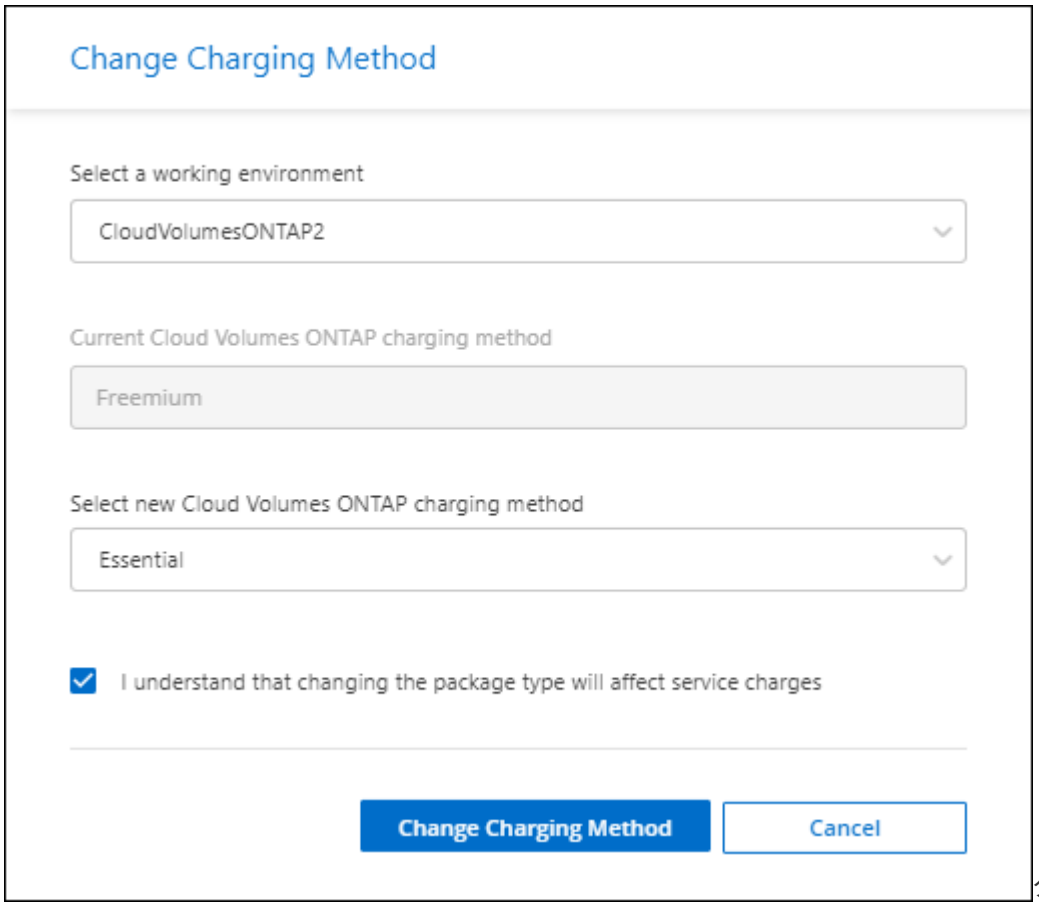
手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [充電方法（Cloud Volumes ONTAP ）]タブで、[*充電方法の変更（* Change Charging method *）]



ボタンがあります。"]

3. 作業環境を選択して新しい充電方法を選択し、パッケージタイプを変更するとサービス料金に影響することを確認します。



ダイアログボックスのスクリーンショット。"]

4. [充電方法の変更*]をクリックします。

結果

BlueXPは、Cloud Volumes ONTAP システムの充電方法を変更します。

また、BlueXPのデジタルウォレットでは、変更に合わせてパッケージタイプごとの消費容量が更新されます。

容量ベースのライセンスを削除する

容量ベースのライセンスの期限が切れて使用できなくなった場合は、いつでも削除できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [ライセンスの削除（Cloud Volumes ONTAP ）]タブで、ライセンスの横にあるアクションメニューをクリックし、[ライセンスの削除（Remove License）]を選択します。
3. [削除（ Remove ）] をクリックして確定します。

Keystoneサブスクリプションの管理

KeystoneサブスクリプションをCloud Volumes ONTAP で使用できるようにすることで、BlueXPのデジタルウォレットから管理できます。コミット済み容量に対する変更を要求したり、サブスクリプションのリンクを解除したりすることもできます。

A_Keystoneサブスクリプション_は、ネットアップが提供する従量課金制のストレージサービスです。

BlueXPデジタルウォレット_を使用すると、Cloud Volumes ONTAP のライセンスを1つの場所から管理できます。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

アカウントを承認します

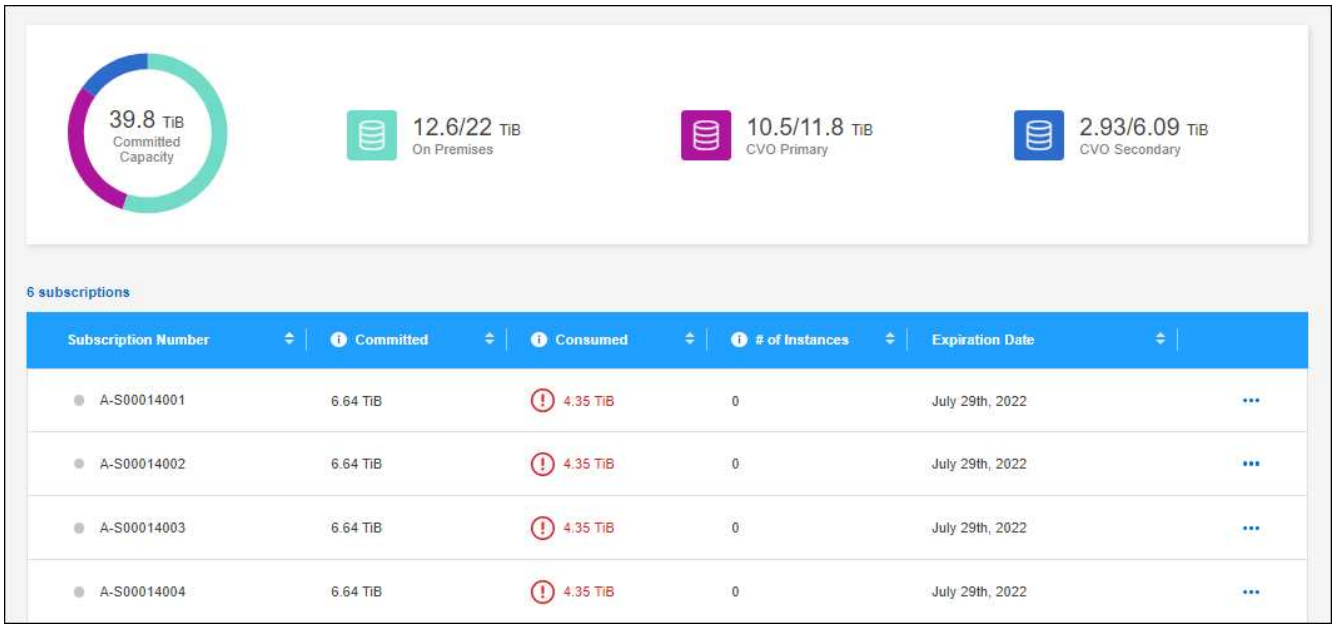
BlueXPでKeystoneサブスクリプションを使用および管理する前に、ネットアップに連絡して、KeystoneサブスクリプションでBlueXPユーザアカウントを承認する必要があります。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [Keystone]*を選択します。
3. 「 NetApp Keystone へようこそ」ページが表示された場合は、ページに記載されているアドレスにメールを送信してください。

   ネットアップの担当者は、お客様のユーザアカウントに登録へのアクセスを許可することで、リクエストを処理します。

4. Keystoneサブスクリプション*に戻ってサブスクリプションを確認してください。



次の手順

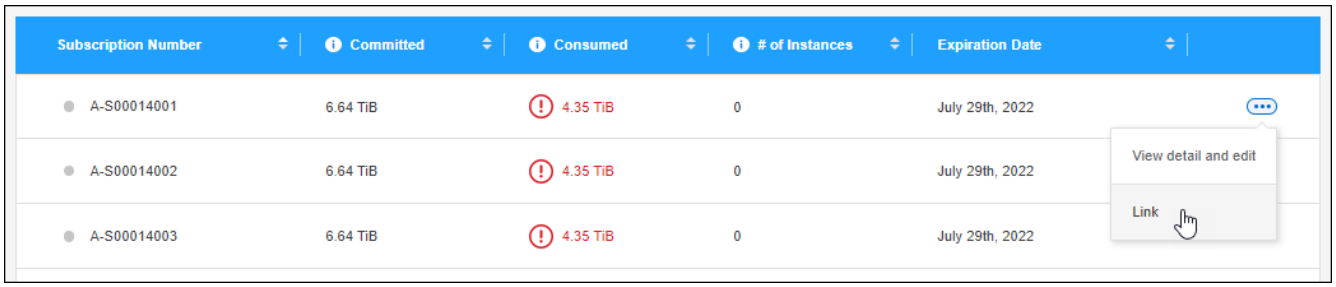
Cloud Volumes ONTAP で使用するサブスクリプションをリンクします。

サブスクリプションをリンクします

ネットアップがお客様のアカウントを承認したら、Cloud Volumes ONTAP で使用するためにKeystoneサブスクリプションをリンクする必要があります。この操作により、新しい Cloud Volumes ONTAP システムの充電方法としてサブスクリプションを選択できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [Keystone]*を選択します。
3. リンクするサブスクリプションの場合は、をクリックします ••• をクリックし、 * Link * を選択します。



結果

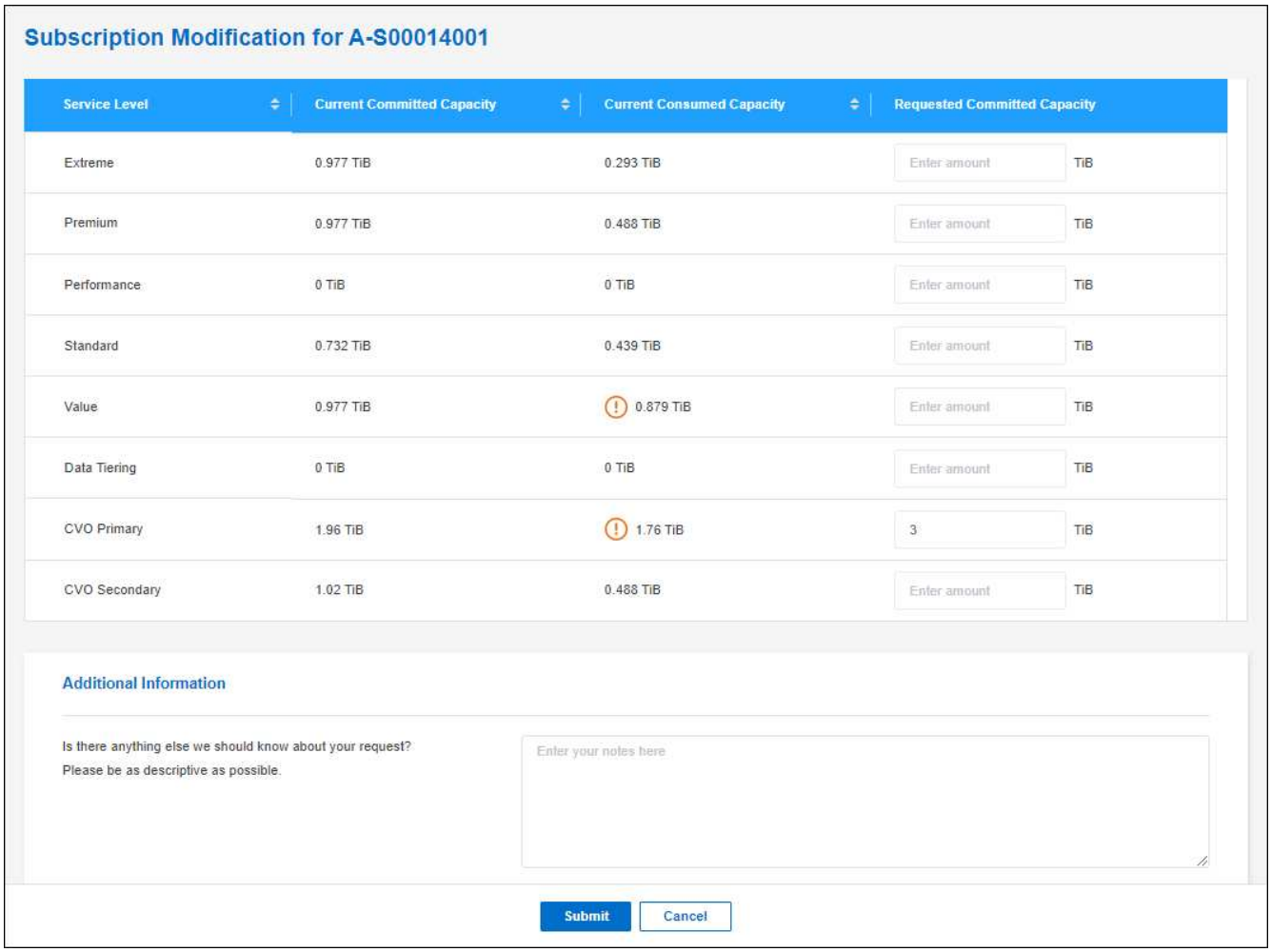
これで、サブスクリプションがBlueXPアカウントにリンクされ、Cloud Volumes ONTAP 作業環境の作成時に選択できるようになりました。

コミット済み容量を増やして申請してください

サブスクリプションのコミット済み容量を調整する必要がある場合は、BlueXPインターフェイスから直接リクエストを送信できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [Keystone]*を選択します。
3. 容量を調整するサブスクリプションの場合、をクリックします ••• をクリックし、 * 詳細を表示して編集 * を選択します。
4. 1 つ以上のサブスクリプションのコミット済み容量を入力します。



5. 下にスクロールしてリクエストの詳細を入力し、 [送信] をクリックします。

結果

リクエストに応じて、ネットアップのシステムで処理用のチケットが作成されます。

サブスクリプションのリンクを解除します

新しいCloud Volumes ONTAP システムでKeystoneサブスクリプションを使用する必要がなくなった場合は、サブスクリプションのリンクを解除できます。既存の Cloud Volumes ONTAP サブスクリプションに関連付けられていないサブスクリプションはリンク解除のみ可能です。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。

2. [Keystone]*を選択します。
3. リンクを解除するサブスクリプションの場合は、をクリックします ••• をクリックし、 * リンク解除 * を選択します。

結果

サブスクリプションがBlueXPアカウントからリンク解除され、Cloud Volumes ONTAP 作業環境の作成時に選択できなくなりました。

ノードベースのライセンスを管理します

BlueXPデジタルウォレットでノードベースライセンスを管理し、各Cloud Volumes ONTAP システムに必要な容量を含む有効なライセンスがあることを確認する。

ノードベースライセンス _ は旧世代のライセンスモデルです（新規のお客様は使用できません）。

- ネットアップから購入した BYOL ライセンス
- クラウドプロバイダの市場から従量課金制（ PAYGO ）で 1 時間単位のサブスクリプションが提供されます

BlueXPデジタルウォレット_を使用すると、Cloud Volumes ONTAP のライセンスを1つの場所から管理できます。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

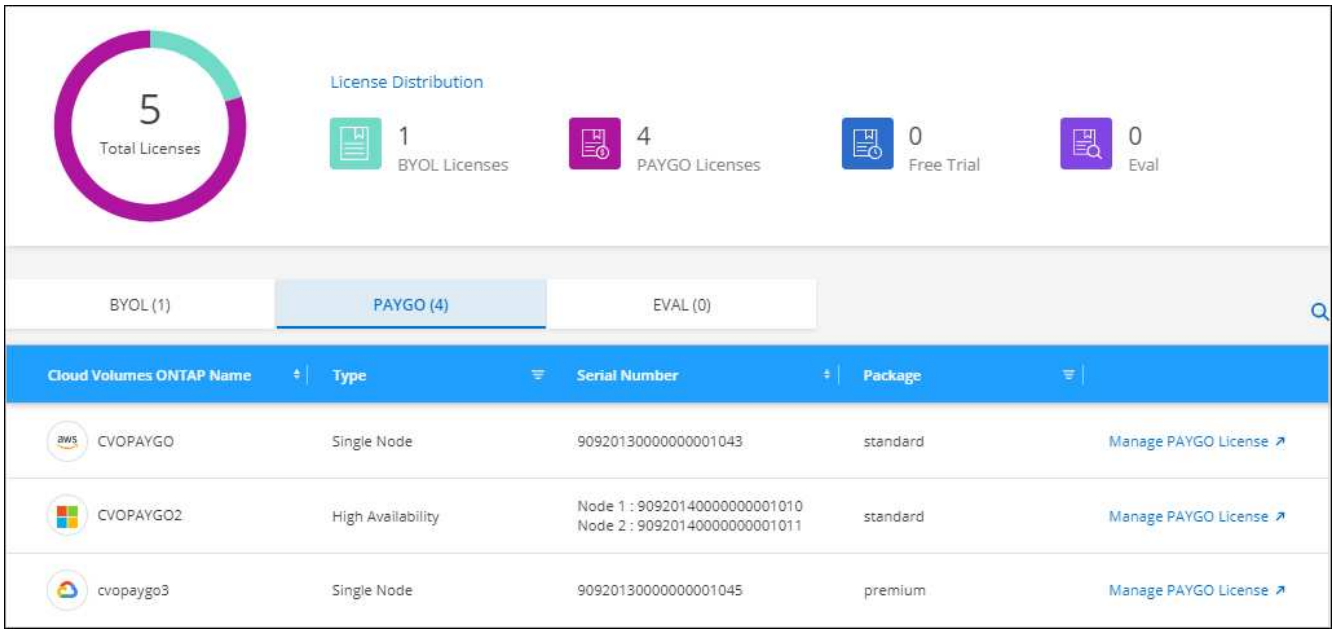
"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

PAYGOライセンスの管理

BlueXPのデジタルウォレットページでは、各PAYGO Cloud Volumes ONTAP システムの詳細（シリアル番号やPAYGOライセンスタイプなど）を確認できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. [PAYGO]*をクリックします。
4. PAYGO ライセンスごとに詳細を表に示します。



5. 必要に応じて、 [PAYGO ライセンスの管理（ Manage PAYGO License ）] をクリックして、 PAYGO ライセンスを変更するか、インスタンスタイプを変更します。

BYOL ライセンスを管理します

システムライセンスと容量ライセンスを追加または削除して、ネットアップから直接購入したライセンスを管理する。

未割り当てのライセンスを追加します

新しいCloud Volumes ONTAP システムの作成時にライセンスを選択できるように、BlueXPデジタルウォレットにノードベースライセンスを追加します。デジタルウォレットは、これらのライセンスを_unassigned_として識別します。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. [* 未割り当て * （ Unassigned * ）]
4. [未割り当てライセンスの追加] をクリックします。
5. ライセンスのシリアル番号を入力するか、ライセンスファイルをアップロードしてください。

   ライセンスファイルがまだない場合は、以下のセクションを参照してください。

6. [ライセンスの追加] をクリックします。

結果

BlueXPはデジタルウォレットにライセンスを追加します。ライセンスは、新しい Cloud Volumes ONTAP システムに関連付けるまでは未割り当てとみなされます。その後、ライセンスはデジタルウォレットの* BYOL *タブに移動します。

未割り当てのノードベースライセンスを交換します

Cloud Volumes ONTAP の未割り当てのノードベースライセンスがある場合は、BlueXPバックアップおよびリカバリライセンス、BlueXP分類ライセンス、またはBlueXP階層化ライセンスに変換することでライセンスを交換できます。

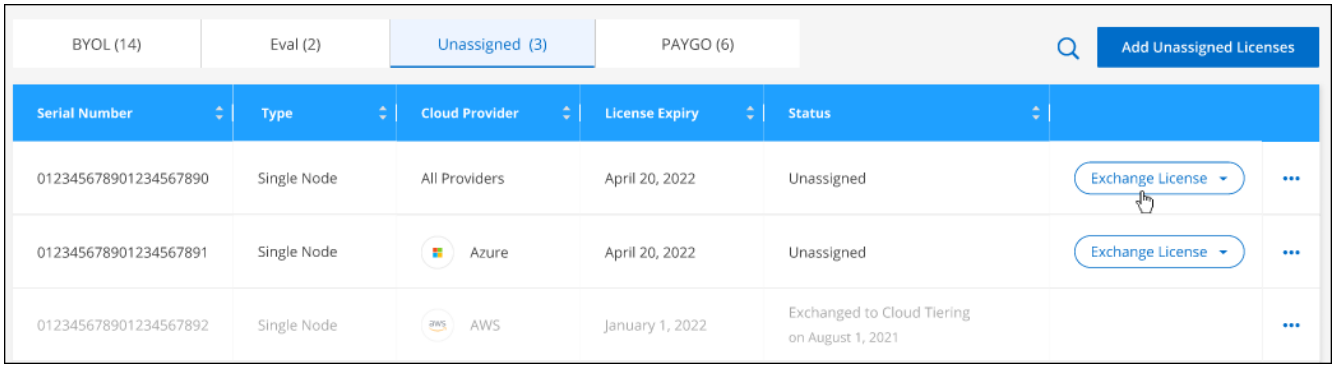
ライセンスを交換すると、 Cloud Volumes ONTAP ライセンスが取り消され、サービスのドル相当ライセンスが作成されます。

- Cloud Volumes ONTAP HA ペアのライセンスは 51TiB のデータサービスライセンスに変換されます
- Cloud Volumes ONTAP シングルノードのライセンスは、 32TiB のデータサービスライセンスに変換されます

変換されたライセンスの有効期限は、 Cloud Volumes ONTAP ライセンスと同じです。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. [* 未割り当て * （ Unassigned * ）]
4. [*Exchange ライセンス *] をクリックします。



5. ライセンスを交換するサービスを選択します。
6. プロンプトが表示されたら、 HA ペア用の追加のライセンスを選択します。
7. 法的同意を読み、 [**Agree**](同意する) をクリックします。

結果

BlueXPは、割り当てられていないライセンスを選択したサービスに変換します。新しいライセンスは、 [* データサービスライセンス *] タブで表示できます。

システムライセンスファイルを取得します

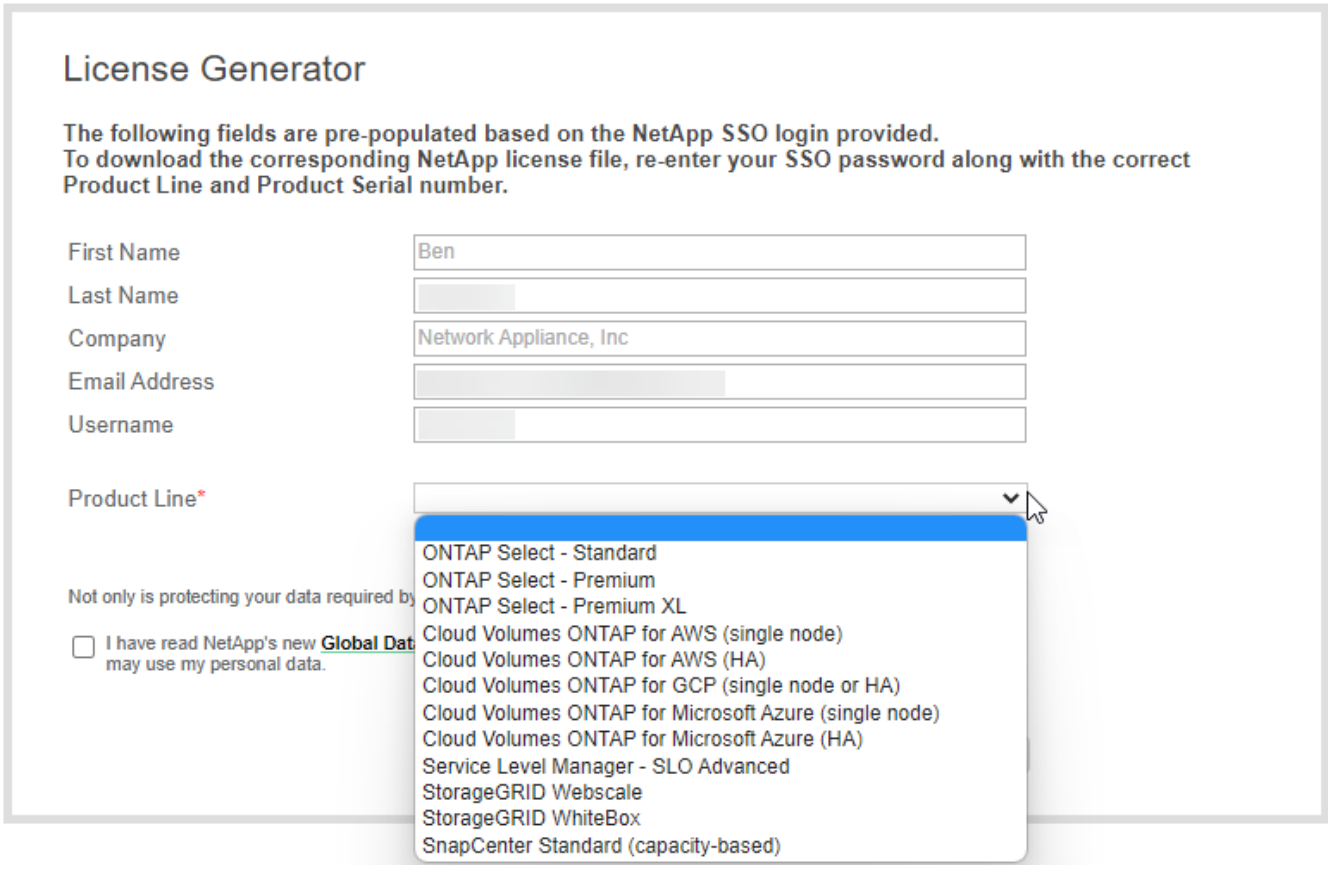
ほとんどの場合、NetApp Support Site アカウントを使用してライセンスファイルを自動的に取得できます。ただし、アップロードできない場合は、ライセンスファイルを手動でアップロードする必要があります。ライセンスファイルがない場合は、 netapp.com から入手できます。

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、NetApp Support Site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。

システムライセンスを更新する

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、BlueXP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てCloud Volumes ONTAP システムにインストールします。

BlueXPがセキュリティ保護された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、自分でファイルを取得し、BlueXPに手動でアップロードできます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. BYOL * タブで、 Cloud Volumes ONTAP システムの詳細を展開します。
4. システムライセンスの横にあるアクションメニューをクリックし、 * ライセンスの更新 * を選択します。
5. ライセンスファイル（ HA ペアがある場合はファイル）をアップロードします。
6. ［ * ライセンスの更新 * ］ をクリックします。

結果

Cloud Volumes ONTAP システムのライセンスが更新されます。

追加の容量ライセンスを管理する

Cloud Volumes ONTAP BYOL システムの追加容量ライセンスを購入すると、 BYOL システムライセンスで提供される 368 TiB を超える容量を割り当てることができます。たとえば、 1 つのライセンス容量を追加購入して、最大 736TiB の容量を Cloud Volumes ONTAP に割り当てることができます。また、容量ライセンスを 3 つ追加購入すれば、最大 1.4 PiB まで拡張できます。

シングルノードシステムまたは HA ペアに対して購入できるライセンスの数に制限はありません。

容量ライセンスを追加

BlueXPの右下にあるチャットアイコンを使って、容量ライセンスを追加購入してください。購入したライセンスは、 Cloud Volumes ONTAP システムに適用できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. BYOL * タブで、 Cloud Volumes ONTAP システムの詳細を展開します。
4. [Add Capacity License*] をクリックします。
5. シリアル番号を入力するか、ライセンスファイル（ HA ペアを使用している場合はファイル）をアップロードします。
6. [Add Capacity License*] をクリックします。

容量ライセンスを更新

容量ライセンスの期間を延長した場合は、BlueXPでライセンスを更新する必要があります。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. BYOL * タブで、 Cloud Volumes ONTAP システムの詳細を展開します。
4. 容量ライセンスの横にあるアクションメニューをクリックし、 * ライセンスの更新 * を選択します。
5. ライセンスファイル（ HA ペアがある場合はファイル）をアップロードします。
6. ［ * ライセンスの更新 * ］ をクリックします。

容量ライセンスを削除します

使用されなくなったために期限切れになった容量ライセンスは、いつでも削除できます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. BYOL * タブで、 Cloud Volumes ONTAP システムの詳細を展開します。

4. 容量ライセンスの横にあるアクションメニューをクリックし、 * ライセンスの削除 * を選択します。
5. [削除（ Remove ）] をクリックします。

評価ライセンスを **BYOL** に変換します

評価用ライセンスは 30 日間有効です。インプレースアップグレードの評価ライセンスの上に、新しい BYOL ライセンスを適用できます。

EvalライセンスをBYOLに変換すると、BlueXPはCloud Volumes ONTAP システムを再起動します。

- シングルノードシステムで再起動を実行すると、リブートプロセス中に I/O が中断されます。
- HA ペアの場合、再起動によってテイクオーバーとギブバックが開始され、クライアントへの I/O の提供が継続されます。

手順

1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. [*Node] Cloud Volumes ONTAP タブで、ドロップダウンから[*Node Based Licenses]を選択します。
3. 「 * 評価 * 」をクリックします。
4. 表で、 Cloud Volumes ONTAP システムの **Convert to BYOL License** をクリックします。
5. シリアル番号を入力するか、ライセンスファイルをアップロードしてください。
6. [ライセンスの変換] をクリックします。

結果

BlueXPが変換プロセスを開始しますCloud Volumes ONTAP は、このプロセスの一環として自動的に再起動します。バックアップが完了すると、ライセンス情報に新しいライセンスが反映されます。

PAYGOと**BYOL**の**2**つのモデルが変わります

システムをPAYGOからノード単位のライセンスからBYOLへ（逆も同様）に変換することはできません。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を切り替える場合は、新しいシステムを導入し、既存のシステムから新しいシステムにデータをレプリケートする必要があります。

手順

1. 新しい Cloud Volumes ONTAP の作業環境を作成します。
2. レプリケートする必要があるボリュームごとに、システム間の1回限りのデータレプリケーションを設定します。

   "システム間でデータをレプリケートする方法について説明します"

3. 元の作業環境を削除して、不要になった Cloud Volumes ONTAP システムを終了します。

   "Cloud Volumes ONTAP 作業環境を削除する方法について説明します"。

ボリュームと **LUN** の管理

FlexVol ボリュームを作成します

初期の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、BlueXPからNFS、CIFS、またはiSCSI用の新しいFlexVol ボリュームを作成できます。

BlueXPでは、いくつかの方法で新しいボリュームを作成できます。

- 新しいボリュームの詳細を指定し、基盤となるデータアグリゲートをBlueXPで処理できるようにします。詳細はこちら。
- 任意のデータアグリゲート上にボリュームを作成します。 詳細はこちら。
- テンプレートからボリュームを作成し、データベースやストリーミングサービスなど特定のアプリケーションのワークロード要件に合わせてボリュームを最適化します。 詳細はこちら。
- HA 構成の第 2 ノードにボリュームを作成する。 詳細はこちら。

始める前に

ボリュームのプロビジョニングに関する注意事項は次のとおりです。

- iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN だけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。
- LUN は、 System Manager または CLI を使用して追加で作成できます。
- 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"。
- Cloud Volumes ONTAP 構成でAmazon EBS Elastic Volumes機能がサポートされている場合は、この処理が必要になることがあります "ボリュームを作成したときの動作の詳細については、こちらをご覧ください"。

ボリュームを作成します

ボリュームを作成する最も一般的な方法は、必要なボリュームのタイプを指定してから、BlueXPがディスク割り当てを処理することです。ボリュームを作成するアグリゲートを選択することもできます。

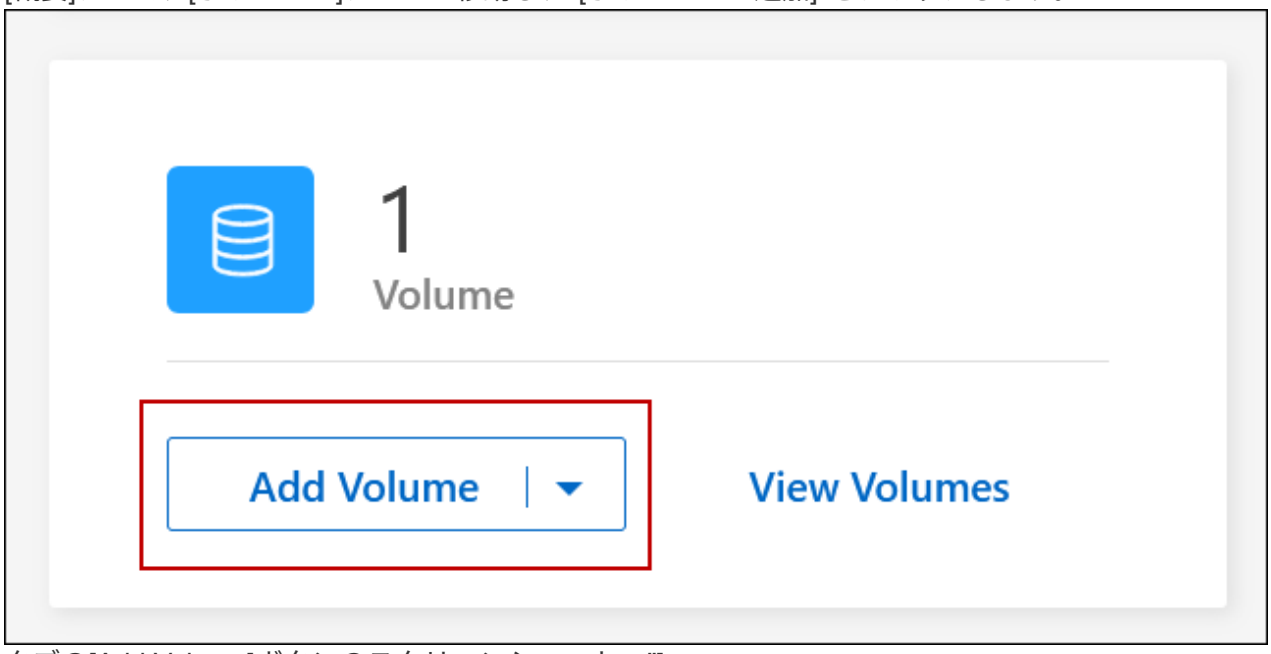
手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、 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。
3. BlueXPにディスク割り当ての処理を許可して新しいボリュームを作成するか、ボリュームの特定のアグリゲートを選択します。

   特定のアグリゲートを選択することが推奨されるのは、 Cloud Volumes ONTAP システムのデータアグリゲートを十分に理解している場合のみです。

任意のアグリゲート

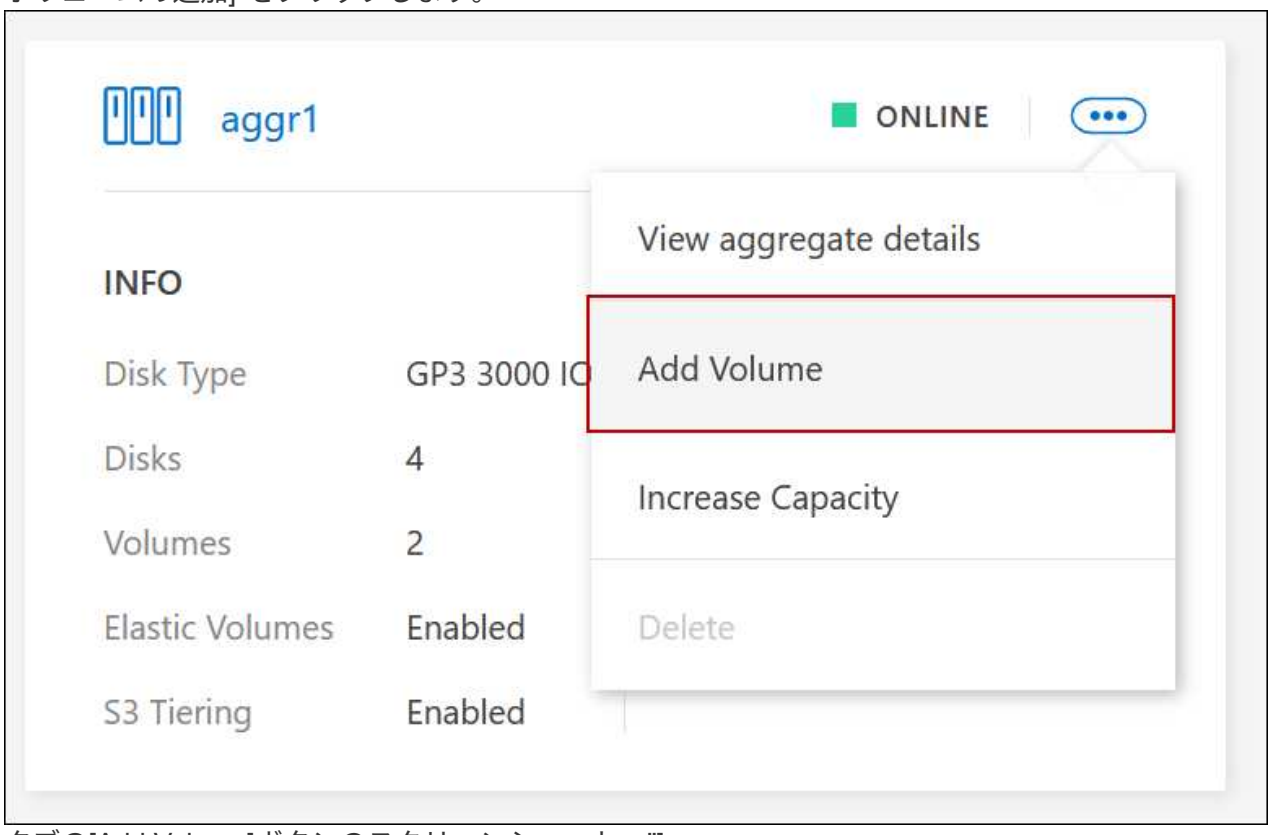
[概要]タブで、[ボリューム]タイルに移動し、*[ボリュームの追加]*をクリックします。



タブの[Add Volume]ボタンのスクリーンショット。"]

特定のアグリゲート

[Aggregates]タブで、目的のアグリゲートタイルに移動します。メニューアイコンをクリックし、*[ボリュームの追加]*をクリックします。



タブの[Add Volume]ボタンのスクリーンショット。"]

4. ウィザードの手順に従って、ボリュームを作成します。

   a. **[ボリューム、詳細、保護、およびタグ]**：ボリュームの基本的な詳細を入力し、Snapshotポリシーを選択します。

      このページのフィールドの一部は分かりやすいもので、説明を必要としません。以下は、説明が必要なフィールドのリストです。

フィールド	説明
ボリューム名	新しいボリュームの識別可能な名前。
ボリュームサイズ	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。
タグ	ボリュームに追加するタグはに関連付けられます "Application Templates サービス"を使用すると、リソースの管理を整理して簡単に行うことができます。
Storage VM（SVM）	Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは SVM または SVM として認識されていることがあります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されますが、一部の設定では追加の Storage VM がサポートされます。新しいボリュームのStorage VMを指定できます。
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。

   b. * プロトコル * ：ボリューム（ NFS 、 CIFS 、または iSCSI ）用のプロトコルを選択し、必要な情報を入力します。

      [CIFS]を選択し、サーバが設定されていない場合は、[Next]をクリックすると、CIFS接続の設定を求めるメッセージが表示されます。

      "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

      以下のセクションでは、説明が必要なフィールドについて説明します。説明はプロトコル別にまとめられています。

NFS

Access Control の略

クライアントがボリュームを使用できるようにするカスタムエクスポートポリシーを選択します。

エクスポートポリシー

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、BlueXP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。

CIFS

権限とユーザ / グループ

ユーザとグループの SMB 共有へのアクセスレベルを制御できます（アクセス制御リストまたは ACL とも呼ばれます）。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 Windows ユーザ名を指定する場合は、 domain\username の形式を使用してユーザのドメインを含める必要があります。

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。

Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。

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。
  "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"
- Google 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=Cloud 」と入力します。
  "Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"

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 "BlueXP自動化ドキュメント" を参照してください。

NTP サーバは、 CIFS サーバを作成するときにのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

iSCSI

LUN

iSCSI ストレージターゲットは LUN （論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN を作成するだけでシンプルになり、管理は不要です。ボリュームを作成したら、 "IQN を使用して、から LUN に接続します ホスト"。

イニシエータグループ

イニシエータグループ（ igroup ）は、ストレージシステム上の指定した LUN にアクセスできるホストを指定します

ホストイニシエータ（ **IQN** ）

iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（ NIC ）、ソフトウェアイニシエータを搭載した TOE カード、 CNA 、または専用の HBA を使用してネットワークに接続され、 iSCSI Qualified Name （ IQN ）で識別されます。

a. * ディスクタイプ * ：パフォーマンスのニーズとコストの要件に基づいて、ボリュームの基盤となるディスクタイプを選択します。
   - "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"
   - "Google Cloudでのシステムのサイジング"

5. * 使用状況プロファイルと階層化ポリシー * ：ボリュームで Storage Efficiency 機能を有効にするか無効にするかを選択し、を選択します "ボリューム階層化ポリシー"。

   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。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。

6. * レビュー * ：ボリュームの詳細を確認して、 * 追加 * をクリックします。

結果

Cloud Volumes ONTAP システムにボリュームが作成されます。

テンプレートからボリュームを作成します

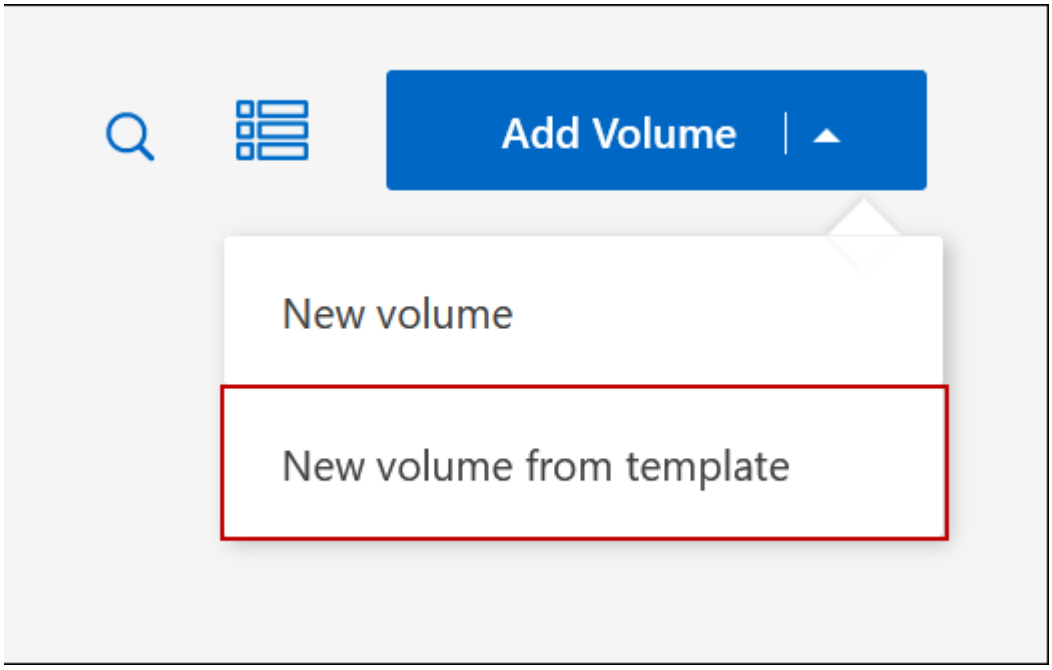
特定のアプリケーションのワークロード要件に最適化されたボリュームを導入できるように、組織で Cloud Volumes ONTAP ボリュームテンプレートを作成している場合は、このセクションの手順に従います。

テンプレートを使用すると、ディスクタイプ、サイズ、プロトコル、スナップショットポリシー、クラウドプロバイダ、 その他。パラメータがすでに事前定義されている場合は、次のボリュームパラメータに進みます。

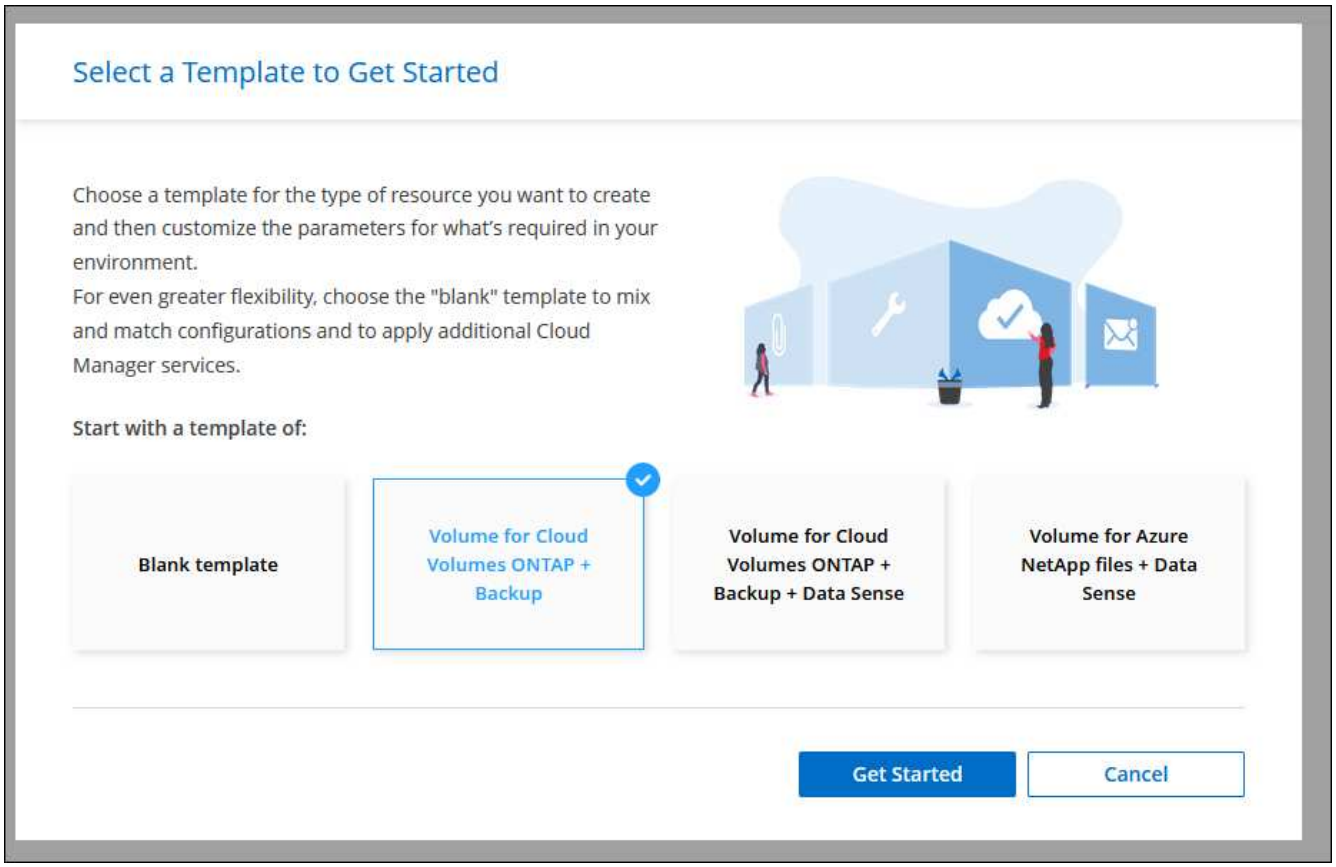
テンプレートを使用する場合にのみ、 NFS ボリュームまたは CIFS ボリュームを作成できます。

手順

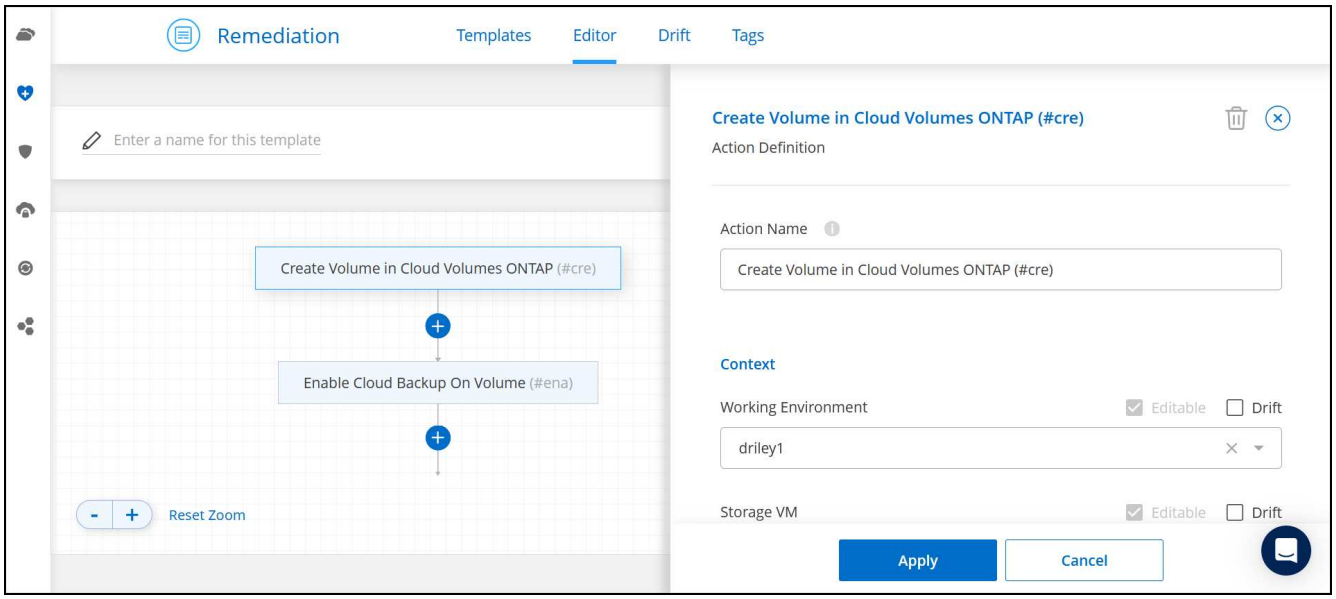
1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、ボリュームをプロビジョニングする Cloud Volumes ONTAP システムの名前をクリックします。
3. [Volumes]タブに移動し、**[Add Volume]**>*[New Volume from Template]*をクリックします。



4. _ テンプレートの選択 _ ページで、ボリュームの作成に使用するテンプレートを選択し、 * 次へ * をクリックします。



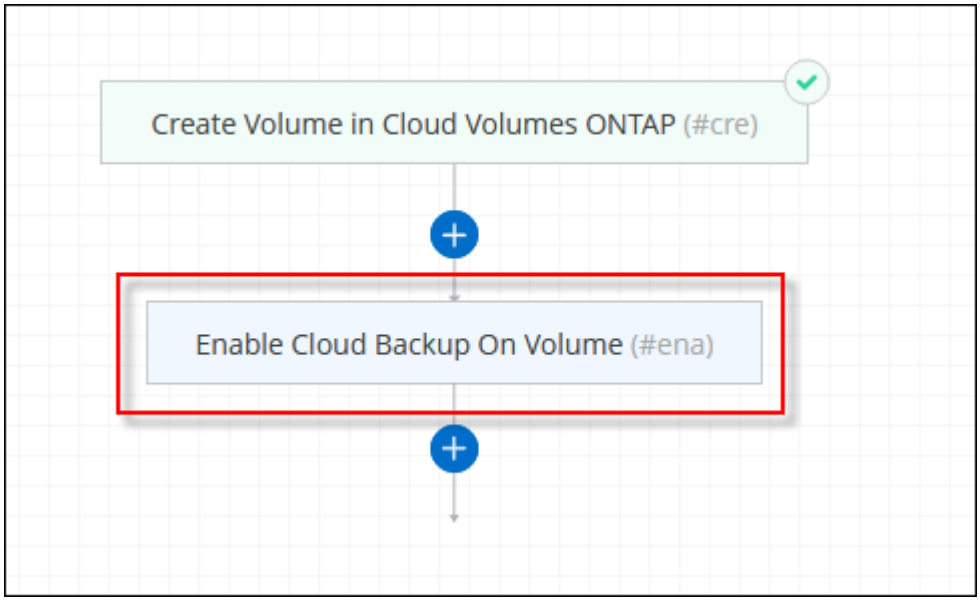
_Editor_pageが表示されます。



5. アクションパネルの上に、テンプレートの名前を入力します。
6. _Context_の下に、を起動した作業環境の名前が作業環境に入力されます。ボリュームを作成する* Storage VM *を選択します。
7. テンプレートからハードコーディングされていないすべてのパラメータに値を追加します。を参照してください ボリュームを作成します Cloud Volumes ONTAP ボリュームの導入を完了するために必要なすべてのパラメータの詳細については、を参照してください。

8. [適用（Apply）]*をクリックして、設定したパラメータを選択したアクションに保存します。
9. 定義する必要のある他の操作（BlueXPのバックアップとリカバリの設定など）がない場合は、*[テンプレートの保存]*をクリックします。

   他のアクションがある場合は、左ペインのアクションをクリックして、完了する必要のあるパラメータを表示します。

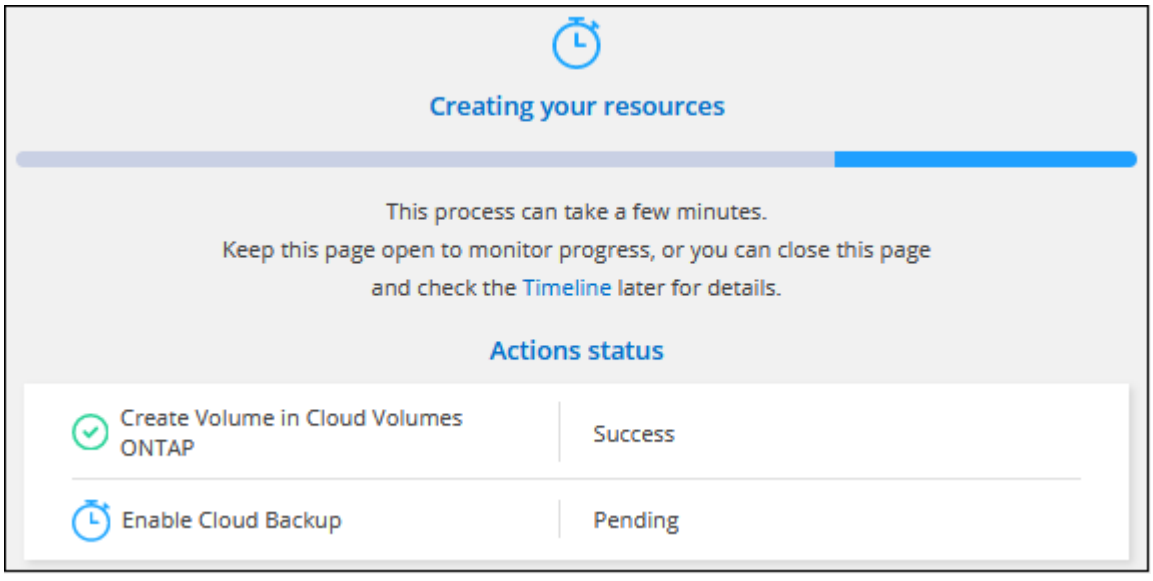


   たとえば、[Enable Cloud Backup on Volume]アクションでバックアップポリシーを選択する必要がある場合は、ここで選択できます。

10. テンプレートアクションの設定が完了したら、*テンプレートの保存*をクリックします。

結果

Cloud Volumes ONTAP によってボリュームがプロビジョニングされ、進捗状況を確認するためのページが表示されます。



また、ボリュームでBlueXPのバックアップとリカバリを有効にするなど、テンプレートにセカンダリアクシ

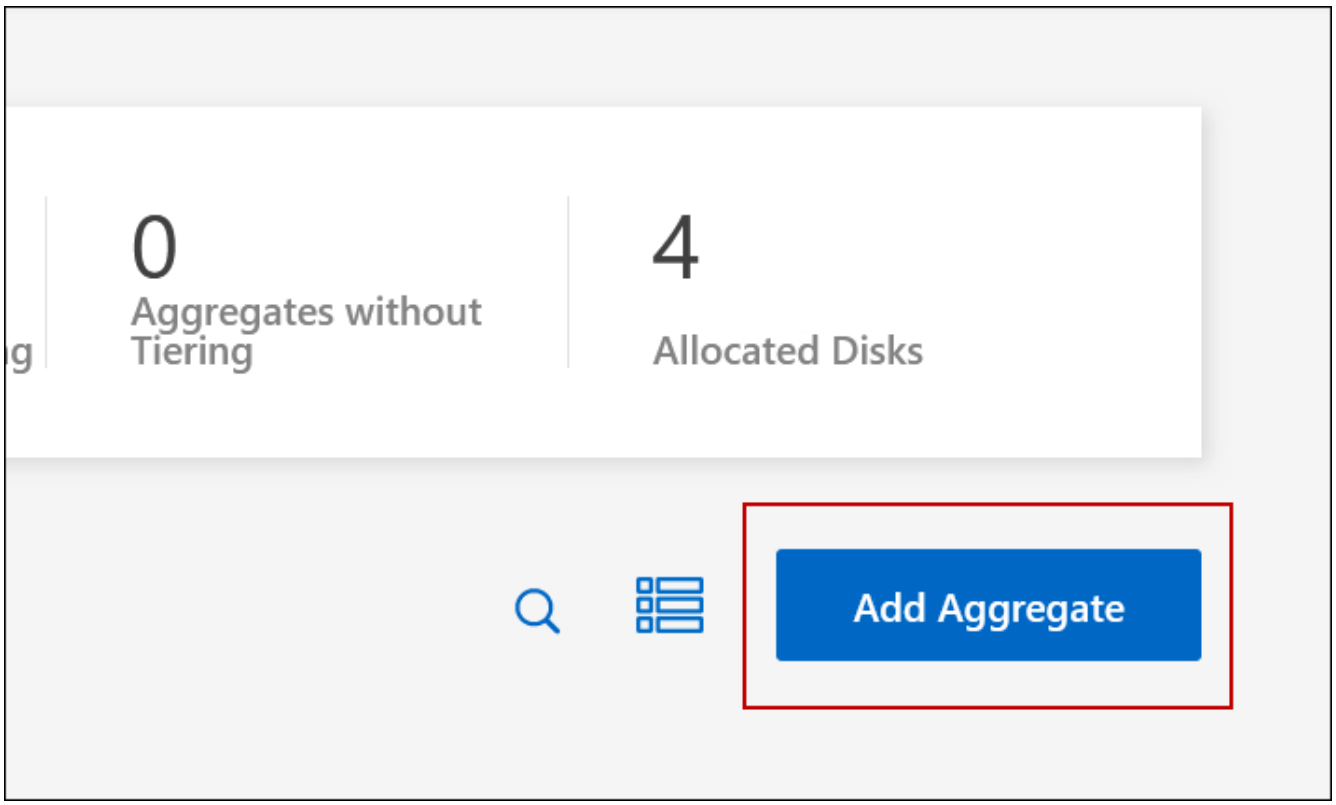
ョンが実装されている場合は、そのアクションも実行されます。

HA 構成の第 2 ノードにボリュームを作成する

デフォルトでは、HA構成の第1ノードにボリュームが作成されます。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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、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。
3. [アグリゲート]タブで、*[アグリゲートの追加]*をクリックします。
4. [Add Aggregate]画面で、アグリゲートを作成します。



5. Home Node には、 HA ペアの 2 番目のノードを選択します。
6. BlueXP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、*ボリュームの作成*をクリックします。
7. 新しいボリュームの詳細を入力し、 * Create * をクリックします。

結果

BlueXPでは、HAペアの2つ目のノードにボリュームが作成されます。

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。

ボリュームを作成したら

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。

既存のボリュームを管理

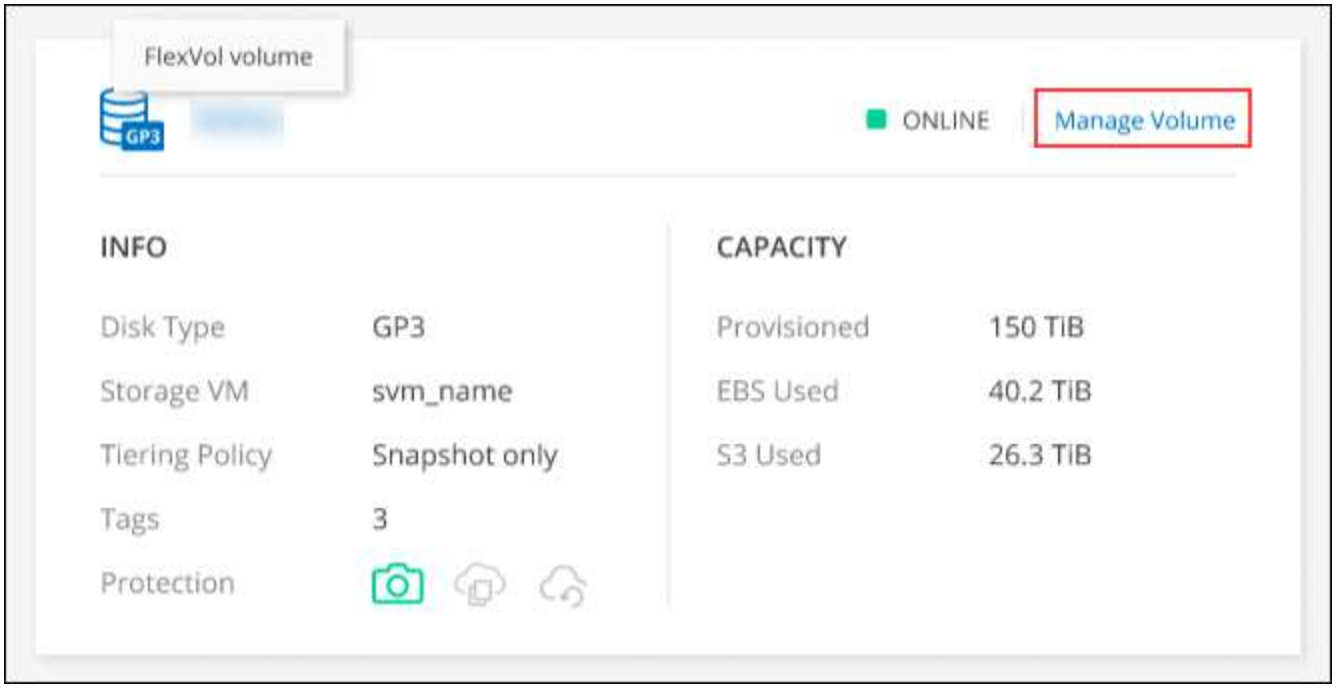
BlueXPを使用すると、ボリュームとCIFSサーバを管理できます。また、容量の問題を回避するためにボリュームを移動するように求められます。

ボリュームを管理します

ストレージニーズの変化に応じてボリュームを管理できます。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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、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。
3. 作業環境で、*[ボリューム]*タブをクリックします。



タブの[Manage Volume]ボタンのスクリーンショット。"]

4. [Volumes]タブで、目的のボリュームタイトルに移動し、*[Manage volume]*をクリックして[Manage Volumes]右側パネルにアクセスします。

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	[ボリュームの管理]パネルの[ボリューム操作]で、*[ボリュームの詳細を表示]*をクリックします。
nfs mount コマンドを取得します	a. [Manage volumes]パネルの[Volume Actions]で、*[Mount Command]*をクリックします。 b. [* コピー（ Copy ）] をクリックします
ボリュームのクローンを作成します	a. [Manage volumes]パネルの[Volume Actions]で、*[Clone the volume]*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"。
ボリュームタグを編集（読み書き可能ボリュームのみ）	a. [ボリュームの管理]パネルの[ボリューム操作]で*[ボリュームタグの編集]*をクリックし、選択したボリュームに割り当てられているボリュームタグを変更します。 b. 該当するフィールドにボリュームタグキーと値を入力します。 c. タグを追加するには、*[新しいタグの追加]*をクリックします。 d. [保存（ Save ）] 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. [ボリュームの管理]パネルの[ボリューム操作]で、*[ボリューム設定の編集]*をクリックします b. ボリュームのSnapshotポリシー、NFSプロトコルバージョン、NFSアクセス制御リスト（エクスポートポリシー）、または共有権限を変更し、*[適用]*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。
ボリュームを削除します	a. [ボリュームの管理]パネルの[ボリューム操作]で、*[ボリュームの削除]*をクリックします。 b. [Delete Volume]ウィンドウで、削除するボリュームの名前を入力します。 c. 再度 * Delete * をクリックして確定します。

タスク	アクション
オンデマンドで Snapshot コピーを作成します	a. [ボリュームの管理]パネルの[保護操作]で、*[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。
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. [ボリュームの管理]パネルの[保護操作]で、*[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。
基になるディスクタイプを変更します	a. [ボリュームの管理]パネルの[詳細な操作]で、*[ディスクタイプの変更]*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。 選択したディスクタイプを使用している既存のアグリゲートにボリュームを移動するか、ボリューム用に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. [ボリュームの管理]パネルの[詳細な操作]で、*[階層化ポリシーの変更]*をクリックします。 b. 別のポリシーを選択し、 * 変更 * をクリックします。 BlueXPは、選択されたディスクタイプを階層化して使用している既存のアグリゲートにボリュームを移動するか、ボリューム用に新しいアグリゲートを作成します。
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. ダイアログにボリュームの名前を入力します。 c. 再度 * Delete * をクリックして確定します。

ボリュームのサイズを変更する

デフォルトでは、スペースが不足したときにボリュームが最大サイズに自動的に拡張されます。デフォルト値は 1 、 000 で、ボリュームはサイズの 11 倍まで拡張できます。この値はコネクタの設定で設定できます。

ボリュームのサイズを変更する必要がある場合は、を使用して変更できます "ONTAP システムマネージャ"。ボリュームのサイズを変更する際は、システムの容量制限を考慮してください。にアクセスします "Cloud Volumes ONTAP リリースノート" 詳細：

CIFS サーバを変更

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. 作業環境の[Overview]タブで、右側のパネルの下にある[Feature]タブをクリックします。
2. [CIFS Setup]フィールドで、*鉛筆アイコン*をクリックして[CIFS Setup]ウィンドウを表示します。
3. CIFS サーバの設定を指定します。

タスク	アクション
Storage VM（SVM）を選択	Cloud Volume ONTAP Storage Virtual Machine（SVM）を選択すると、そのSVMの設定されたCIFS情報が表示されます。
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。
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。 ifdef ::gcp[] Google Managed Active Directory を設定している場合は、デフォルトで 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.x.x の IP アドレスを使用して AD にアクセスできます。 endif：GCP []
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。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

タスク	アクション
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。 "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" • Google 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=Cloud 」と入力します。 "Google Cloud ドキュメント：「 Organizational Units in Google Managed Microsoft AD"

4. [設定]*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。

ボリュームを移動する

容量利用率やパフォーマンスの向上、およびサービスレベル契約を満たすためにボリュームを移動する。

System Manager でボリュームを移動するには、ボリュームとデスティネーションアグリゲートを選択してボリューム移動処理を開始し、必要に応じてボリューム移動ジョブを監視します。System Manager を使用すると、ボリューム移動処理が自動的に完了します。

手順

1. 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。

   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"。

BlueXPに「**Action Required**」**(**アクションが必要です**)**というメッセージが表示されたら、ボリュームを移動し

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通知する「Action Required」メッセージがBlueXPに表示されることがありますが、問題 を手動で修正する必要があります。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。

アグリゲートの使用容量が90%に達すると、「Action Required」メッセージが表示されます。データ階層化が有効になっている場合は、アグリゲートの使用容量が 80% に達するとメッセージが表示されます。デフォルトでは、 10% の空きスペースがデータ階層化用に予約されています。 "データ階層化のための空きスペース率について詳しくは、こちらをご覧ください"。

手順

1. [容量の問題を解決する方法を特定する]。
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。
   - [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します]。
   - [容量の問題を回避するためにボリュームを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ボリュームの移動が推奨されない場合は、移動が必要なボリュームと、そのボリュームを同じシステムの別のアグリゲートまたは別のシステムのどちらに移動すべきかを特定する必要があります。

手順

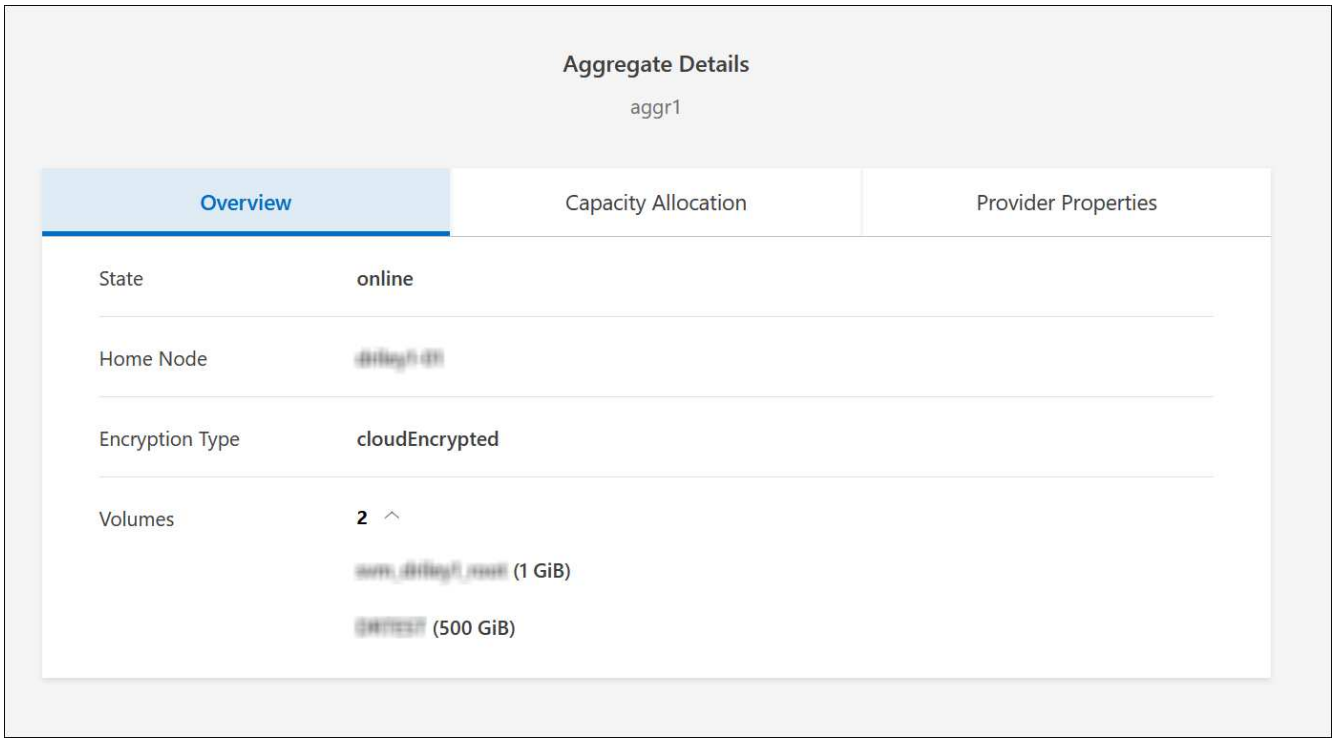
1. Action Required メッセージの詳細情報を表示して、容量制限に達したアグリゲートを特定します。

   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、*[アグリゲート]タブ*をクリックします。
   b. 目的のアグリゲートタイルに移動し、 （楕円アイコン）>アグリゲートの詳細を表示*。
   c. [Aggregate Details]画面の[Overview]タブで、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 容量の問題を回避するためにボリュームを別のアグリゲートに移動します。

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 容量の問題を回避するためにボリュームを別のアグリゲートに移動します。

   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アグリゲートに移動します。

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します

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。

> 容量の問題を回避するためにボリュームを移動する必要がありますが、システムがディスクの上限に達しているため、BlueXPではこの操作を実行できません。

手順

1. 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。
2. 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"。

3. [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"。

4. 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"。

5. 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 "ボリュームを管理します"。

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。

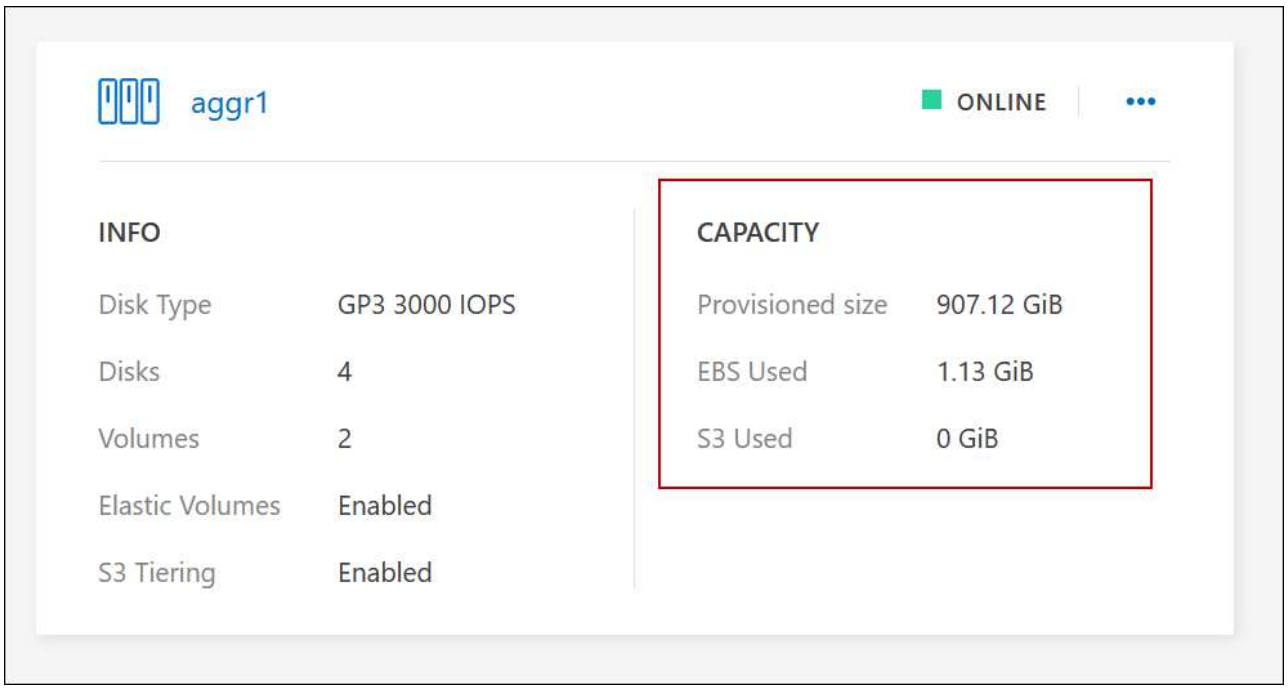
このタスクについて

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。

> 容量の問題を回避するには2つ以上のボリュームを移動する必要がありますが、BlueXPではこの操作を実行できません。

手順

1. 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。
   a. 作業環境で、*[アグリゲート]タブ*をクリックします。
   b. 目的のアグリゲートタイルに移動し、 （楕円アイコン）>アグリゲートの詳細を表示*。
   c. アグリゲートタイルで、使用可能容量（プロビジョニング済みサイズから使用済みアグリゲート容量を引いた値）を確認します。



2. 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、*をクリックします。 （楕円アイコン）>[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。
3. 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"。

4. 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。
5. 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"。

ボリューム移動の実行に時間がかかる場合がある理由

Cloud Volumes ONTAP で次のいずれかの条件に該当する場合、ボリュームの移動に予想よりも時間がかかることがあります。

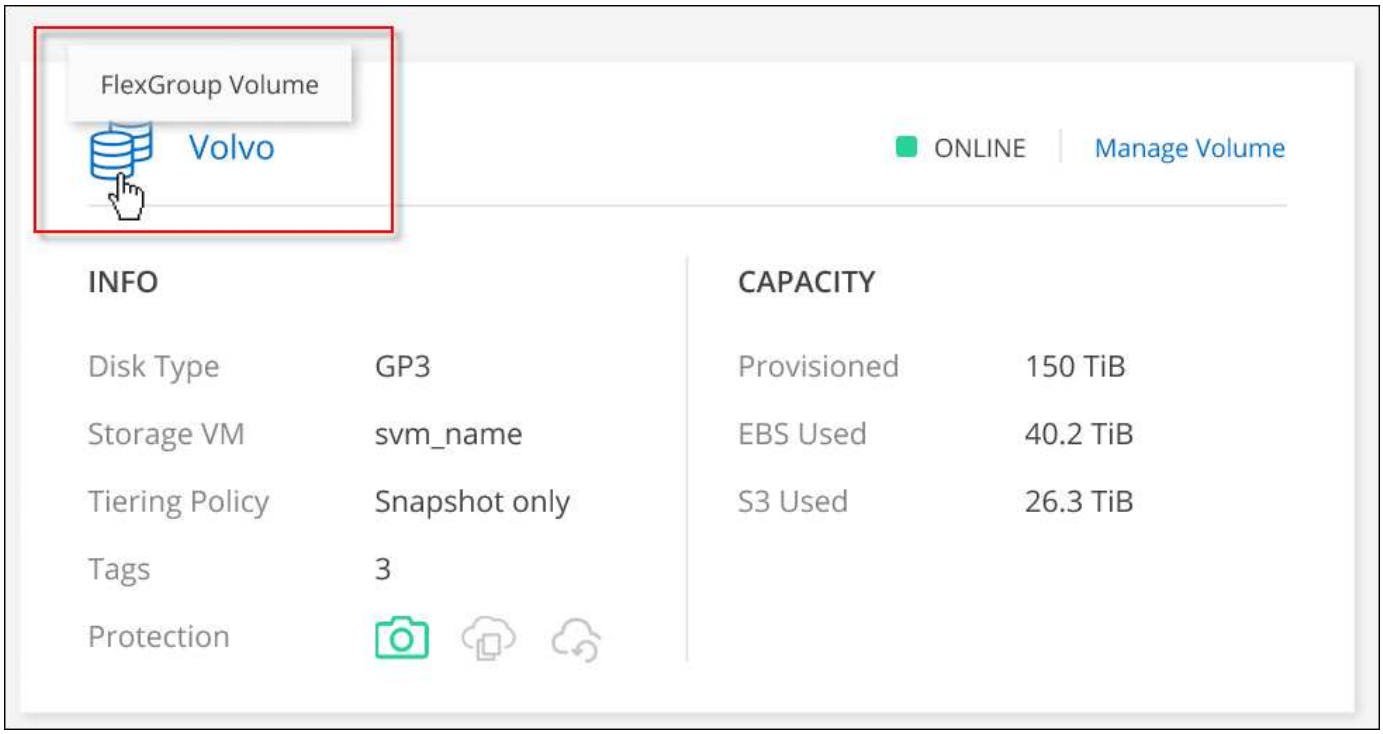
- ボリュームがクローンである。
- ボリュームがクローンの親です。
- ソースアグリゲートまたはデスティネーションアグリゲートには、スループットが最適化された HDD （ st1 ）が 1 本含まれています。
- いずれかのアグリゲートでオブジェクトに古い命名規則が使用されています。両方のアグリゲートで同じ名前形式を使用する必要があります。

  9.4 リリース以前のアグリゲートでデータの階層化が有効になっている場合は、古い命名規則が使用されます。

- 暗号化設定がソースアグリゲートとデスティネーションアグリゲートで一致しないか、キーの変更を実行中です。
- 階層化ポリシーを変更するためにボリューム移動で -tiering-policy _ オプションが指定されています。
- ボリューム移動で、 generate-destination-key_option が指定されました。

FlexGroup ボリュームを表示します

CLIまたはSystem Managerで作成されたFlexGroup ボリュームは、BlueXPの[Volumes]タブで直接表示できます。作成されたFleGroupボリュームの詳細情報は、FlexVol ボリュームの場合と同じです。BlueXPでは、作成されたFleGroupボリュームの詳細情報を専用の[Volumes]タイルで確認できます。[Volumes]タイルでは、アイコンにカーソルを合わせると各FlexGroup ボリュームグループを特定できます。また、ボリュームリストビューの[Volume Style]列で、FlexGroup ボリュームを特定してソートすることもできます。



現時点では、BlueXPでは既存のFlexGroup ボリュームのみを表示できます。BlueXP でFlexGroup ボリュームを作成することはできませんが、今後のリリースでサポートする予定です。

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

ホットデータ用の SSD または HDD の高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、 Cloud Volumes ONTAP のストレージコストを削減できます。データ階層化は、 FabricPool テクノロジによって実現されます。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"。

データの階層化を設定するには、次の操作を実行する必要があります。

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 システムがある場合は、に進んでください。 "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、必要な権限がBlueXPに割り当てられていれば何も行う必要はありません。 詳細はこちら。。
- Google Cloudの場合は、プライベートGoogleアクセスのサブネットを設定し、サービスアカウントを設定する必要があります。 詳細はこちら。。

3 階層化が有効なアグリゲートがあることを確認してください

ボリュームでデータ階層化を有効にするには、アグリゲートでデータ階層化が有効になっている必要があります。新しいボリュームと既存のボリュームの要件を確認しておく必要があります。 詳細はこちら。。

4 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、または複製するときに、階層化ポリシーを選択するよう求めるメッセージが表示されます。

- "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。
- 大容量階層用のオブジェクトストアを作成する必要はありません。BlueXPはそのような機能を提供します。
- システムレベルでデータの階層化を有効にする必要はありません。

  BlueXPでは'システムの作成時にコールドデータ用のオブジェクトストアが作成されます 接続または権限に問題がないことが必要です。その後は、ボリューム（および場合によっては、 アグリゲート）。

データ階層化をサポートする構成

特定の構成や機能を使用する場合は、データの階層化を有効にすることができます。

AWSでのサポート

- Cloud Volumes ONTAP 9.2以降では、AWSでデータ階層化がサポートされます。
- パフォーマンス階層には、汎用 SSD （ GP3 または gp2 ）またはプロビジョニングされる IOPS SSD （ io1 ）を使用できます。

スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

Azure でのサポート

- Azureでは、次のデータ階層化がサポートされています。
  - シングルノードシステムの場合はバージョン9.4
  - HAペアではバージョン9.6
- 高パフォーマンス階層には、Premium SSD Managed Disks、Standard SSD Managed Disks、Standard HDD Managed Disksがあります。

Google Cloudのサポート

- Cloud Volumes ONTAP 9.6以降では、Google Cloudでデータ階層化がサポートされます。
- パフォーマンス階層には、 SSD 永続ディスク、分散型永続ディスク、標準の永続ディスクがあります。

機能の相互運用性

- 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。

要件

クラウドプロバイダに応じて、 Cloud Volumes ONTAP がコールドデータをオブジェクトストレージに階層化できるように、特定の接続と権限を設定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

BlueXPに必要な権限があれば、高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。BlueXPでは、コネクタのカスタムロールに次の権限がある場合にvnetサービスエンドポイントが有効になります。

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

権限はデフォルトでカスタムロールに含まれています。 "ConnectorのAzure権限を表示します"

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

- 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"。
- サービスアカウントがCloud Volumes ONTAP に接続されている必要があります。

  "このサービスアカウントの設定方法について説明します"。

  Cloud Volumes ONTAP 作業環境の作成時に、このサービスアカウントを選択するよう求められます。

導入時にサービスアカウントを選択しなかった場合は、Cloud Volumes ONTAP をシャットダウンし、Google Cloudコンソールに移動して、Cloud Volumes ONTAP インスタンスにサービスアカウントを接続する必要があります。データの階層化は、次のセクションの説明に従って有効にできます。

- バケットをお客様が管理する暗号化キーで暗号化するには、 Google Cloud ストレージバケットでキーを使用できるようにします。

  "お客様が管理する暗号化キーを Cloud Volumes ONTAP で使用する方法について説明します"。

要件の実装後にデータ階層化を有効化

BlueXPでは'接続やアクセス権に問題がない限り'システムの作成時にコールドデータ用のオブジェクトストアが作成されますシステムを作成するまで上記の要件を実装しなかった場合は、APIまたはSystem Managerを使用して階層化を手動で有効にする必要があります。APIまたはSystem Managerを使用すると、オブジェクトストアが作成されます。

BlueXPユーザインターフェイスで階層化を有効にする機能は、Cloud Volumes ONTAPの今後のリリースで提供される予定です。

アグリゲートで階層化が有効になっていることを確認してください

ボリュームでデータ階層化を有効にするには、アグリゲートでデータ階層化が有効になっている必要があります。新しいボリュームと既存のボリュームの要件を確認しておく必要があります。

- * 新しいボリューム *

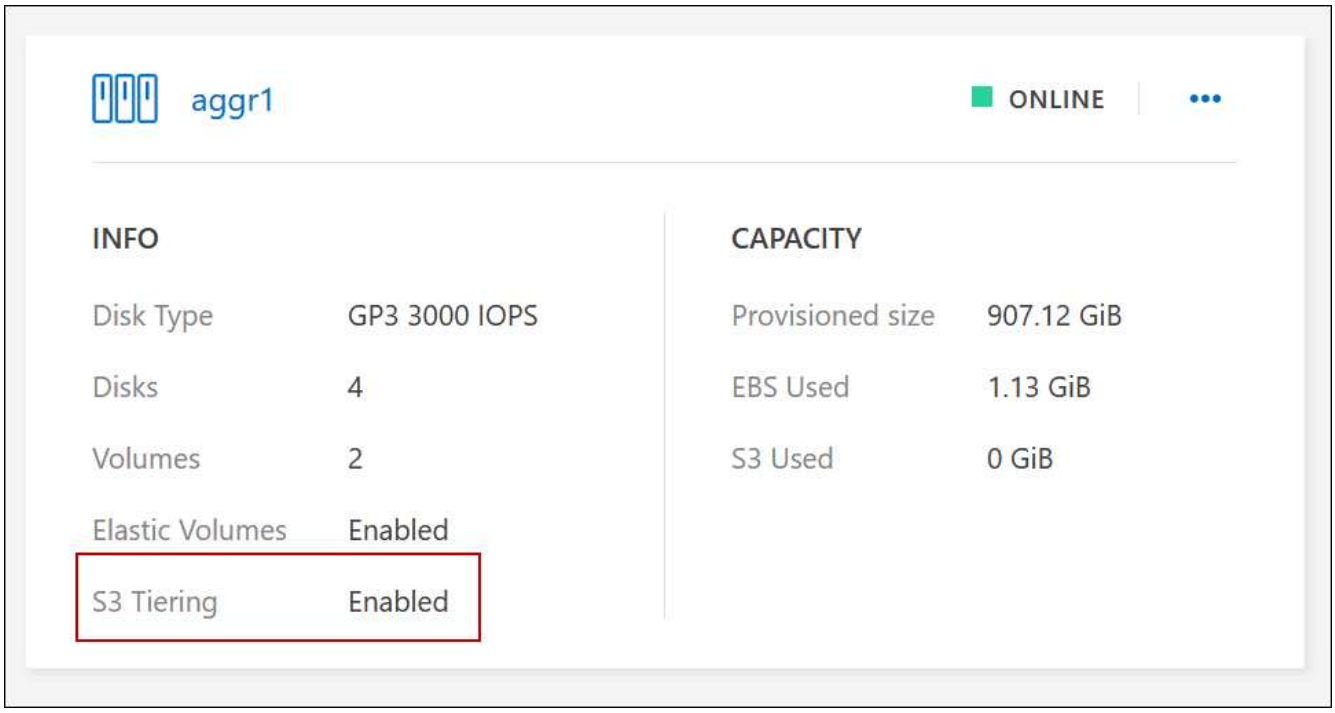
  新しいボリュームでデータ階層化を有効にする場合、アグリゲートでデータ階層化を有効にする必要はありません。階層化が有効になっている既存のアグリゲート上にボリュームが作成されます。データ階層化が有効になっているアグリゲートがない場合は、ボリューム用の新しいアグリゲートが作成されます。

- * 既存のボリューム *

  既存のボリュームでデータ階層化を有効にする場合は、基盤となるアグリゲートでデータ階層化を有効にする必要があります。既存のアグリゲートでデータ階層化が有効になっていない場合は、 System Manager を使用して、既存のアグリゲートをオブジェクトストアに接続する必要があります。

アグリゲートで階層化が有効になっているかどうかを確認する手順

1. BlueXPで作業環境を開きます
2. [Aggregates]タブをクリックします。
3. 目的のタイルに移動し、アグリゲートで階層化が有効になっているか無効になっているかを確認します。



アグリゲートで階層化を有効にする手順

1. System Manager で、 * Storage > Tiers * をクリックします。
2. アグリゲートの操作メニューをクリックし、 * クラウド階層の接続 * を選択します。
3. 接続するクラウド階層を選択し、 * 保存 * をクリックします。

次の手順

次のセクションで説明するように、新規および既存のボリュームでデータ階層化を有効にできます。

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

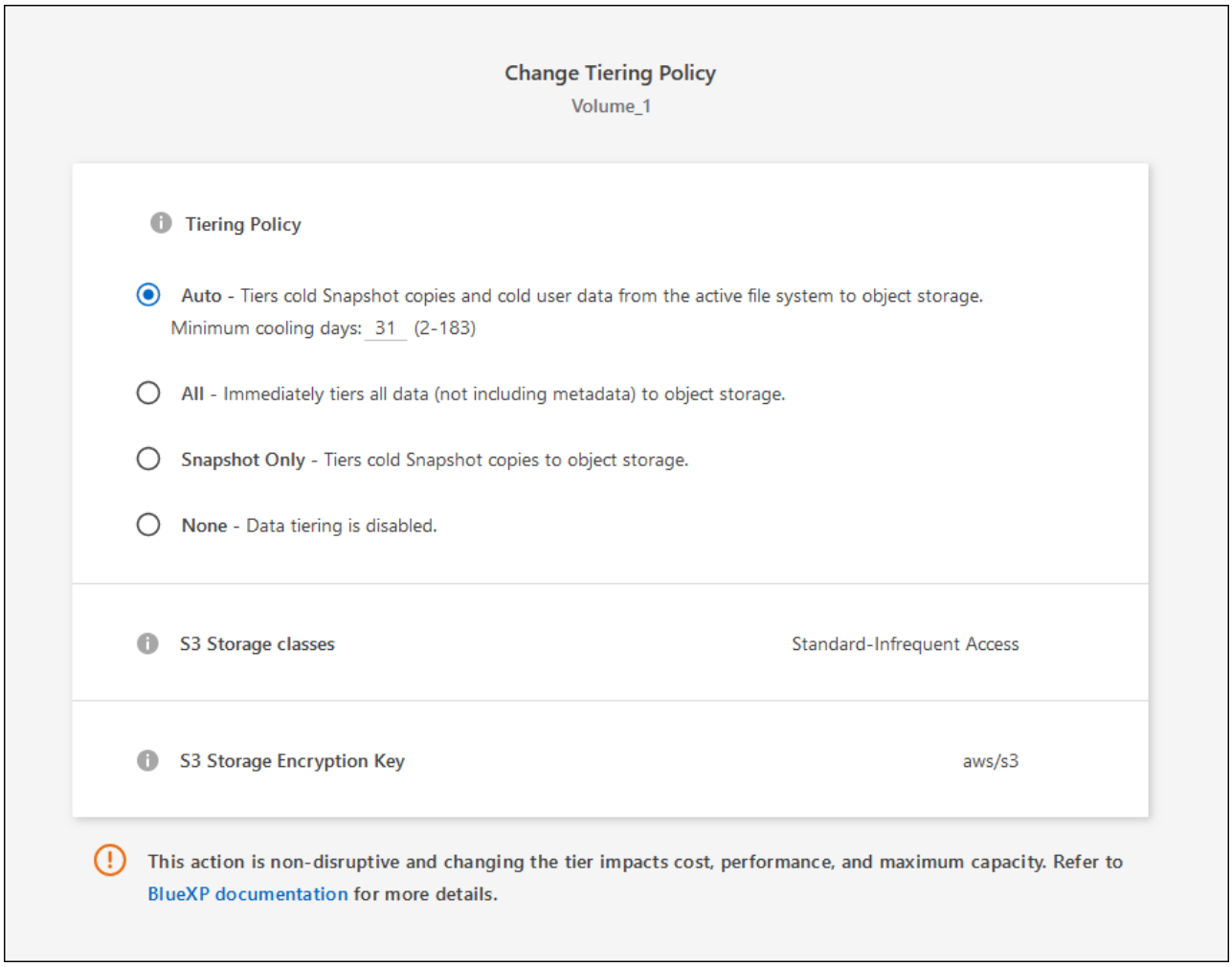
1. 作業環境の[Volumes]タブで、新しいボリュームを作成するか、既存のボリュームの階層を変更します。

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	目的のボリュームタイルを選択し、[ボリュームの管理]*をクリックして[ボリュームの管理]右側パネルにアクセスし、右パネルの[高度な操作]および[階層化ポリシーの変更]*をクリックします。

2. 階層化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 *



データ階層化が有効なアグリゲートがない場合、ボリューム用の新しいアグリゲートがBlueXPで作成されます。

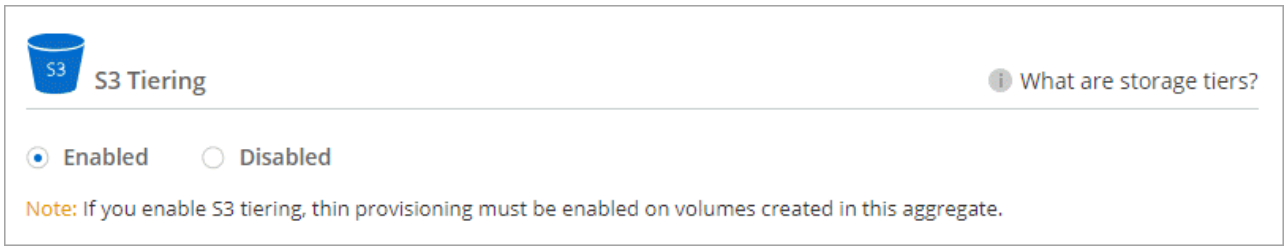
データ保護ボリュームのデータを階層化する

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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、ソースボリュームを含む作業環境を選択し、ボリュームを複製する作業環境にドラッグします。
3. 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"。

階層化データのストレージクラスを変更する

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ストレージクラスを 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とアクセスコストが高くなるため、ストレージクラスを変更する前にこの点を考慮する必要があります。

階層化データのストレージクラスはシステム全体に適用され、ボリュームごとにではないものに限られます。

サポートされているストレージクラスについては、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、 * 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. ストレージクラスを選択して、「 * 保存」をクリックします。

データ階層化の空きスペース率を変更する

データ階層化の空きスペース率は、オブジェクトストレージへのデータの階層化時に Cloud Volumes ONTAP SSD / HDD で必要な空きスペースの量を定義します。デフォルトの設定は 10% の空きスペースですが、必要に応じて設定を調整できます。

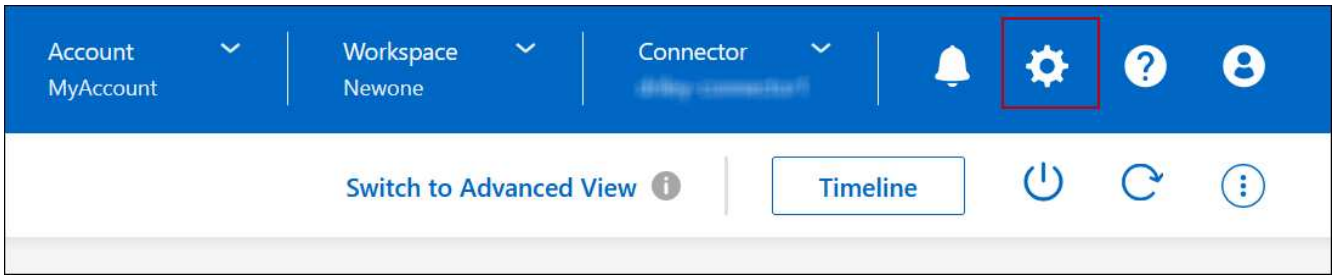
たとえば、購入容量を確実に使用するために、空きスペースを 10% 未満にすることができます。追加の容量が必要になった場合（アグリゲートのディスクの上限に達するまで）、BlueXPで追加のディスクを購入できます。

十分なスペースがないと、 Cloud Volumes ONTAP はデータを移動できず、パフォーマンスが低下する可能性があります。変更は慎重に行ってください。不明な点がある場合は、ネットアップサポートにお問い合わせください。

この比率はディザスタリカバリシナリオで重要になります。オブジェクトストレージからデータが読み取られると、 Cloud Volumes ONTAP はパフォーマンスを向上させるためにデータを SSD / HDD に移動するためです。十分なスペースがないと、 Cloud Volumes ONTAP はデータを移動できません。この比率を変更する際は、ビジネス要件を満たすためにこの点を考慮してください。

手順

1. BlueXPコンソールの右上にある「設定」アイコンをクリックし、「コネクタ設定」を選択します。



2. 容量 * で、アグリゲート容量しきい値 - データ階層化の空きスペース率 * をクリックします。
3. 必要に応じて空き領域の比率を変更し、 [保存（ Save ）] をクリックします。

auto 階層化ポリシーのクーリング期間を変更します

_auto_tiering ポリシーを使用して Cloud Volumes ONTAP ボリュームのデータ階層化を有効にした場合は、ビジネスニーズに基づいてデフォルトのクーリング期間を調整できます。このアクションは、APIとCLIでのみサポートされます。

クーリング期間とは、ボリューム内のユーザデータが「コールド」とみなされてオブジェクトストレージに移動されるまでの期間です。

auto 階層化ポリシーのデフォルトのクーリング期間は 31 日です。冷却期間は次のように変更できます。

- 9.8 以降： 2 日 ～ 183 日
- 9.7 以前： 2 日から 63 日

ステップ

1. ボリュームの作成時や既存のボリュームの変更時に、 API 要求で *minimumCoolingDays* パラメータを使用します。

LUN をホストに接続します

iSCSIボリュームを作成すると、BlueXPによって自動的にLUNが作成されます。ボリュームごとに 1 つの LUN を作成するだけでシンプルになり、管理は不要です。ボリュームの作成後、 IQN を使用してホストから LUN に接続します。

次の点に注意してください。

- BlueXPの自動容量管理はLUNには適用されませんBlueXPでLUNを作成すると'自動拡張機能が無効になります
- LUN は、 System Manager または CLI を使用して追加で作成できます。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、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。
3. 作業環境で、*[ボリューム]*タブをクリックします。
4. [Volumes]タブで、目的のボリュームタイトルに移動し、*[Manage volume]*をクリックして[Manage Volumes]右側パネルにアクセスします。

5. [Target IQN]*をクリックします。
6. [* Copy*] をクリックして IQN 名をコピーします。
7. ホストから LUN への iSCSI 接続をセットアップします。
    - "ONTAP 9 Red Hat Enterprise Linux 向けの iSCSI の簡単な設定：ターゲットとの iSCSI セッションの開始"
    - "ONTAP 9 Windows 向けの iSCSI の簡単な設定：ターゲットとの iSCSI セッションの開始"
    - "ONTAP SAN ホスト構成"

FlexCache ボリュームでデータアクセスを高速化

FlexCacheボリュームは、元の（ソース）ボリュームのSMBおよび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。

BlueXPでは、FlexCacheボリュームを "BlueXPのボリュームキャッシュ" サービス

ONTAP CLIまたはONTAPシステムマネージャを使用して、FlexCacheボリュームを作成および管理することもできます。

- "FlexCache Volumes for Faster Data Access Power Guide"
- "System Manager での FlexCache ボリュームの作成"

すべての新しいCloud Volumes ONTAPシステムに対してFlexCacheライセンスが生成されます。ライセンスの使用量は 500GiB に制限されています。

アグリゲートの管理

アグリゲートを作成する

アグリゲートは、手動で作成することも、ボリュームの作成時にBlueXPに自動で作成させることもできます。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。

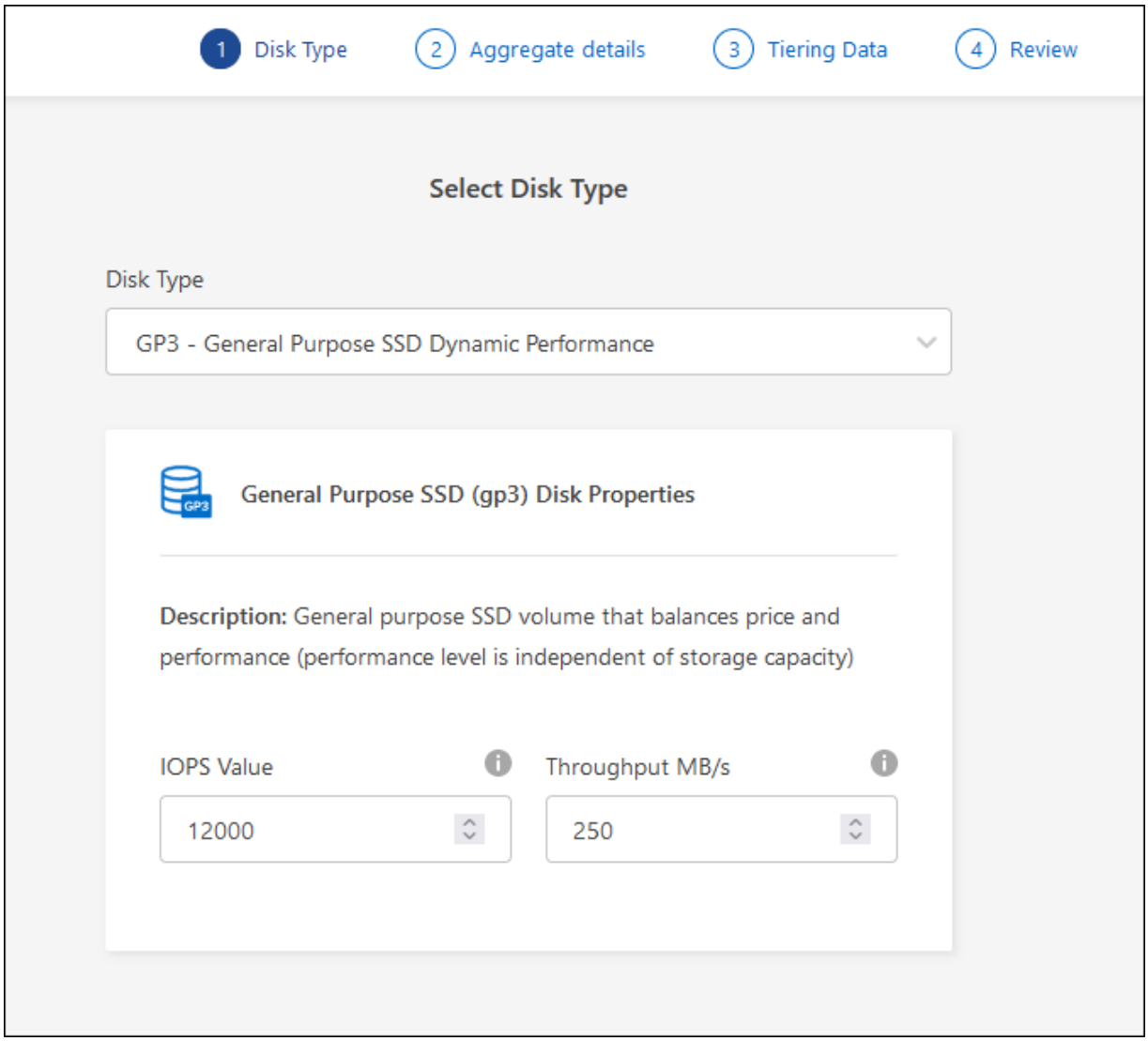
> すべてのディスクとアグリゲートは、BlueXPから直接作成および削除する必要があります。これらのアクションは、別の管理ツールから実行しないでください。これにより、システムの安定性が低下し、将来ディスクを追加できなくなる可能性があります。また、クラウドプロバイダの冗長料金が発生する可能性もあります。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、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。
3. [アグリゲート]タブで、*[アグリゲートの追加]*をクリックし、アグリゲートの詳細を指定します。

AWS

- ディスクタイプとディスクサイズの選択を求めるメッセージが表示された場合は、を参照してください "AWSでCloud Volumes ONTAP 構成を計画"。
- アグリゲートの容量のサイズを入力するように求められたら、Amazon EBS Elastic Volumes機能をサポートする構成でアグリゲートを作成します。次のスクリーンショットは、GP3ディスクで構成される新しいアグリゲートの例を示しています。



"Elastic Volumesのサポートに関する詳細情報"。

Azure

ディスクの種類とサイズについては、を参照してください "AzureでCloud Volumes ONTAP 構成を計画"。

Google Cloud

ディスクの種類とサイズについては、を参照してください "Google CloudでCloud Volumes ONTAP 構成を計画する"。

4. [* Go *] をクリックし、 [* 承認して購入 *] をクリックします。

アグリゲートを管理する

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。

> すべてのディスクとアグリゲートは、BlueXP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。

作業を開始する前に

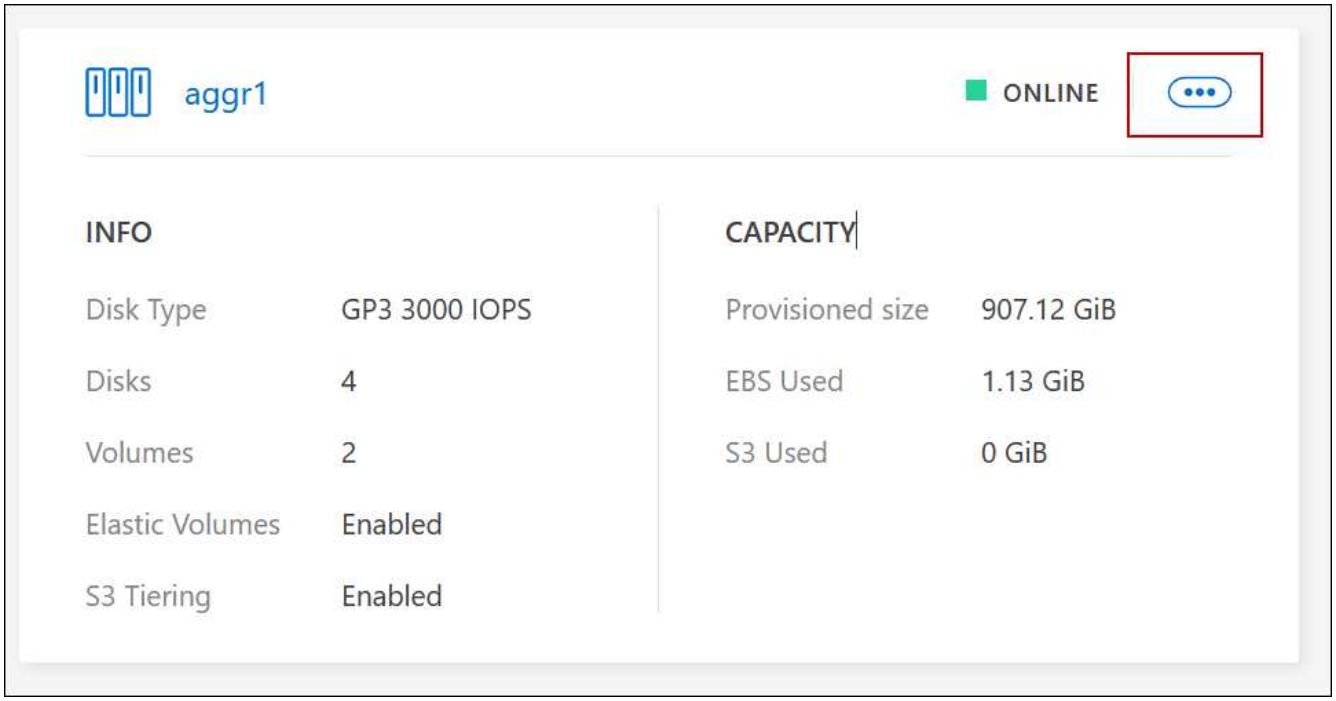
アグリゲートを削除する場合は、まずアグリゲート内のボリュームを削除しておく必要があります。

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、 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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、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。
3. 作業環境で、*[アグリゲート]*タブをクリックします。
4. [アグリゲート]タブで、目的のタイトルに移動し、 （楕円アイコン）*。



メニューオプションのスクリーンショット。"]

5. 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	下に…（楕円アイコン）メニューで*[アグリゲートの詳細を表示]*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	下に…（楕円アイコン）メニューで*[ボリュームの追加]*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. 下に…（楕円アイコン）メニューで*[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。
Amazon EBS Elastic Volumes をサポートするアグリゲートの容量を増やす	a. 下に…（楕円アイコン）メニューで、*容量の拡張*をクリックします。 b. 追加する容量を入力し、*[拡張]*をクリックします。 アグリゲートの容量は256GiB以上、またはアグリゲートのサイズの10%以上拡張する必要があります。 たとえば、アグリゲートのサイズが1.77TiBの場合、10%は181GiBです。これは256 GiBよりも小さいため、アグリゲートのサイズを256 GiB以上増やす必要があります。
アグリゲートを削除します	a. ボリュームが含まれていないアグリゲートタイルを選択する[**…**（楕円アイコン）**>**削除。 b. 再度 * Delete * をクリックして確定します。

コネクタの容量設定を管理します

各コネクタには、Cloud Volumes ONTAP のアグリゲート容量の管理方法を決定する設定があります。

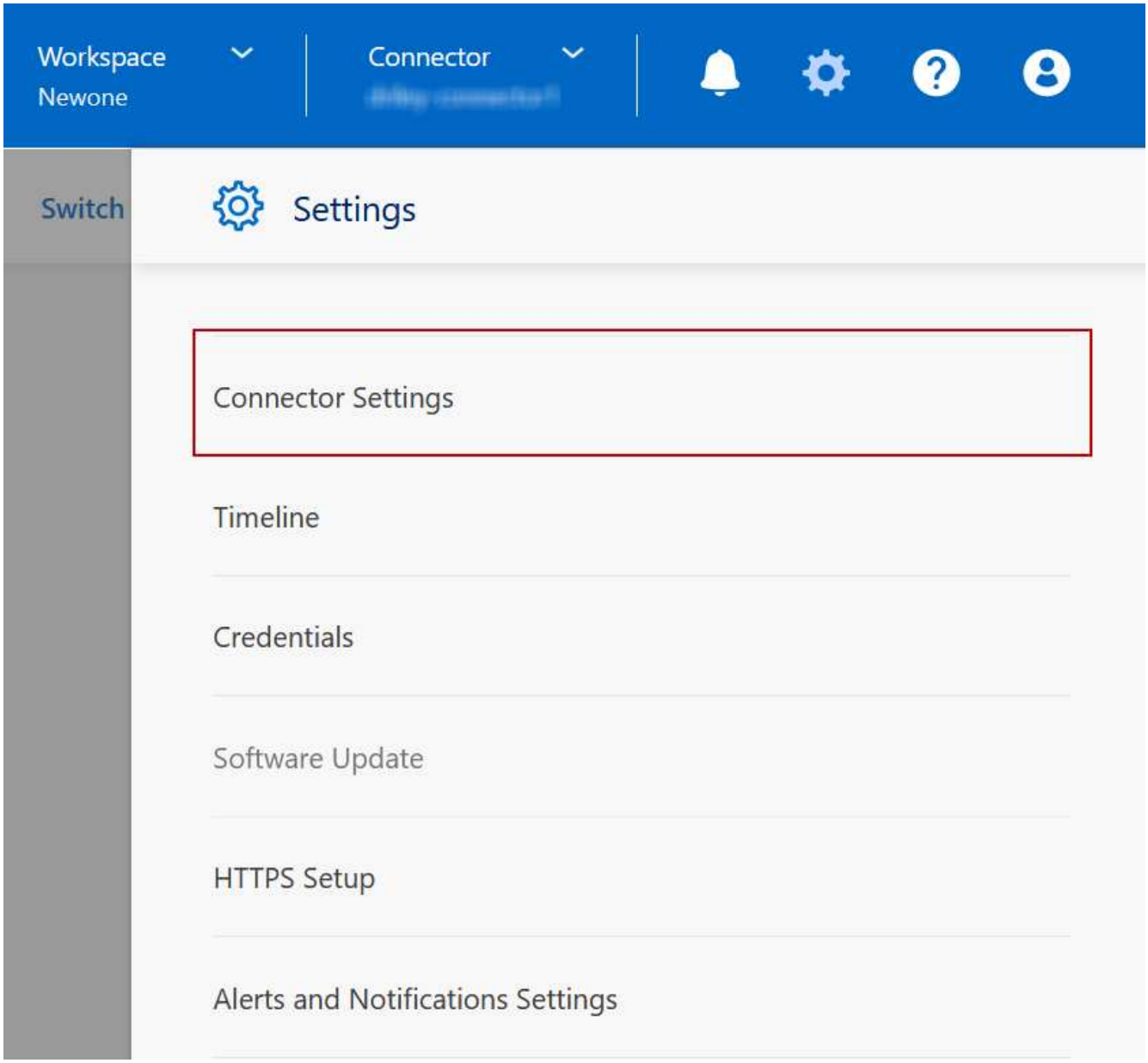
これらの設定は、コネクタによって管理されるすべてのCloud Volumes ONTAP システムに適用されます。別のコネクタがある場合は、別の方法で設定できます。

必要な権限

コネクタ設定を変更するには、アカウント管理者権限が必要です。

手順

1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[コネクタの設定]を選択します。



2. *容量*で、次のいずれかの設定を変更します。

Capacity Management Mode （容量管理モード）

ストレージ容量の決定についてBlueXPから通知するかどうか、またはBlueXPが容量要件を自動的に管理するかどうかを選択します。

"容量管理モードの仕組みをご確認ください"。

アグリゲート容量のしきい値-空きスペース率

アグリゲートの空きスペース率が指定したしきい値を下回ったときに通知をトリガーします。

空きスペース率は、次のように計算します。

（アグリゲート容量-アグリゲートで使用されている合計容量）/アグリゲートの容量

アグリゲート容量のしきい値-データ階層化の空きスペース率

データを大容量階層（オブジェクトストレージ）に階層化するときに必要な高パフォーマンス階層（ディスク）の空きスペースの量を定義します。

この比率はディザスタリカバリのシナリオにとって重要です。大容量階層からデータが読み取られると、Cloud Volumes ONTAP はパフォーマンス階層にデータを移動してパフォーマンスを向上させます。十分なスペースがないと、 Cloud Volumes ONTAP はデータを移動できません。

3. [保存（ Save ）] をクリックします。

Storage VM 管理

BlueXPでStorage VMを管理します

Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは、 _ SVM _ または _ SVM _ であることがわかります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されますが、一部の設定では追加の Storage VM がサポートされます。

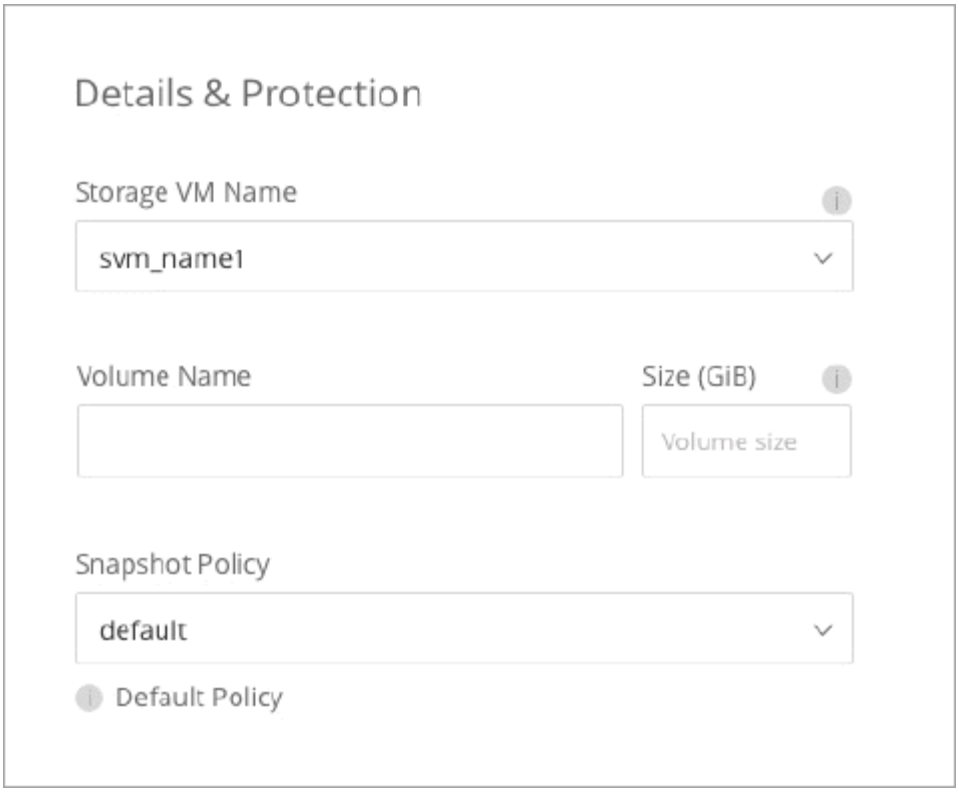
サポートされている Storage VM 数

一部の構成では複数のStorage VMがサポートされます。にアクセスします "Cloud Volumes ONTAP リリースノート" 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

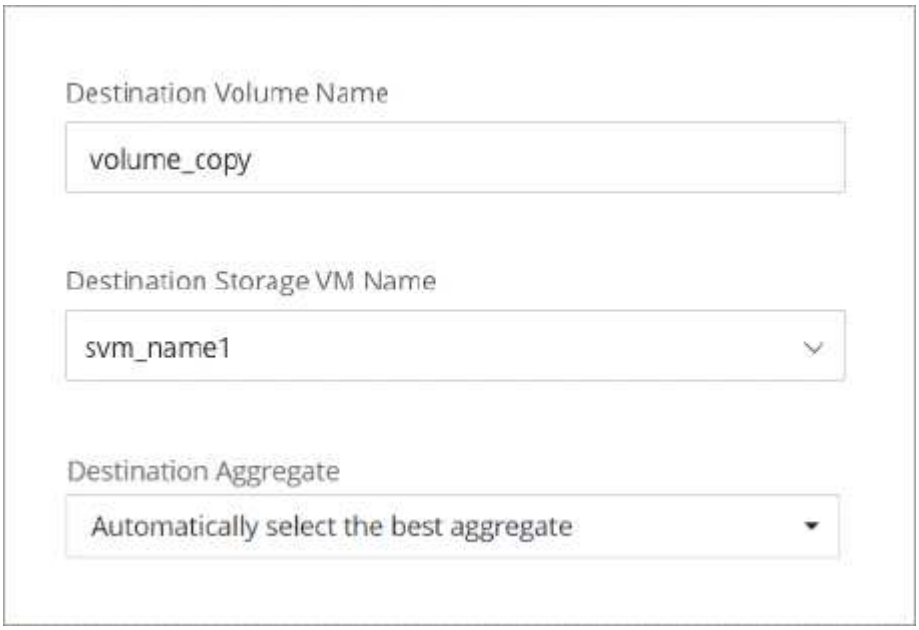
複数の Storage VM を使用できます

BlueXPでは、System ManagerまたはCLIから作成した追加のStorage VMがサポートされます。

たとえば、次の図は、ボリュームの作成時に Storage VM を選択する方法を示しています。



次の図は、ボリュームを別のシステムにレプリケートするときに Storage VM を選択する方法を示しています。



デフォルトの **Storage VM** の名前を変更します

Cloud Volumes ONTAP 用に作成した1つのStorage VMには、BlueXPによって自動的に名前が付けられます。厳密な命名基準がある場合は、System Manager、CLI、またはAPIを使用してStorage VMの名前を変更できます。たとえば、 ONTAP クラスタの Storage VM の命名規則に沿った名前に変更できます。

AWS で Cloud Volumes ONTAP 用のデータ提供用 Storage VM を作成します

Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは、 _ SVM _ または _ SVM _ であることがわかります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されますが、一部の設定では追加の Storage VM がサポートされます。

データを提供する Storage VM を追加で作成するには、 AWS で IP アドレスを割り当ててから、 Cloud Volumes ONTAP の設定に基づいて ONTAP コマンドを実行する必要があります。

サポートされている Storage VM 数

9.7 以降のリリースでは、特定の Cloud Volumes ONTAP 構成で複数の Storage VM を使用できます。にアクセスします "Cloud Volumes ONTAP リリースノート" 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

他のすべての Cloud Volumes ONTAP 構成で、ディザスタリカバリに使用する 1 つのデータ提供用 Storage VM と 1 つのデスティネーション Storage VM がサポートされます。ソース Storage VM で停止が発生した場合は、デスティネーション Storage VM をデータアクセス用にアクティブ化できます。

構成の制限を確認します

各 EC2 インスタンスでは、ネットワークインターフェイスごとにサポートされるプライベート IPv4 アドレスの最大数が決まっています。新しい Storage VM に AWS で IP アドレスを割り当てる前に、上限を確認する必要があります。

手順

1. に移動します "ストレージの制限に関するセクションは、 Cloud Volumes ONTAP リリースノートを参照してください"。
2. インスタンスタイプのインターフェイスごとの IP アドレスの最大数を確認します。
3. AWS で IP アドレスを割り当てるときは次のセクションで必要になるため、この数値をメモしておいてください。

AWS で IP アドレスを割り当てます

新しい Storage VM 用の LIF を作成する前に、 AWS のポート e0a にプライベート IPv4 アドレスを割り当てる必要があります。

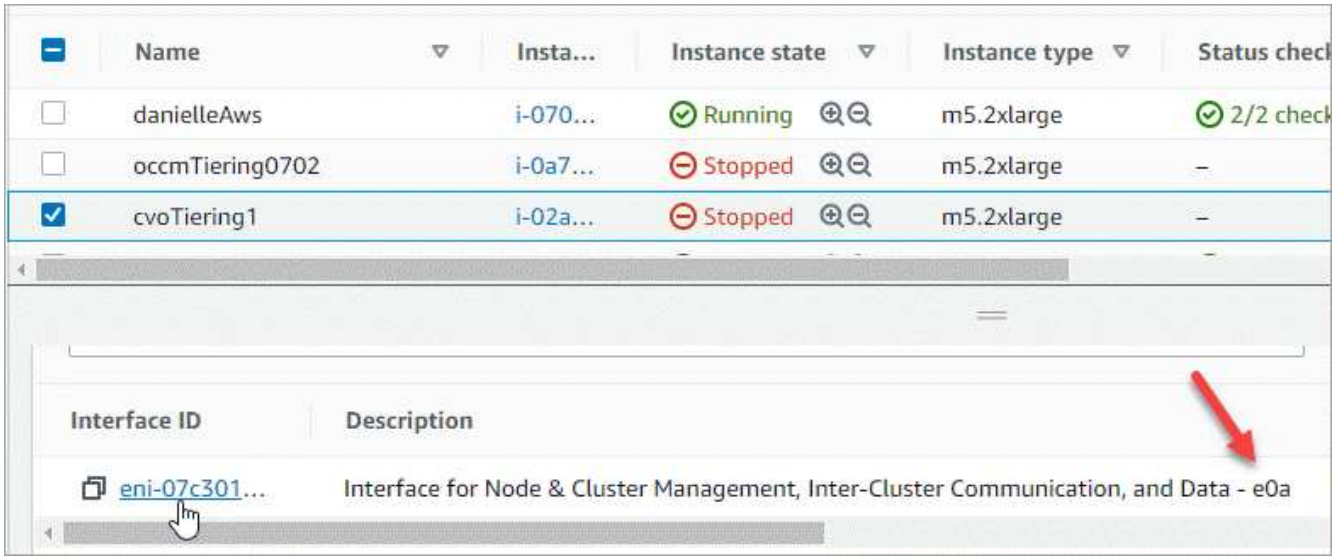
Storage VM 用のオプションの管理 LIF では、単一のノードシステムおよび単一の AZ 内の HA ペア上にプライベート IP アドレスが必要です。この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

手順

1. AWS にログインして EC2 サービスを開きます。
2. Cloud Volumes ONTAP インスタンスを選択し、 * ネットワーク * をクリックします。

   HA ペアで Storage VM を作成する場合は、ノード 1 を選択します。

3. ネットワークインターフェイス * までスクロールし、ポート e0a の * インターフェイス ID * をクリックします。



4. ネットワークインターフェイスを選択し、 * Actions > Manage IP Addresses * をクリックします。
5. e0a の IP アドレスのリストを展開します。
6. IP アドレスを確認します。
   a. 割り当てられた IP アドレスの数を数えて、ポートに追加の IP 用のスペースがあることを確認します。

      このページの前のセクションで、インターフェイスごとにサポートされる IP アドレスの最大数を確認しておく必要があります。

   b. オプション： Cloud Volumes ONTAP の CLI に移動し、 * network interface show * を実行して、各 IP アドレスが使用中であることを確認します。

      IP アドレスが使用されていない場合は、新しい Storage VM で使用できます。

7. AWS コンソールに戻り、「 * 新しい IP アドレスを割り当て * 」をクリックして、新しい Storage VM に必要な量に基づいて追加の IP アドレスを割り当てます。
   - シングルノードシステム：未使用のセカンダリプライベート IP が 1 つ必要です。

     Storage VM に管理 LIF を作成する場合は、オプションのセカンダリプライベート IP が必要です。

   - 単一の AZ における HA ペア：ノード 1 には、未使用のセカンダリプライベート IP が 1 つ必要です。

     Storage VM に管理 LIF を作成する場合は、オプションのセカンダリプライベート IP が必要です。

   - 複数の AZ にまたがる HA ペア：各ノードには、未使用のセカンダリプライベート IP が 1 つ必要です。
8. 単一の AZ 内の HA ペアに IP アドレスを割り当てる場合は、 * セカンダリプライベート IPv4 アドレスの再割り当てを許可 * を有効にします。
9. [保存（ Save ）] をクリックします。
10. 複数の AZ に HA ペアを作成する場合は、ノード 2 に対して上記の手順を繰り返す必要があります。

シングルノードシステムに **Storage VM** を作成する

以下の手順では、シングルノードシステムに新しい Storage VM を作成します。NAS LIF を作成するには 1 つのプライベート IP アドレスが必要で、管理 LIF を作成する場合はもう 1 つのプライベート IP アドレスが必要です。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. NAS LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

ここで、 _private_IP_x_は 、 e0a 上の未使用のセカンダリプライベート IP です。

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

ここで、 *private_IP_y* は e0a 上の別の未使用のセカンダリプライベート IP です。

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

の **HA** ペアに **Storage VM** を作成します 単一 **AZ**

以下の手順では、単一の AZ の HA ペアに新しい Storage VM を作成します。NAS LIF を作成するには 1 つのプライベート IP アドレスが必要で、管理 LIF を作成する場合はもう 1 つのプライベート IP アドレスが必要です。

これらの両方の LIF はノード 1 に割り当てられます。障害が発生した場合、プライベート IP アドレスをノード間で移動できます。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. ノード 1 に NAS LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

ここで、 _private_IP_x_は 、 CVO-node1 の e0a にある未使用のセカンダリプライベート IP です。テイクオーバーの際には、この IP アドレスを CVO-node2 の e0a に再配置できます。これは、サービスポリシー default-data-files が、 IP をパートナーノードに移行できることを示しているためです。

3. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

ここで、 *private_IP_y* は e0a 上の別の未使用のセカンダリプライベート IP です。

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

5. Cloud Volumes ONTAP 9.11.1以降を実行している場合は、Storage VMのネットワークサービスポリシーを変更します。

サービスの変更が必要となるのは、Cloud Volumes ONTAP がiSCSI LIFをアウトバウンド管理接続に使用できるようにするためです。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

複数の **HA** ペアに **Storage VM** を作成する **AZS**

以下の手順は、複数の AZ にまたがる HA ペア上に新しい Storage VM を作成します。

NAS LIF には _floated_ip アドレスが必要です。これは管理 LIF のオプションです。これらのフローティング IP アドレスでは、 AWS でプライベート IP を割り当てる必要はありません。代わりに、 AWS ルートテーブルに、同じ VPC 内の特定のノードの ENI を指すようにフローティング IP が自動的に設定されます。

フローティング IP が ONTAP と連携するためには、各ノードのすべての Storage VM でプライベート IP アドレスを設定する必要があります。以下の手順は、ノード 1 とノード 2 に iSCSI LIF を作成したものです。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. ノード 1 に NAS LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

   - 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。192.168.209.27 は、フローティング IP アドレスの例です。 "フローティング IP アドレスの選択の詳細については、こちらを参照してください"。
   - `-service-policy default-data-files` IPをパートナーノードに移行できることを示します。

3. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address floating_ip -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. ノード 1 に iSCSI LIF を作成

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmask nodei1Mask -lif
ip_node1_iscsi_2 -home-node cvo-node1
```

   - この iSCSI LIF は、 Storage VM でフローティング IP の LIF 移行をサポートするために必要です。iSCSI LIF である必要はありませんが、ノード間で移行するように設定することはできません。
   - `-service-policy default-data-block` IPアドレスがノード間で移行されないことを示します。
   - _private_IP_は 、 CVO-node1 の eth0 （ e0a ）上の未使用のセカンダリプライベート IP アドレスです。

5. ノード2にiSCSI LIFを作成します。

```
network interface create -vserver svm_2 -service-policy default-data-
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif
ip_node2_iscsi_2 -home-node cvo-node2
```

- この iSCSI LIF は、 Storage VM でフローティング IP の LIF 移行をサポートするために必要です。iSCSI LIF である必要はありませんが、ノード間で移行するように設定することはできません。
- `-service-policy default-data-block` IPアドレスがノード間で移行されないことを示します。
- _private_IP_は 、 CVO-node2 の eth0 （ e0a ）上の未使用のセカンダリプライベート IP アドレスです。

6. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

7. Cloud Volumes ONTAP 9.11.1以降を実行している場合は、Storage VMのネットワークサービスポリシーを変更します。

サービスの変更が必要となるのは、Cloud Volumes ONTAP がiSCSI LIFをアウトバウンド管理接続に使用できるようにするためです。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client
```

Azure で Cloud Volumes ONTAP 用のデータ提供用 Storage VM を作成します

Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは、 _ SVM _ または _ SVM _ であることがわかります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されていますが、 Azure で Cloud Volumes ONTAP を実行している場合は追加の Storage VM がサポートされます。

データを提供する Storage VM を追加で作成するには、 Azure で IP アドレスを割り当ててから、 ONTAP コマンドを実行して Storage VM とデータ LIF を作成する必要があります。

サポートされている Storage VM 数

9.9.0 リリース以降では、特定の Cloud Volumes ONTAP 構成で複数の Storage VM がサポートされます。に

アクセスします "Cloud Volumes ONTAP リリースノート" 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

他のすべての Cloud Volumes ONTAP 構成で、ディザスタリカバリに使用する 1 つのデータ提供用 Storage VM と 1 つのデスティネーション Storage VM がサポートされます。ソース Storage VM で停止が発生した場合は、デスティネーション Storage VM をデータアクセス用にアクティブ化できます。

Azure で IP アドレスを割り当てます

Storage VM を作成して LIF を割り当てる前に、 Azure で IP アドレスを割り当てる必要があります。

シングルノードシステム

Storage VM を作成して LIF を割り当てる前に、 Azure で IP アドレスを nic0 に割り当てる必要があります。

データ LIF アクセス用の IP アドレスと、 Storage VM （ SVM ）管理 LIF のオプションの IP アドレスを作成する必要があります。この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

手順

1. Azure ポータルにログインし、 * Virtual Machine * サービスを開きます。
2. Cloud Volumes ONTAP VM の名前をクリックします。
3. [* ネットワーク] をクリックします。
4. nic0 のネットワークインターフェイスの名前をクリックします。
5. [* 設定] で、 [* IP 設定 *] をクリックします。
6. [追加（ Add ）] をクリックします。
7. IP 設定の名前を入力し、 * Dynamic * を選択して、 * OK * をクリックします。
8. 作成した IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

   静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

SVM 管理 LIF を作成する場合は、上記の手順を繰り返して追加の IP アドレスを作成します。

完了後

作成したプライベート IP アドレスをコピーします。新しい Storage VM の LIF を作成するときに、これらの IP アドレスを指定する必要があります。

HA ペア

HA ペアに IP アドレスを割り当てる方法は、使用しているストレージプロトコルによって異なります。

iSCSI

Storage VM を作成して LIF を割り当てる前に、 Azure で iSCSI IP アドレスを nic0 に割り当てる必要があります。iSCSI はフェイルオーバーに ALUA を使用するため、 iSCSI の IPS はロードバランサではなく nic0 に割り当てられます。

次の IP アドレスを作成する必要があります。

- ノード 1 からの iSCSI データ LIF アクセス用に IP アドレス × 1
- ノード 2 からの iSCSI データ LIF アクセス用に 1 つの IP アドレス
- Storage VM （ SVM ）管理 LIF のオプションの IP アドレスです

  この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

手順

1. Azure ポータルにログインし、 * Virtual Machine * サービスを開きます。
2. ノード 1 の Cloud Volumes ONTAP VM の名前をクリックします。
3. [* ネットワーク] をクリックします。
4. nic0 のネットワークインターフェイスの名前をクリックします。
5. [* 設定] で、 [* IP 設定 *] をクリックします。
6. [追加（ Add ）] をクリックします。
7. IP 設定の名前を入力し、 * Dynamic * を選択して、 * OK * をクリックします。
8. 作成した IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

   静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

9. ノード 2 で上記の手順を繰り返します。
10. SVM 管理 LIF を作成する場合は、ノード 1 で上記の手順を繰り返します。

NFS

NFS に使用する IP アドレスはロードバランサに割り当てられます。これにより、フェイルオーバー時に IP アドレスがもう一方のノードに移行できるようになります。

次の IP アドレスを作成する必要があります。

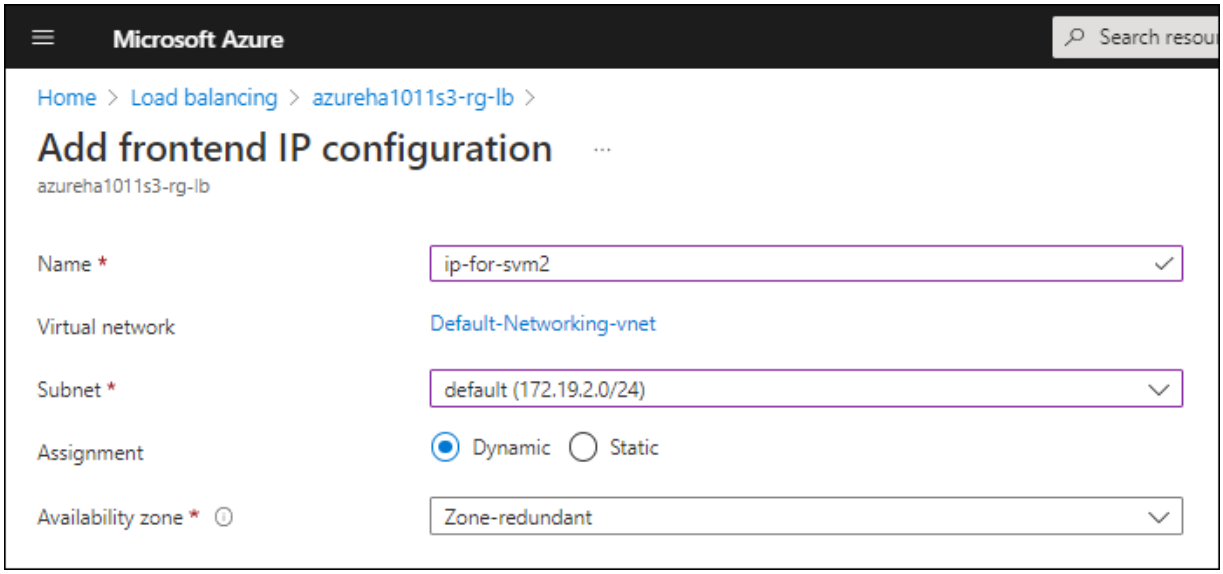
- ノード 1 から NAS データ LIF にアクセスするための IP アドレス × 1
- ノード 2 からの NAS データ LIF アクセス用に 1 つの IP アドレス
- Storage VM （ SVM ）管理 LIF のオプションの IP アドレスです

  iSCSI LIFはDNS通信に必要です。iSCSI LIF はフェイルオーバー時に移行されないため、この目的に使用されます。

  この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

手順

1. Azure ポータルで、 * ロードバランサ * サービスを開きます。
2. HA ペアのロードバランサの名前をクリックします。
3. データ LIF へのアクセスに使用するフロントエンド IP 設定をノード 1 から、データ LIF へのアクセスに使用するフロントエンド IP をノード 2 から、 Storage VM （ SVM ）管理 LIF のもう 1 つのオプションのフロントエンド IP に作成します。
   a. [* 設定] で、 [* フロントエンド IP 設定 *] をクリックします。
   b. [追加（ Add ）] をクリックします。
   c. フロントエンドIPの名前を入力し、Cloud Volumes ONTAP HAペアのサブネットを選択し、* Dynamic *が選択されたままにしておきます。また、アベイラビリティゾーンに障害が発生した場合でもIPアドレスを使用できるようにするには、ゾーン冗長*を選択したままにします。

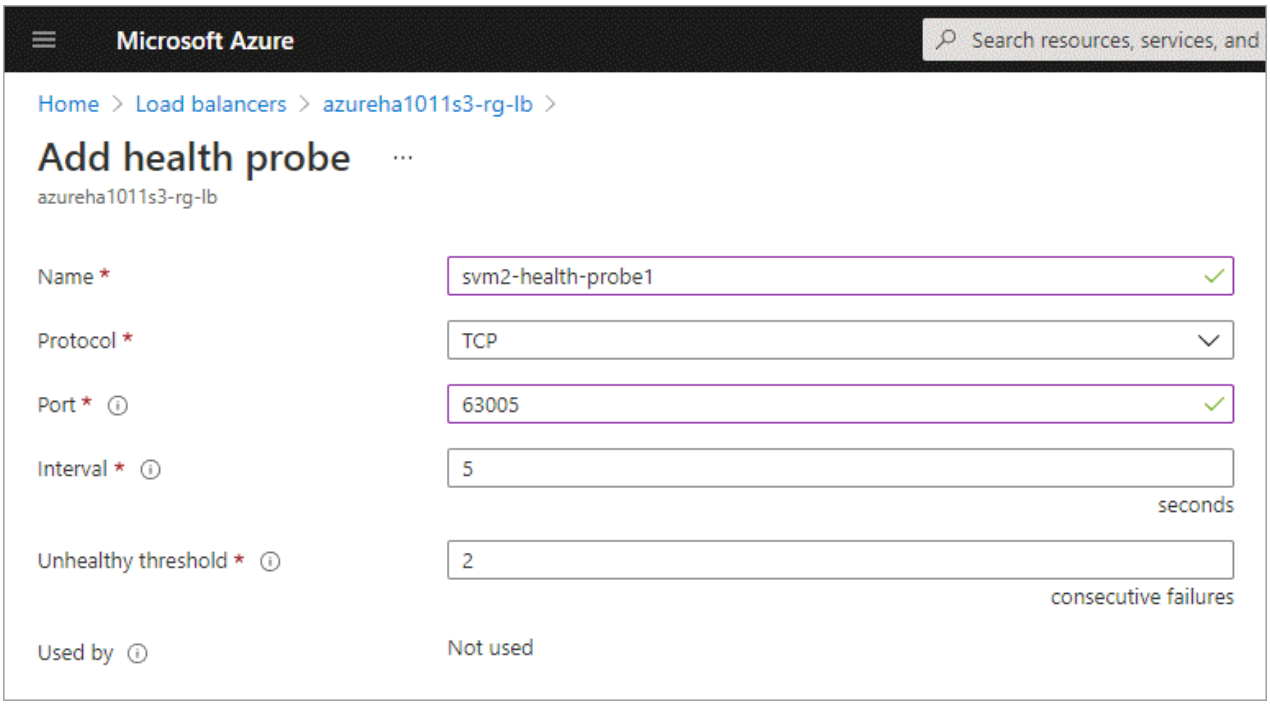


   d. 作成したフロントエンド IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

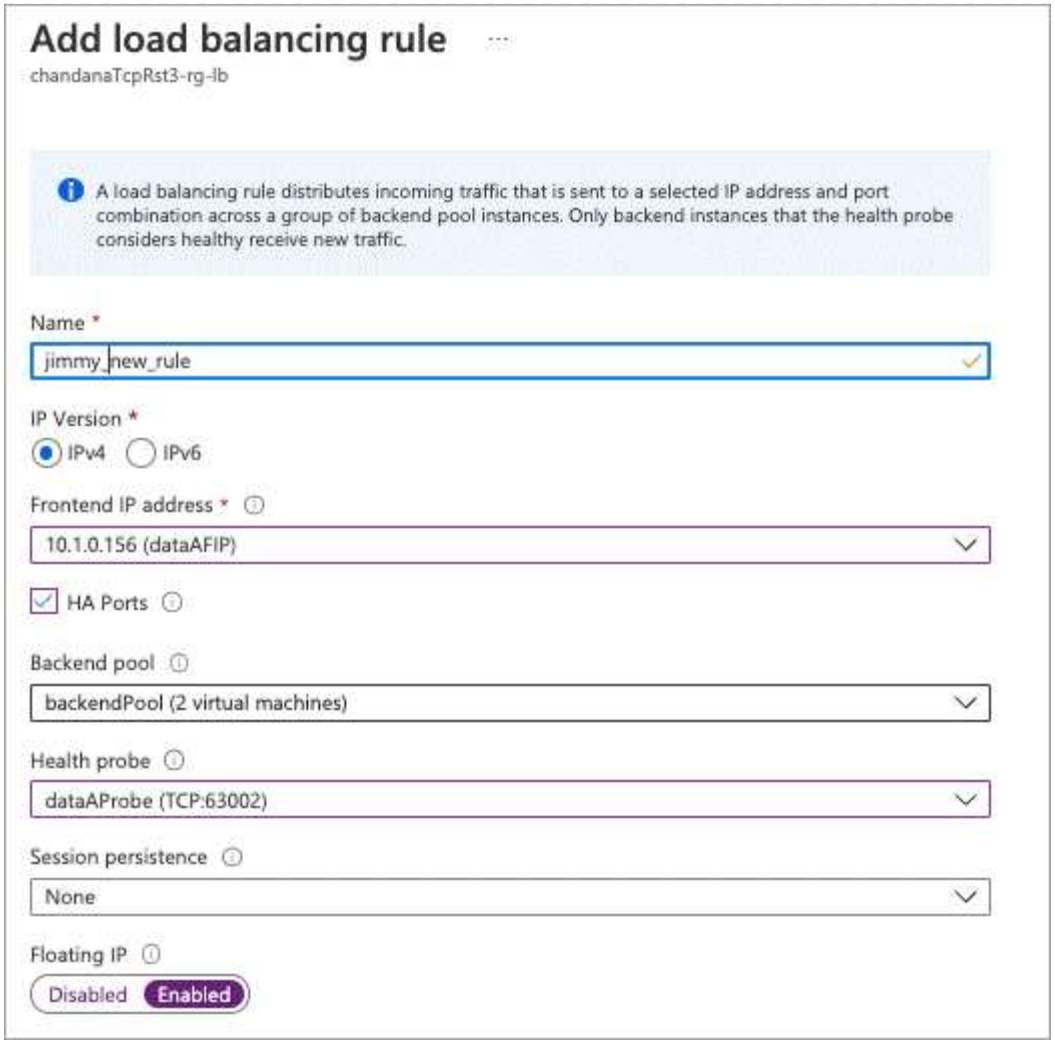
      静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

4. 作成した各フロントエンド IP のヘルスプローブを追加します。
   a. ロードバランサーの * 設定 * で、 * ヘルスプローブ * をクリックします。
   b. [追加（ Add ）] をクリックします。
   c. ヘルスプローブの名前を入力し、 63005 ～ 65000. のポート番号を入力します。他のフィールドはデフォルト値のままにします。

      ポート番号が 63005 ～ 65000. であることが重要です。たとえば、 3 つのヘルスプローブを作成する場合、ポート番号 63005 、 63006 、および 63007 を使用するプローブを入力できます。



5. フロントエンド IP ごとに新しいロードバランシングルールを作成します。
   a. ロードバランサーの * 設定 * で、 * ロードバランシングルール * をクリックします。
   b. [* 追加（ Add ）] をクリックして、必要な情報を入力する。
      - * 名前 * ：ルールの名前を入力します。
      - * IP バージョン * ：「 * ipv4 * 」を選択します。
      - * フロントエンド IP アドレス *: 作成したフロントエンド IP アドレスのいずれかを選択します。
      - *HA Ports *: このオプションを有効にします。
      - * バックエンドプール * ：すでに選択されているデフォルトのバックエンドプールをそのまま使用します。
      - * ヘルスプローブ * ：選択したフロントエンド IP に対して作成したヘルスプローブを選択します。
      - * セッション持続性 *: 「なし」を選択します。
      - * フローティング IP * ： * 有効 * を選択します。



6. Cloud Volumes ONTAP のネットワークセキュリティグループルールで、ロードバランサが上記の手順 4 で作成したヘルスプローブの TCP プローブを送信できることを確認します。これはデフォルトで許可されています。

SMB

SMB データに使用する IP アドレスはロードバランサに割り当てられます。これにより、フェイルオーバー時に IP アドレスを別のノードに移行できるようになります。

ロードバランサでは、次のIPアドレスを作成する必要があります。

- ノード 1 から NAS データ LIF にアクセスするための IP アドレス × 1
- ノード 2 からの NAS データ LIF アクセス用に 1 つの IP アドレス
- 各VMのそれぞれのNIC0のノード1のiSCSI LIFのIPアドレス
- ノード2のiSCSI LIFのIPアドレス×1

  iSCSI LIF は、 DNS 通信と SMB 通信に必要です。iSCSI LIF はフェイルオーバー時に移行されないため、この目的に使用されます。

- Storage VM （ SVM ）管理 LIF のオプションの IP アドレスです

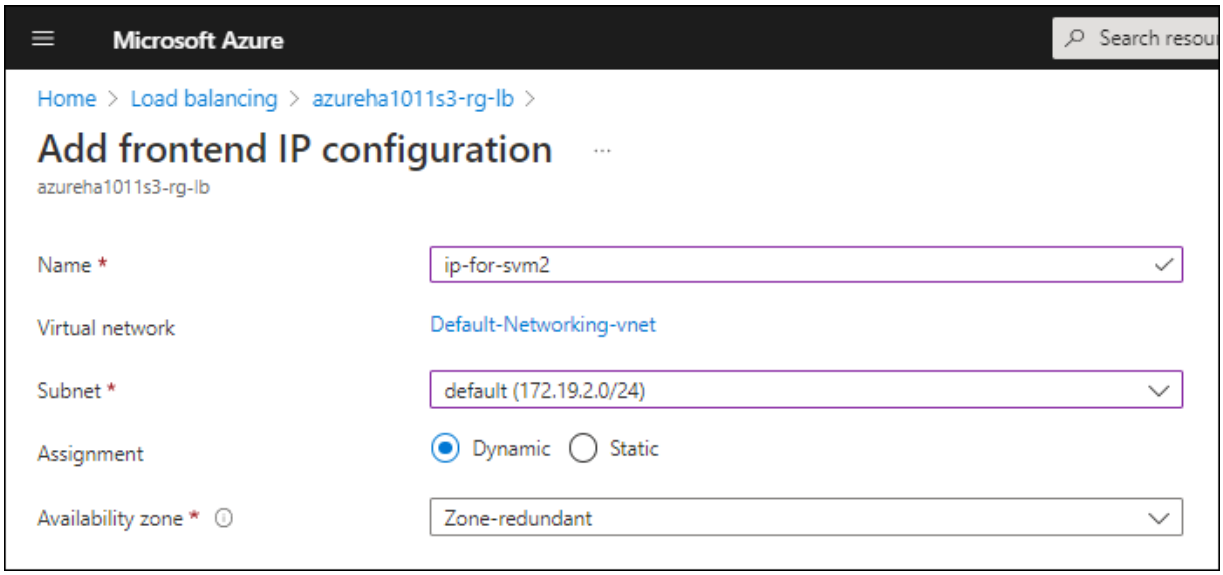
  この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

手順

1. Azure ポータルで、 * ロードバランサ * サービスを開きます。
2. HA ペアのロードバランサの名前をクリックします。
3. データLIFとSVM LIFのみに、必要な数のフロントエンドIP構成を作成します。

   フロントエンドIPは、対応する各SVMのNIC0の下にのみ作成する必要があります。SVM NIC0にIPアドレスを追加する方法の詳細については、「手順7 [ハイパーリンク]」を参照してください。

   a. [* 設定] で、 [* フロントエンド IP 設定 *] をクリックします。
   b. [追加（ Add ）] をクリックします。
   c. フロントエンドIPの名前を入力し、Cloud Volumes ONTAP HAペアのサブネットを選択し、* Dynamic *が選択されたままにしておきます。また、アベイラビリティゾーンに障害が発生した場合でもIPアドレスを使用できるようにするには、ゾーン冗長*を選択したままにします。



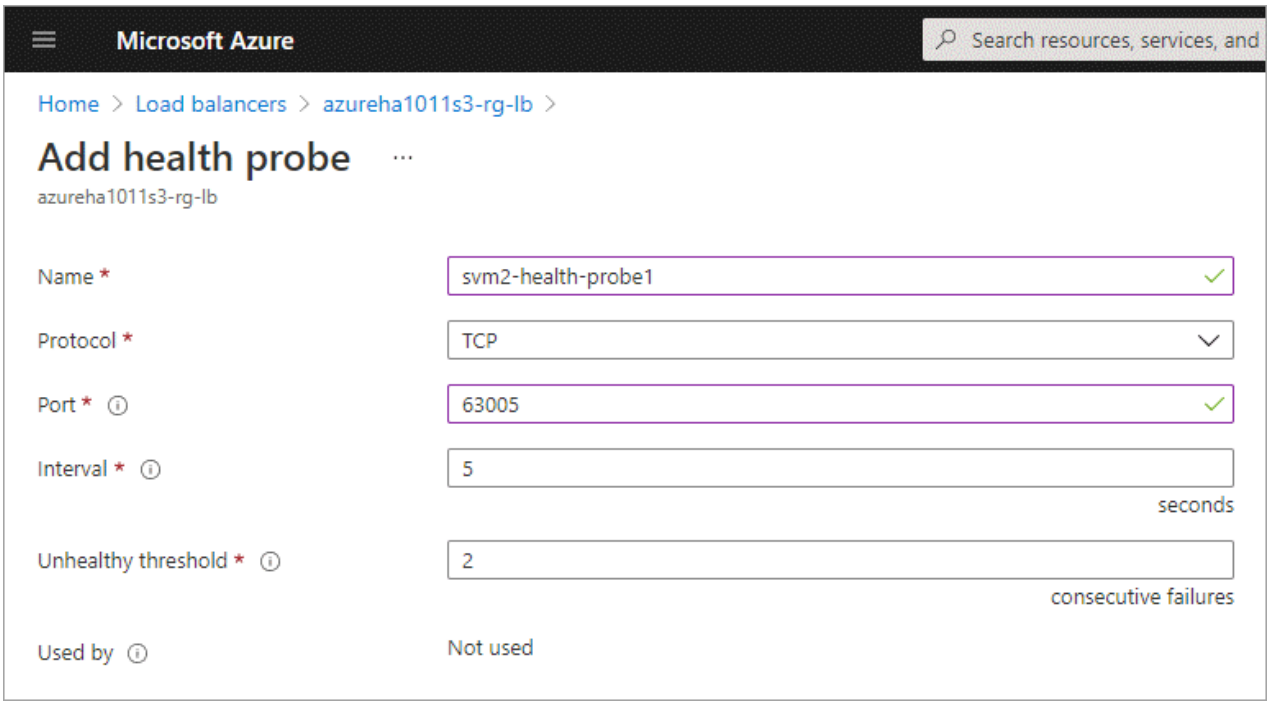
   d. 作成したフロントエンド IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

      静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

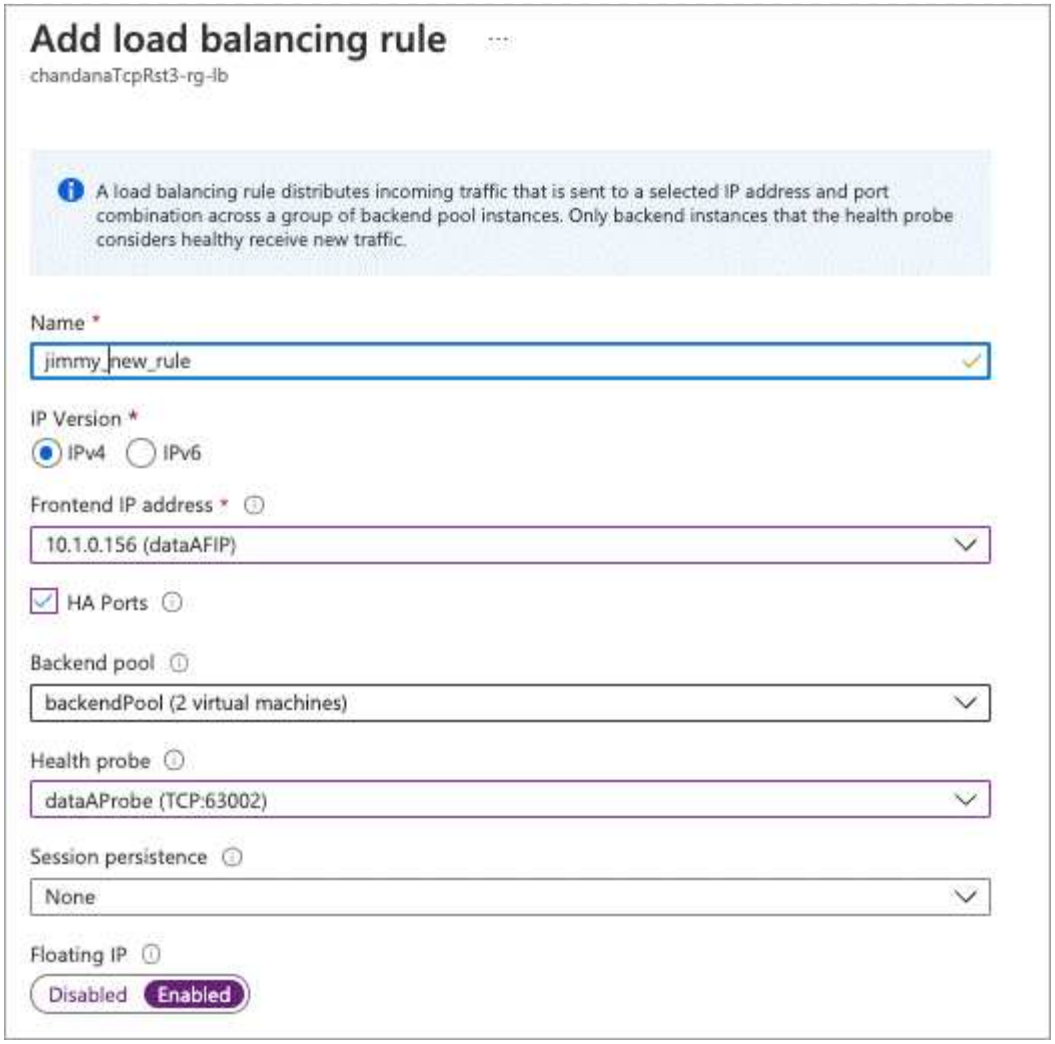
4. 作成した各フロントエンド IP のヘルスプローブを追加します。

   a. ロードバランサーの * 設定 * で、 * ヘルスプローブ * をクリックします。
   b. [追加（ Add ）] をクリックします。
   c. ヘルスプローブの名前を入力し、 63005 ～ 65000. のポート番号を入力します。他のフィールドはデフォルト値のままにします。

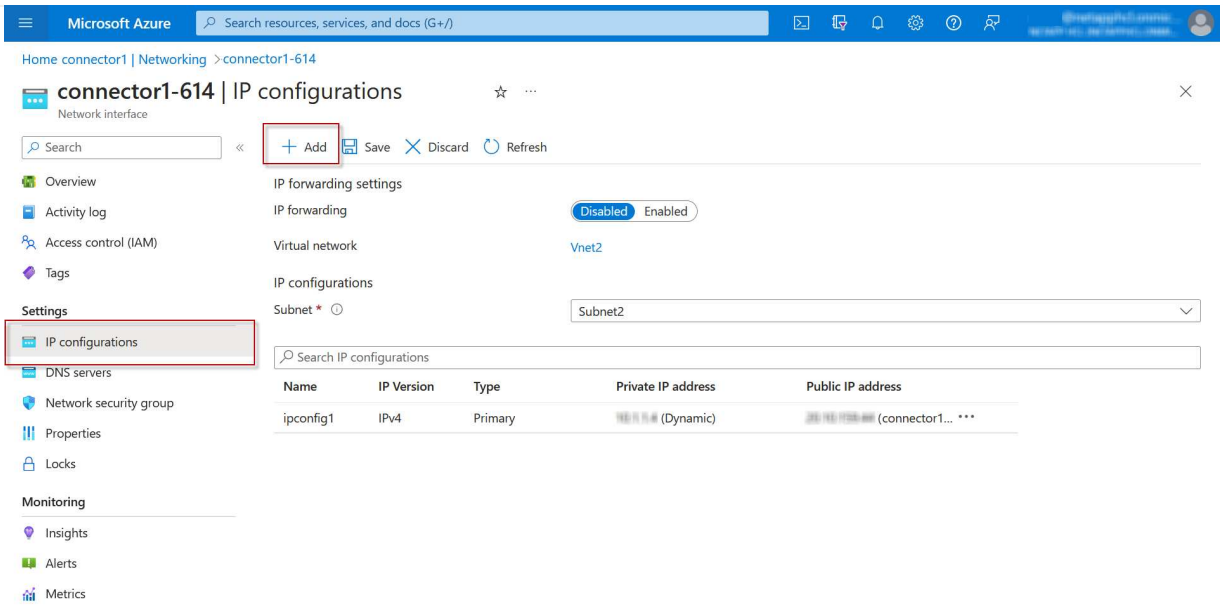
      ポート番号が 63005 ～ 65000. であることが重要です。たとえば、 3 つのヘルスプローブを作成する場合、ポート番号 63005 、 63006 、および 63007 を使用するプローブを入力できます。



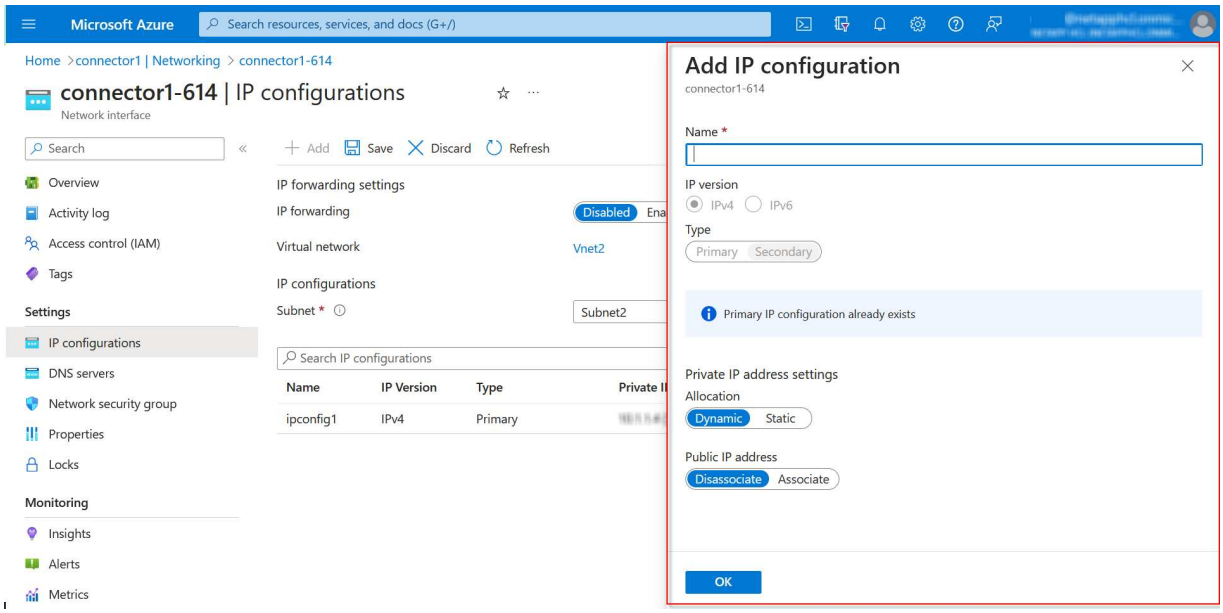
5. フロントエンド IP ごとに新しいロードバランシングルールを作成します。
   a. ロードバランサーの * 設定 * で、 * ロードバランシングルール * をクリックします。
   b. [* 追加（ Add ）] をクリックして、必要な情報を入力する。
      - * 名前 * ：ルールの名前を入力します。
      - * IP バージョン * ：「 * ipv4 * 」を選択します。
      - * フロントエンド IP アドレス *: 作成したフロントエンド IP アドレスのいずれかを選択します。
      - *HA Ports *: このオプションを有効にします。
      - * バックエンドプール * ：すでに選択されているデフォルトのバックエンドプールをそのまま使用します。
      - * ヘルスプローブ * ：選択したフロントエンド IP に対して作成したヘルスプローブを選択します。
      - * セッション持続性 *: 「なし」を選択します。
      - * フローティング IP * ： * 有効 * を選択します。



6. Cloud Volumes ONTAP のネットワークセキュリティグループルールで、ロードバランサが上記の手順 4 で作成したヘルスプローブの TCP プローブを送信できることを確認します。これはデフォルトで許可されています。
7. iSCSI LIFの場合は、NIC0のIPアドレスを追加します。
   a. Cloud Volumes ONTAP VM の名前をクリックします。
   b. [* ネットワーク] をクリックします。
   c. nic0 のネットワークインターフェイスの名前をクリックします。
   d. [Settings]で、*[IP configurations]*をクリックします。
   e. [追加（ Add ）] をクリックします。



f. IP設定の名前を入力し、[Dynamic]を選択して*[OK]*をクリックします。



ウィンドウのスクリーンショット"]

g. 作成したIP設定の名前をクリックし、AssignmentをStaticに変更して* Save *をクリックします。

静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

完了後

作成したプライベート IP アドレスをコピーします。新しい Storage VM の LIF を作成するときに、これらの IP アドレスを指定する必要があります。

Storage VM と LIF を作成

Azure で IP アドレスを割り当てると、単一のノードシステムまたは HA ペアに新しい Storage VM を作成できます。

シングルノードシステム

シングルノードシステムで Storage VM と LIF を作成する方法は、使用しているストレージプロトコルによって異なります。

iSCSI

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -netmask-length <# of mask bits> -lif <lif-name>
-home-node <name-of-node1> -data-protocol iscsi
```

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

NFS

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

SMB

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nas-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

HA ペア

HA ペアで Storage VM と LIF を作成する方法は、使用しているストレージプロトコルによって異なります。

iSCSI

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. データ LIF を作成します。

   a. 次のコマンドを使用して、ノード 1 に iSCSI LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 次のコマンドを使用して、ノード2にiSCSI LIFを作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

3. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default
```

   この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

5. Cloud Volumes ONTAP 9.11.1以降を実行している場合は、Storage VMのネットワークサービスポリシーを変更します。

   a. 次のコマンドを入力して、アドバンストモードにアクセスします。

      ```
      ::> set adv -con off
      ```

      サービスの変更が必要となるのは、Cloud Volumes ONTAP がiSCSI LIFをアウトバウンド管理接続に使用できるようにするためです。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

NFS

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. データ LIF を作成します。
   a. 次のコマンドを使用して、ノード 1 に NAS LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. 次のコマンドを使用して、ノード2にNAS LIFを作成します。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. DNS通信を提供するiSCSI LIFを作成します。
   a. 次のコマンドを使用して、ノード 1 に iSCSI LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 次のコマンドを使用して、ノード2にiSCSI LIFを作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

5. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

6. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

7. Cloud Volumes ONTAP 9.11.1以降を実行している場合は、Storage VMのネットワークサービスポリシーを変更します。

   a. 次のコマンドを入力して、アドバンストモードにアクセスします。

```
::> set adv -con off
```

   サービスの変更が必要となるのは、Cloud Volumes ONTAP がiSCSI LIFをアウトバウンド管理接続に使用できるようにするためです。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

SMB

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume
<root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name>
-gateway <ip-of-gateway-server>
```

2. NAS データ LIF を作成します。
   a. 次のコマンドを使用して、ノード 1 に NAS LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node1> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

   b. 次のコマンドを使用して、ノード2にNAS LIFを作成します。

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. DNS通信を提供するiSCSI LIFを作成します。
   a. 次のコマンドを使用して、ノード 1 に iSCSI LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node1> -data-protocol iscsi
```

   b. 次のコマンドを使用して、ノード2にiSCSI LIFを作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -netmask-length <# of mask bits> -lif
<lif-name> -home-node <name-of-node2> -data-protocol iscsi
```

4. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy system-defined -firewall-policy mgmt -home-port e0a
-auto-revert false -failover-group Default -probe-port <port-number-
for-azure-health-probe3>
```

この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

5. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

6. Cloud Volumes ONTAP 9.11.1以降を実行している場合は、Storage VMのネットワークサービスポリシーを変更します。

   a. 次のコマンドを入力して、アドバンストモードにアクセスします。

```
::> set adv -con off
```

サービスの変更が必要となるのは、Cloud Volumes ONTAP がiSCSI LIFをアウトバウンド管理接続に使用できるようにするためです。

```
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name>
-policy default-data-iscsi -service management-nis-client
```

次の手順

HA ペアに Storage VM を作成したら、その SVM でストレージをプロビジョニングする前に 12 時間待つことを推奨します。Cloud Volumes ONTAP 9.10.1リリース以降、12時間の間にHAペアのロードバランサの設定がスキャンされます。新しいSVMがある場合、計画外フェイルオーバーを短時間にする設定がBlueXPで有効になります。

Google CloudでCloud Volumes ONTAP 用のデータ提供用Storage VMを作成

Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは、 _ SVM _ または _ SVM _ であることがわかります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されますが、一部の設定では追加の Storage VM がサポートされます。

サポートされている **Storage VM** 数

9.11.1リリース以降、Google Cloudの特定のCloud Volumes ONTAP 構成で複数のStorage VMがサポートされています。にアクセスします "Cloud Volumes ONTAP リリースノート" 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

他のすべての Cloud Volumes ONTAP 構成で、ディザスタリカバリに使用する 1 つのデータ提供用 Storage VM と 1 つのデスティネーション Storage VM がサポートされます。ソース Storage VM で停止が発生した場合は、デスティネーション Storage VM をデータアクセス用にアクティブ化できます。

Storage VM を作成

ライセンスでサポートされている場合は、1つのノードシステムまたはHAペアに複数のStorage VMを作成できます。HAペアでStorage VMを作成する場合はBlueXP APIを使用する必要がありますが、CLIまたはSystem Managerを使用してシングルノードシステムでStorage VMを作成できます。

シングルノードシステム

以下の手順では、CLIを使用してシングルノードシステムに新しいStorage VMを作成します。データLIFを作成するにはプライベートIPアドレスが1つ必要で、管理LIFを作成する場合はプライベートIPアドレスをもう1つ必要になります。

手順

1. Google Cloudで、Cloud Volumes ONTAP インスタンスに移動し、各LIFのnic0にIPアドレスを追加します。

Storage VMに管理LIFを作成する場合は、データLIF用に1つのIPアドレスが必要です。また、オプションのIPアドレスをもう1つ追加する必要があります。

"Google Cloudのドキュメント：「Adding alias IP ranges to an existing instance"

2. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway <ip-of-gateway-server>
```

3. Google Cloudで追加したIPアドレスを指定してデータLIFを作成します。

iSCSI

```
network interface create -vserver <svm-name> -home-port e0a -address
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data
-protocol iscsi
```

NFS または **SMB**

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

4. オプション：Google Cloudで追加したIPアドレスを指定して、Storage VM管理LIFを作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role data
-data-protocol none -address <svm-mgmt-ip-address> -netmask-length
<length> -home-node <name-of-node1> -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert false
-failover-group Default
```

5. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver <svm-name> -aggregates <aggr1,aggr2>
```

この手順は、 Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

HA ペア

Google CloudのCloud Volumes ONTAP システムでStorage VMを作成するには、BlueXP APIを使用する必要があります。BlueXPでは、必要なLIFサービスがStorage VMに設定され、アウトバウンドのSMB / CIFS通信に必要なiSCSI LIFが設定されるため、API（System ManagerやCLIではなく）を使用する必要があります。

BlueXPはGoogle Cloudで必要なIPアドレスを割り当て、SMB / NFSアクセス用のデータLIFとアウトバウンドSMB通信用のiSCSI LIFを備えたStorage VMを作成します。

必要な**Google Cloud**権限

Cloud Volumes ONTAP HAペア用のStorage VMを作成および管理するには、コネクタに特定の権限が必要です。必要な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"。

手順

1. Storage VMを作成するには、次のAPI呼び出しを使用します。

   ```
   POST /occm/api/gcp/ha/working-environments/{WE_ID}/svm/
   ```

   要求の本文には次の情報が含まれている必要があります

   ```
   { "svmName": "myNewSvm1" }
   ```

HAペアのStorage VMを管理します

また、BlueXP APIでは、HAペアのStorage VMの名前変更と削除もサポートされています。

Storage VMの名前を変更します

必要に応じて、Storage VMの名前はいつでも変更できます。

手順

1. Storage VMの名前を変更するには、次のAPI呼び出しを使用します。

   ```
   PUT /occm/api/gcp/ha/working-environments/{WE_ID}/svm
   ```

   要求の本文には次の情報が含まれている必要があります

   ```
   {
   "svmNewName": "newSvmName",
   "svmName": "oldSvmName"
   }
   ```

Storage VMを削除します

不要になったStorage VMはCloud Volumes ONTAP から削除できます。

手順

1. Storage VMを削除するには、次のAPI呼び出しを使用します。

   ```
   DELETE /occm/api/gcp/ha/working-environments/{WE_ID}/svm/{SVM_NAME}
   ```

SVMディザスタリカバリのセットアップ

BlueXPは、Storage VM（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のサポートは提供していません。System Manager または CLI を使用する必要があります。

2つのCloud Volumes ONTAPシステム間にSnapMirror SVMレプリケーションを設定する場合は、2つのHAペ

アシステム間または2つのシングルノードシステム間でレプリケーションを行う必要があります。HAペアとシングルノードシステムの間にSnapMirror SVMレプリケーションをセットアップすることはできません。

CLIの手順については、次のドキュメントを参照してください。

- "SVM ディザスタリカバリ設定エクスプレスガイド"
- "SVM ディザスタリカバリエクスプレスガイド"

セキュリティとデータ暗号化

ネットアップの暗号化ソリューションによるボリュームの暗号化

Cloud Volumes ONTAP は、 NetApp Volume Encryption （ NVE ）および NetApp Aggregate Encryption （ NAE ）をサポートしています。NVEとNAEは、FIPS 140-2に準拠したボリュームの保管データ暗号化を可能にするソフトウェアベースのソリューションです。 "これらの暗号化ソリューションの詳細については、こちらをご覧ください"。

NVE と NAE はどちらも外部キー管理機能でサポートされています。

AWS Key Management Serviceを使用してキーを管理します

を使用できます "AWS Key Management Service（KMS）" Google Cloud Platform導入アプリケーションでONTAP 暗号化キーを保護します。

AWS KMSを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

KMSを使用する場合は、デフォルトではデータSVMのLIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、AWSの認証サービスとの通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

作業を開始する前に

- Cloud Volumes ONTAPでバージョン9.12.0以降が実行されている必要があります
- Volume Encryption（VE）ライセンスとをインストールしておく必要があります
- Multi-tenant Encryption Key Management（MTEKM）ライセンスをインストールしておく必要があります。
- クラスタ管理者またはSVMの管理者である必要があります
- 有効なAWSサブスクリプションが必要です

設定できるのはデータSVMのキーだけです。

設定

AWS

1. を作成する必要があります "グラント" 暗号化を管理するIAMロールで使用されるAWS KMSキー用。IAM

ロールには、次の処理を許可するポリシーが含まれている必要があります。

- `DescribeKey`
- `Encrypt`
- `Decrypt`
  認可を作成するには、を参照してください "AWSのドキュメント"。

2. "適切なIAMロールにポリシーを追加します。" ポリシーでがサポートされている必要があります `DescribeKey`、 `Encrypt`および `Decrypt` 操作：

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP環境に切り替えます。
2. advanced 権限レベルに切り替えます。
   `set -privilege advanced`
3. AWSキー管理ツールを有効にします。
   `security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. プロンプトが表示されたら、シークレットキーを入力します。
5. AWS KMSが正しく設定されたことを確認します。
   `security key-manager external aws show -vserver svm_name`

Azure Key Vaultを使用してキーを管理します

を使用できます "Azure キーボールト（ AKV ）" Azureで導入されたアプリケーションでONTAP 暗号化キーを保護するため。

AKVは保護に使用できます "NetApp Volume Encryption （ NVE ）キー" データSVMの場合のみ。

AKVを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

AKVを使用する場合、デフォルトではクラウドキー管理エンドポイントとの通信にデータSVM LIFが使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（login.microsoftonline.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

作業を開始する前に

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption（VE）ライセンスがインストールされている（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る）
- マルチテナント暗号化キー管理（MT_EK_MGMT）ライセンスが必要です
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなAzureサブスクリプション

制限

- AKVはデータSVM上でのみ設定できます

設定プロセス

AzureにCloud Volumes ONTAP 構成を登録する方法と、Azure Key Vaultとキーを作成する方法を概説しています。これらの手順をすでに完了している場合は、特に、で正しい設定を行っていることを確認してください Azureキーバックアップを作成しますをクリックし、に進みます Cloud Volumes ONTAP 構成。

- Azureアプリケーション登録
- Azureクライアントシークレットを作成する
- Azureキーバックアップを作成します
- 暗号化キーを作成します
- Azure Active Directoryエンドポイントの作成（HAのみ）
- Cloud Volumes ONTAP 構成

Azureアプリケーション登録

1. Cloud Volumes ONTAP からAzure Key Vaultへのアクセスに使用するAzureサブスクリプションにアプリケーションを登録しておく必要があります。Azureポータルで、アプリケーション登録を選択します。
2. 新規登録を選択します。
3. アプリケーションの名前を指定し、サポートされているアプリケーションタイプを選択します。デフォルトの単一テナントでAzure Key Vaultの使用量が十分に設定されていること。[登録]を選択します。
4. Azureの概要ウィンドウで、登録したアプリケーションを選択します。アプリケーション（クライアント）**ID**およびディレクトリ（テナント）**ID**を安全な場所にコピーします。これらの情報は、後で登録プロセスで必要になります。

Azureクライアントシークレットを作成する

1. Azure Key Vaultアプリケーション登録用のAzureポータルで、[証明書とシークレット]ペインを選択します。
2. ［新しいクライアントシークレット］を選択します。クライアントシークレットにわかりやすい名前を入力します。ネットアップでは24カ月の有効期限を推奨していますが、クラウドガバナンスポリシーによっては、別の設定が必要になる場合があります。
3. クライアントシークレットを作成するには、[追加]をクリックします。value**カラムに表示されているシークレット文字列をコピーし、後でで使用できるように安全な場所に保存します Cloud Volumes ONTAP 構成。シークレット値は、ページから移動したあとに再び表示されません。

Azureキーバックアップを作成します

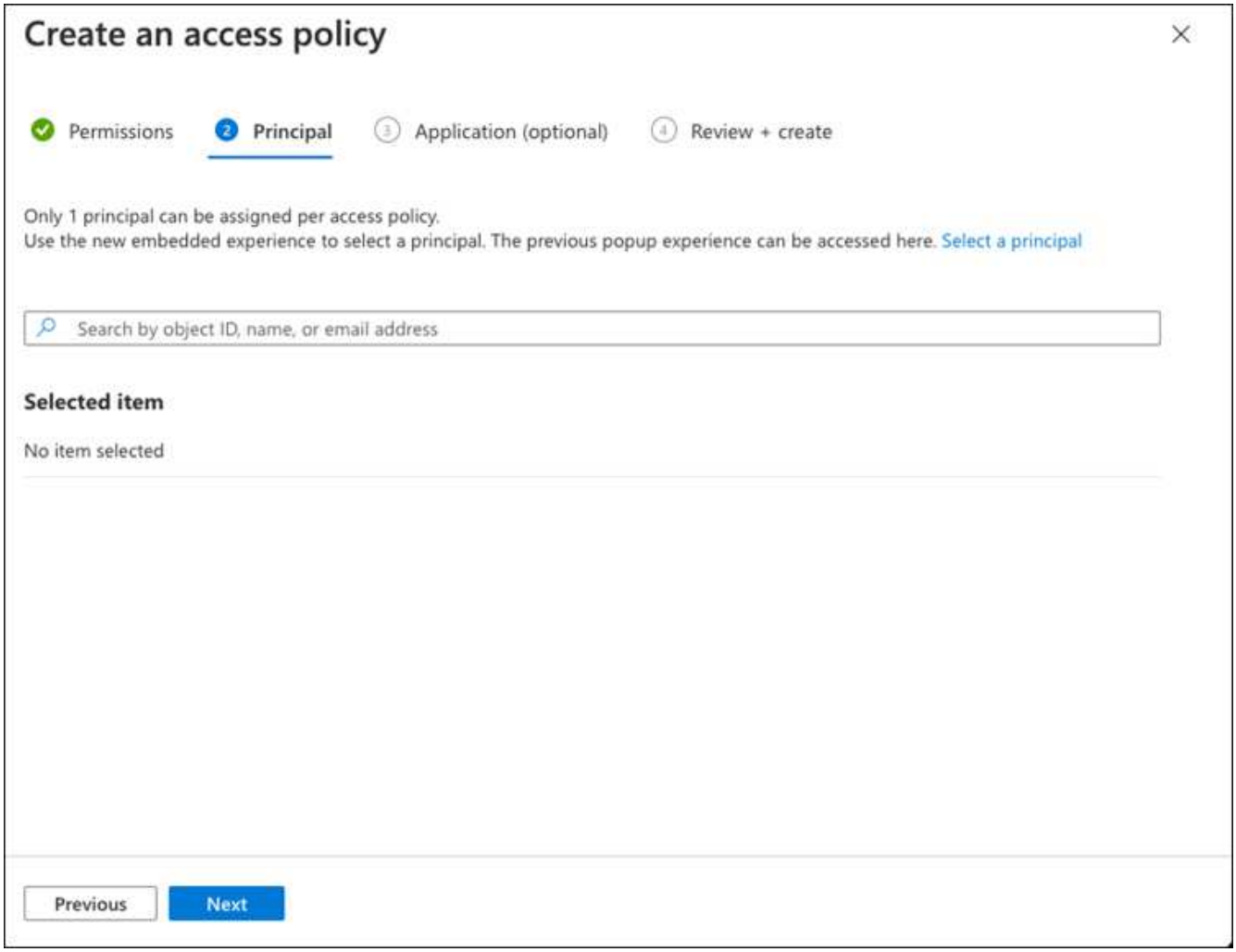
1. 既存のAzure Key Vaultがある場合はCloud Volumes ONTAP 構成に接続できますが、このプロセスの設定にアクセスポリシーを適用する必要があります。
2. Azureポータルで、[** Key Vaults（キーボルト）]セクションに移動します。
3. **[+Create]**をクリックして、リソースグループ、地域、価格階層などの必要な情報を入力します。また、削除したボールトを保持する日数を入力し、キーボールトでパージ保護を有効にする**を選択します。
4. アクセスポリシーを選択するには、 **Next**を選択してください。
5. 次のオプションを選択します。
   a. [アクセス構成]で、[ボールトアクセスポリシー]を選択します。
   b. [リソースアクセス]で、[**Azure Disk Encryption for Volume Encryption**]を選択します。

6. アクセスポリシーを追加するには、**+Create**を選択します。
7. [テンプレートから構成する]の下のドロップダウンメニューをクリックし、[キー]、[シークレット]、[証明書管理]テンプレートを選択します。
8. 各ドロップダウンメニュー(キー、シークレット、証明書)を選択し、メニューリストの一番上にある**[All]**を選択して、使用可能なすべてのアクセス許可を選択します。次の作業を完了しておきます
   - キーの権限：20を選択
   - シークレット権限:8が選択されています
   - 証明書のアクセス許可:16が選択されています


Create an access policy
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign
Privileged Key Operations
Select all
Purge
Release
Rotation Policy Operations
Select all
Rotate
Get Rotation Policy
Set Rotation Policy
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
List Certificate Authorities
Set Certificate Authorities
Delete Certificate Authorities
Privileged Certificate Operations
Select all
Purge
Previous
Next

9. **Next**をクリックして、で作成した**Principal** Azure登録アプリケーションを選択します Azureアプリケーション登録。 **Next** を選択します。

   1つのポリシーに割り当てることができるプリンシパルは1つだけです。



10. 「次へ」を2回クリックして「レビュー」および「作成」に到着します。次に、[作成]をクリックします。
11. **Next**を選択して、**Networking**オプションに進みます。
12. 適切なネットワークアクセス方法を選択するか、すべてのネットワークおよびレビュー+作成を選択して、キーボールトを作成します。（ネットワークアクセス方法は、ガバナンスポリシーまたは企業のクラウドセキュリティチームによって規定されている場合があります）。
13. キーボールトURIを記録します。作成したキーボールトで、概要メニューに移動し、右側のカラムから**Vault URI** をコピーします。これはあとで実行する必要があります。

暗号化キーを作成します

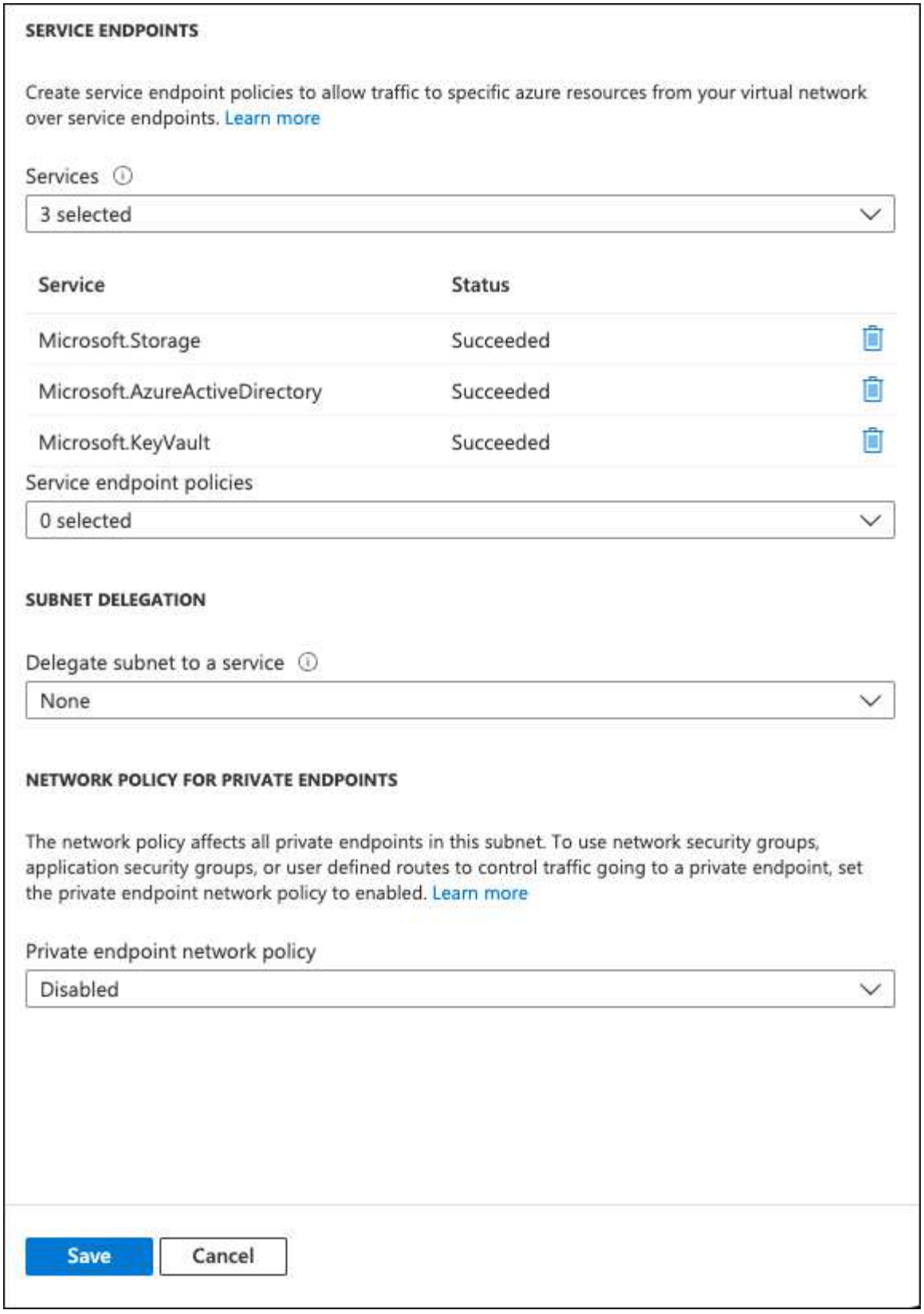
1. Cloud Volumes ONTAP 用に作成したキー・ボールトのメニューで、[**Keys**（キー**）]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。

- 暗号化キー名
- キータイプ：rsa
- RSAキーのサイズ：2048
- 有効：はい

5. [**Create]を選択して、暗号キーを作成します。
6. [**Keys**（キー**）]メニューに戻り、作成したキーを選択します。
7. キーのプロパティを表示するには、[**Current version**（現在のバージョン**）]でキーIDを選択します。
8. [**Key Identifier**（キー識別子**）]フィールドを探します。URIを16進数の文字列以外の値にコピーします。

Azure Active Directoryエンドポイントの作成（**HA**のみ）

1. このプロセスは、HA Cloud Volumes ONTAP 作業環境用にAzure Key Vaultを設定する場合にのみ必要です。
2. Azureポータルで、**Virtual Networks**に移動します。
3. Cloud Volumes ONTAP 作業環境を展開した仮想ネットワークを選択し、ページの左側にある **Subnets** メニューを選択します。
4. Cloud Volumes ONTAP 環境のサブネット名をリストから選択します。
5. [サービスエンドポイント]見出しに移動します。ドロップダウンメニューで、次のいずれかを選択します。
   - **Microsoft.AzureActiveDirectory**
   - **Microsoft.KeyVault**
   - **Microsoft.Storage**（オプション）



6. 保存を選択して、設定を取得します。

Cloud Volumes ONTAP 構成

1. 優先SSHクライアントを使用してクラスタ管理LIFに接続します。
2. ONTAP でadvanced権限モードに切り替えます。

```
set advanced -con off
```

3. 目的のデータSVMを特定し、そのDNS設定を確認します。
   `vserver services name-service dns show`

   a. 目的のデータSVMのDNSエントリが存在し、そのエントリにAzure DNSのエントリが含まれている場合は、対処は必要ありません。表示されない場合は、Azure DNS、プライベートDNS、またはオンプレミスサーバを指すデータSVMのDNSサーバエントリを追加します。 クラスタ管理SVMのエントリと同じである必要があります。
      `vserver services name-service dns create -vserver SVM_name -domains domain -name-servers IP_address`

   b. データSVM用にDNSサービスが作成されたことを確認します。
      `vserver services name-service dns show`

4. アプリケーションの登録後に保存されたクライアントIDとテナントIDを使用して、Azure Key Vaultを有効にします。
   `security key-manager external azure enable -vserver SVM_name -client-id Azure_client_ID -tenant-id Azure_tenant_ID -name Azure_key_vault_name -key-id Azure_key_ID`

5. キー管理ツールのステータスを確認します。
   `security key-manager external azure check`
   出力は次のようになります。

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
    Status: OK

Category: ekmip_server
    Status: OK

Category: kms_wrapped_key_status
    Status: UNKNOWN
    Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

状況に応じて `service_reachability` ステータスがではありません `OK`では、必要なすべての接続と権限を使用してSVMがAzure Key Vaultサービスにアクセスすることはできません。Azureのネットワークポリシーとルーティングによって、プライベートVNetがAzure KeyVaultパブリックエンドポイントに到達できないようにしてください。その場合は、Azureプライベートエンドポイントを使用してVNet内からキーヴォールトにアクセスすることを検討してください。エンドポイントのプライベートIPアドレスを解決するために、SVMに静的ホストエントリを追加する必要がある場合もあります。

。 `kms_wrapped_key_status` が報告します `UNKNOWN` 初期設定時。ステータスがに変わります `OK` 最初

のボリュームが暗号化されたあと。

6. オプション：NVEの機能を検証するテストボリュームを作成する

   ```
   vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size
   -state online -policy default
   ```

   正しく設定されていれば、Cloud Volumes ONTAP でボリュームが自動的に作成され、ボリューム暗号化が有効になります。

7. ボリュームが正しく作成および暗号化されたことを確認します。表示されている場合は、 `-is -encrypted` パラメータは次のように表示される `true`。
   `vol show -vserver SVM_name -fields is-encrypted`

GoogleのCloud Key Management Serviceを使用してキーを管理します

を使用できます "Google Cloud Platform のキー管理サービス（ Cloud KMS ）" Google Cloud Platform導入アプリケーションでONTAP 暗号化キーを保護します。

Cloud KMSを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にすることができます。

Cloud KMSを使用する場合は、デフォルトではデータSVMのLIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（oauth2.googleapis.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

作業を開始する前に

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption （ VE ）ライセンスがインストールされている
- Cloud Volumes ONTAP 9.12.1 GA以降、マルチテナント暗号化キー管理（MTEKM）ライセンスがインストールされています。
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなGoogle Cloud Platformサブスクリプション

制限

- クラウドKMSはデータSVMでのみ設定できます

設定

Google Cloud

1. Google Cloud環境では、 "対称GCPキーリングとキーを作成します"。
2. Cloud Volumes ONTAP サービスアカウント用のカスタムロールを作成します。

```
gcloud iam roles create kmsCustomRole
    --project=<project_id>
    --title=<kms_custom_role_name>
    --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loca
tions.get,cloudkms.locations.list,resourcemanager.projects.get
    --stage=GA
```

3. Cloud KMSキーとCloud Volumes ONTAPサービスアカウントにカスタムロールを割り当てます。
   `gcloud kms keys add-iam-policy-binding` *`key_name`* `--keyring` *`key_ring_name`* `--location` *`key_location`* `--member serviceAccount:_service_account_Name_ --role projects/`*`customer_project_id`*`/roles/kmsCustomRole`
4. サービスアカウントのJSONキーをダウンロード：
   `gcloud iam service-accounts keys create key-file --iam-account=`*`sa-name`*`@`*`project-id`*`.iam.gserviceaccount.com`

Cloud Volumes ONTAP

1. 優先SSHクライアントを使用してクラスタ管理LIFに接続します。
2. advanced 権限レベルに切り替えます。
   `set -privilege advanced`
3. データSVM用のDNSを作成
   `dns create -domains c.<`*`project`*`>.internal -name-servers` *`server_address`* `-vserver` *`SVM_name`*
4. CMEKエントリの作成：
   `security key-manager external gcp enable -vserver` *`SVM_name`* `-project-id` *`project`* `-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
5. プロンプトが表示されたら、GCPアカウントのJSONキーを入力します。
6. 有効なプロセスが成功したことを確認します。
   `security key-manager external gcp check -vserver` *`svm_name`*
7. オプション：暗号化をテストするボリュームを作成します。 `vol create` *`volume_name`* `-aggregate` *`aggregate`* `-vserver` *`vserver_name`* `-size 10G`

トラブルシューティングを行う

トラブルシューティングが必要な場合は、上記の最後の2つの手順でREST APIのrawログをテールできます。

1. `set d`
2. `systemshell -node` *`node`* `-command tail -f /mroot/etc/log/mlog/kmip2_client.log`

ランサムウェアからの保護を強化

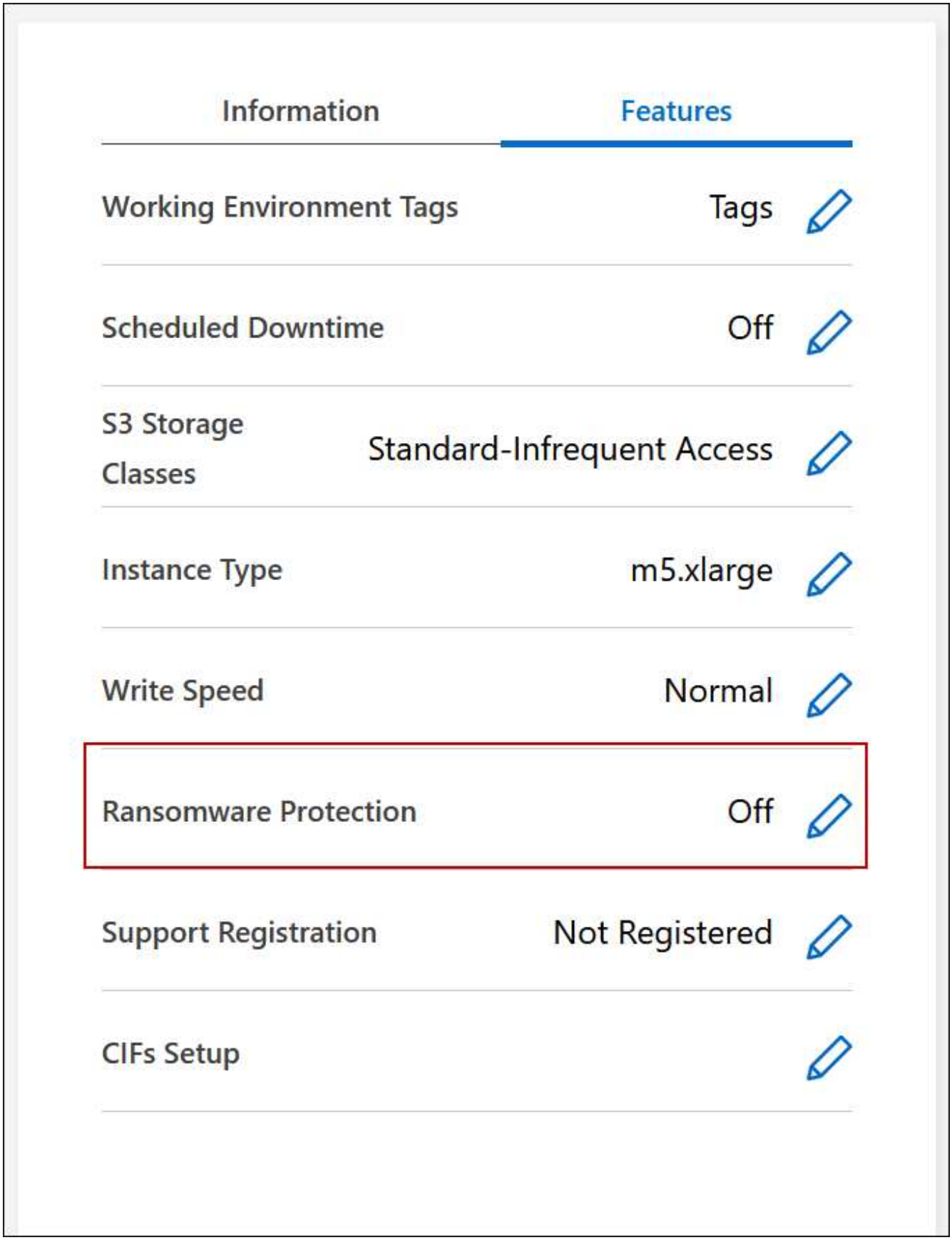
ランサムウェア攻撃は、ビジネス時間、リソース、評判を低下させる可能性があります。BlueXPでは、ランサムウェア向けの2つのNetAppソリューションを実装できます。一般的なランサムウェアファイル拡張子からの保護と、自律型ランサムウェア対策（ARP）です。これらのソリューションは、可視化、検出、修復のための効果的なツールを提供します。

一般的なランサムウェアのファイル拡張子から保護

BlueXPで利用可能なランサムウェア対策設定を使用すると、ONTAP FPolicy機能を利用して、一般的なランサムウェアファイル拡張子タイプから保護できます。

手順

1. [Canvas]ページで、ランサムウェア対策に設定したシステムの名前をダブルクリックします。
2. [Overview]タブで、[Features]パネルをクリックし、*[Ransomware Protection]*の横にある鉛筆アイコンをクリックします。



3. 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。

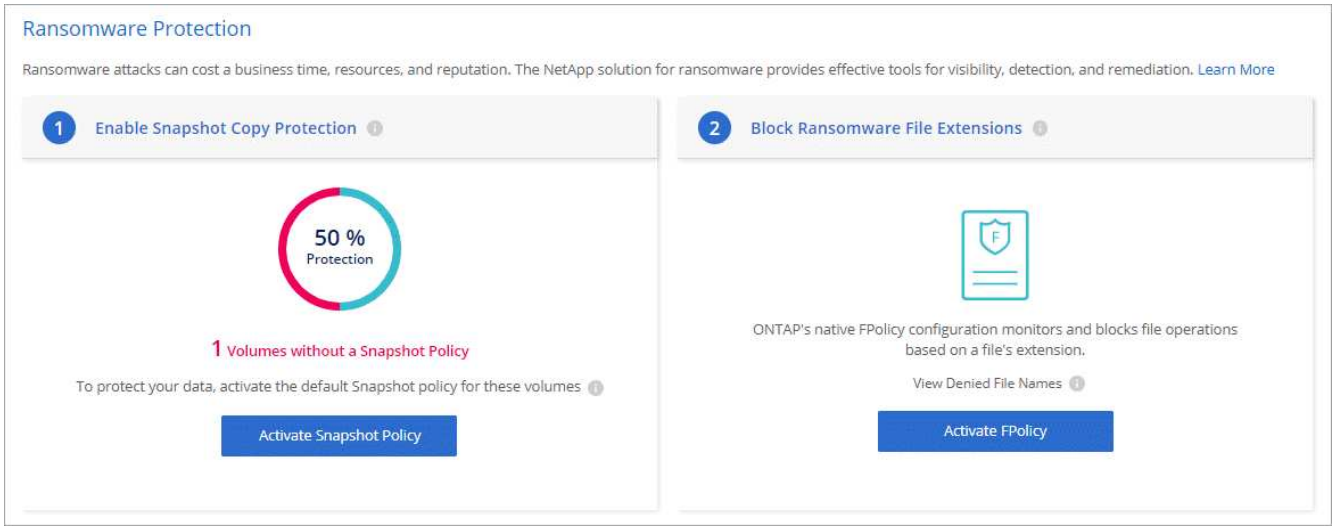
b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

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。

デフォルトの FPolicy スコープは、次の拡張子を持つファイルをブロックします。

マイクロ、暗号化、ロック、暗号化、暗号化、暗号化 crinf 、 r5a 、 XRNT 、 XTBL 、 R16M01D05 、 pzdc 、 good 、 LOL! 、 OMG! 、 RDM 、 RRK 、 encryptedRS 、 crjoker 、 enciphered 、 LeChiffre

Cloud Volumes ONTAP でFPolicyをアクティブ化すると、このスコープが作成されます。このリストは、一般的なランサムウェアのファイルタイプに基づいています。ブロックされるファイル拡張子をカスタマイズするには、 Cloud Volumes ONTAP CLI から _ vserver fpolicy policy scope_コマンド を使用します。



自律的なランサムウェア防御

Cloud Volumes ONTAPは、Autonomous Ransomware Protection（ARP）機能をサポートしています。この機能は、ワークロードを分析し、ランサムウェア攻撃の可能性がある異常なアクティビティをプロアクティブに検出して警告します。

で提供されるファイル拡張子保護とは別に、 "ランサムウェア対策設定"ARP機能は、ワークロード分析を使用して、検出された「異常なアクティビティ」に基づいて潜在的な攻撃についてユーザに警告します。ランサムウェア対策設定とARP機能の両方を組み合わせて、包括的なランサムウェア対策を行うことができます。

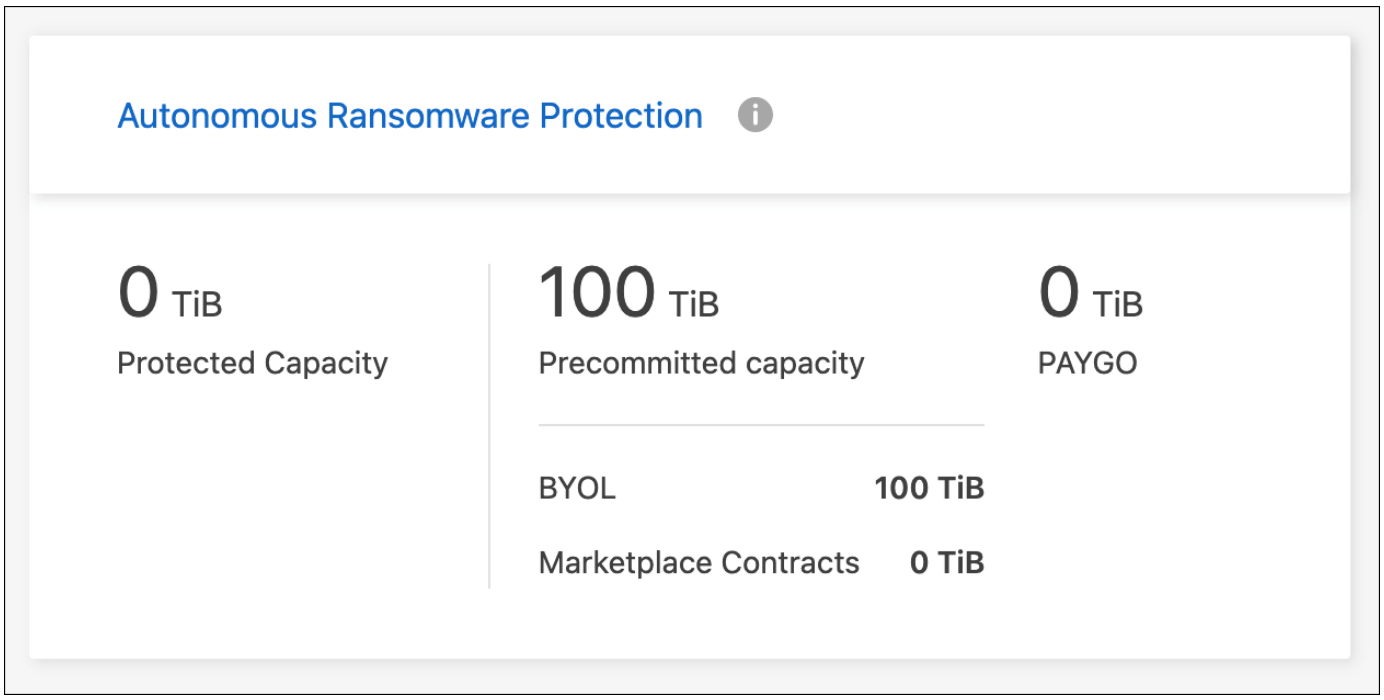
ARP機能は、ノードベースと容量ベースの両方のライセンスモデルで、BYOLライセンス（1年、2年、3年契

約）でのみ使用できます。Cloud Volumes ONTAPのARP機能で使用する新しいアドオンライセンスを別途購入するには、NetAppの営業担当者にお問い合わせください。

アドオンライセンスを購入してデジタルウォレットに追加すると、Cloud Volumes ONTAPを使用してボリューム単位でARPを有効にできます。ボリュームのARPの設定は、ONTAP System ManagerとONTAP CLIを使用して実行します。

ONTAP System ManagerおよびCLIでARPを有効にする方法の詳細については、を参照してください "自動ランサムウェア対策を有効化"。

ライセンスがないと、ライセンスされた機能の使用はサポートされません。



システム管理

Cloud Volumes ONTAP ソフトウェアをアップグレードします

Cloud Volumes ONTAP をBlueXPからアップグレードすると、最新の新機能と拡張機能にアクセスできます。ソフトウェアをアップグレードする前に、 Cloud Volumes ONTAP システムを準備する必要があります。

アップグレードの概要

Cloud Volumes ONTAP のアップグレードプロセスを開始する前に、次の点に注意してください。

BlueXPのみからのアップグレード

Cloud Volumes ONTAP のアップグレードは、BlueXP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

アップグレード方法

BlueXPには、Cloud Volumes ONTAP をアップグレードする2つの方法があります。

- アップグレード通知が作業環境に表示されます
- アップグレードイメージをHTTPSの場所に配置し、BlueXPにURLを提供する

サポートされているアップグレードパス

アップグレード可能な Cloud Volumes ONTAP のバージョンは、現在実行している Cloud Volumes ONTAP のバージョンによって異なります。

現在のバージョン	に直接アップグレードできるバージョン
9.13.0	9.13.1.
9.12.1:	9.13.1.
	9.13.0
9.12.0	9.12.1:
9.11.1	9.12.1:
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2.	9.3
9.1	9.2.
9.0	9.1
8.3	9.0

次の点に注意してください。

- Cloud Volumes ONTAP でサポートされるアップグレードパスは、オンプレミスの ONTAP クラスタの場

合とは異なります。

- 作業環境に表示されるアップグレード通知に従ってアップグレードすると、これらのサポートされているアップグレードパスに続くリリースにアップグレードするように求められます。
- HTTPS の場所にアップグレードイメージを配置してアップグレードする場合は、サポートされているアップグレードパスに従ってください。
- 場合によっては、ターゲットリリースに到達するために数回アップグレードが必要になることがあります。

  たとえば、バージョン 9.8 を実行していて、 9.10.1 にアップグレードする場合は、まずバージョン 9.9.1 にアップグレードしてから 9.10.1 にアップグレードする必要があります。

- パッチ（P）リリースの場合は、あるバージョンリリースから次のバージョンの任意のPリリースにアップグレードできます。

  以下にいくつかの例を示します。

  - 9.13.0 > 9.13.1P15
  - 9.12.1 > 9.13.1P2

リバートまたはダウングレードする

Cloud Volumes ONTAP を以前のリリースにリバートまたはダウングレードすることはできません。

サポート登録

このページで説明されているいずれかの方法でソフトウェアをアップグレードするには、 Cloud Volumes ONTAP をネットアップサポートに登録する必要があります。PAYGO と BYOL の両方に該当します。必要なのは、です "PAYGO システムは手動で登録"、 BYOL システムはデフォルトで登録されます。

サポートに登録されていないシステムでも、新しいバージョンが利用可能になったときにBlueXPに表示されるソフトウェア更新通知を受け取ります。ただし、ソフトウェアをアップグレードする前に、システムを登録する必要があります。

HA メディエーターのアップグレード

また、Cloud Volumes ONTAP アップグレードプロセス中に必要に応じてメディエーターインスタンスも更新されます。

アップグレードを準備

アップ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、必要な設定の変更を行ってください。

- [ダウンタイムを計画]
- [自動ギブバックが有効になっていることを確認します]
- SnapMirror 転送を一時停止
- [アグリゲートがオンラインになっていることを確認する]

ダウンタイムを計画

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。

多くの場合、HAペアのアップグレードは無停止で実行され、I/Oが中断されることはありません。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。

セッション指向プロトコルは、アップグレードの実行中に特定領域のクライアントとアプリケーションに原因が悪影響を及ぼす可能性があります。詳細については、 "ONTAPのドキュメントを参照"

自動ギブバックが有効になっていることを確認します

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 転送を一時停止

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。

BlueXPのバックアップとリカバリではSnapMirrorを実装してバックアップファイル（SnapMirror Cloud）を作成しますが、システムのアップグレード時にバックアップを一時停止する必要はありません。

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. デスティネーションシステムから System Manager にログインします。

   System Manager にログインするには、 Web ブラウザでクラスタ管理 LIF の IP アドレスを指定します。IP アドレスは Cloud Volumes ONTAP の作業環境で確認できます。

   BlueXPにアクセスしているコンピュータには、Cloud Volumes ONTAP へのネットワーク接続が必要です。たとえば、クラウドプロバイダーネットワークにあるジャンプホストからBlueXPにログインする必要がある場合があります。

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になっていることを確認する

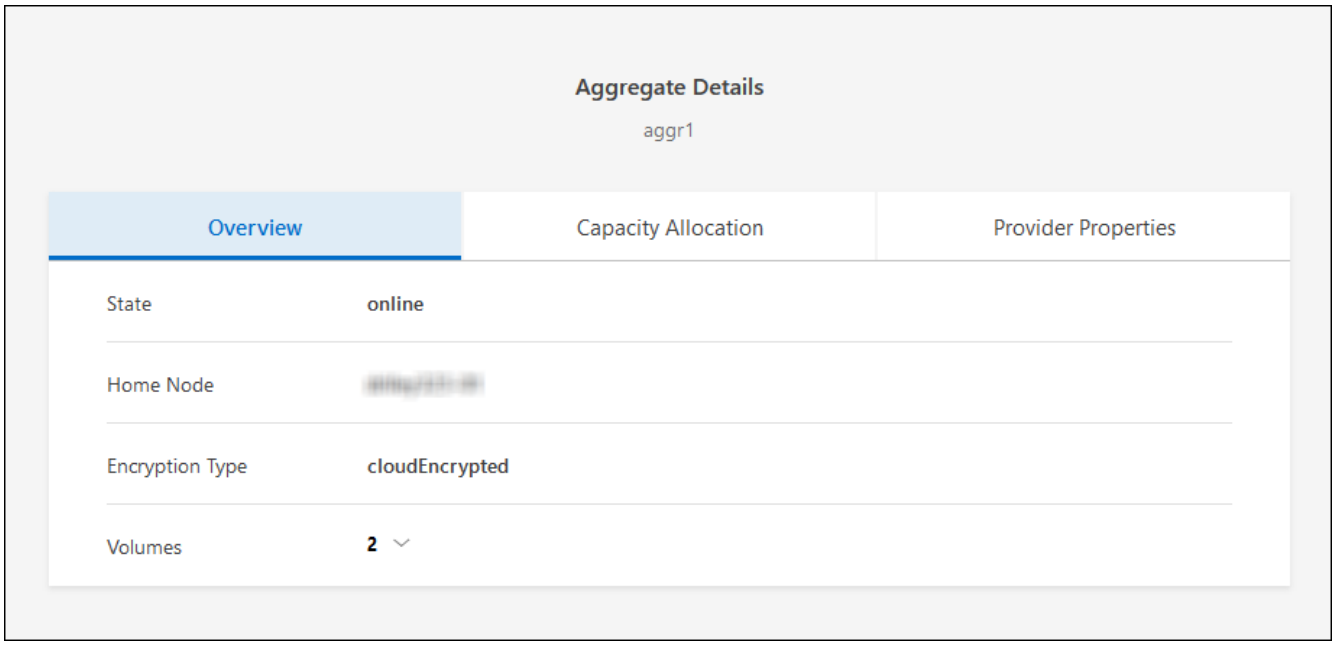
ソフトウェアを更新する前に、 Cloud Volumes ONTAP のアグリゲートがオンラインである必要があります。アグリゲートはほとんどの構成でオンラインになっている必要がありますが、オンラインになっていない場合はオンラインにしてください。

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、*[アグリゲート]*タブをクリックします。
2. アグリゲートのタイトルの下にある楕円ボタンをクリックし、*[アグリゲートの詳細の表示]*を選択します。



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. 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。
   b. 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 Volumes ONTAP をアップグレードします

新しいバージョンがアップグレード可能になると、BlueXPから通知が表示されます。この通知からアップグレードプロセスを開始できます。詳細については、を参照してください BlueXP通知からアップグレードします。

外部 URL 上のイメージを使用してソフトウェアのアップグレードを実行するもう 1 つの方法。このオプションは、BlueXP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や、パッチが提供されている場合に便利です。詳細については、を参照してください URL にあるイメージからアップグレードします。

BlueXP通知からアップグレードします

新しいバージョンのCloud Volumes ONTAP が使用可能になると、Cloud Volumes ONTAP の作業環境に通知が表示されます。

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。

作業を開始する前に

Cloud Volumes ONTAP システムでボリュームやアグリゲートの作成などのBlueXP処理を実行中でないことを確認してください。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. 作業環境を選択します。

   新しいバージョンが利用可能な場合は、[Overview]タブに通知が表示されます。

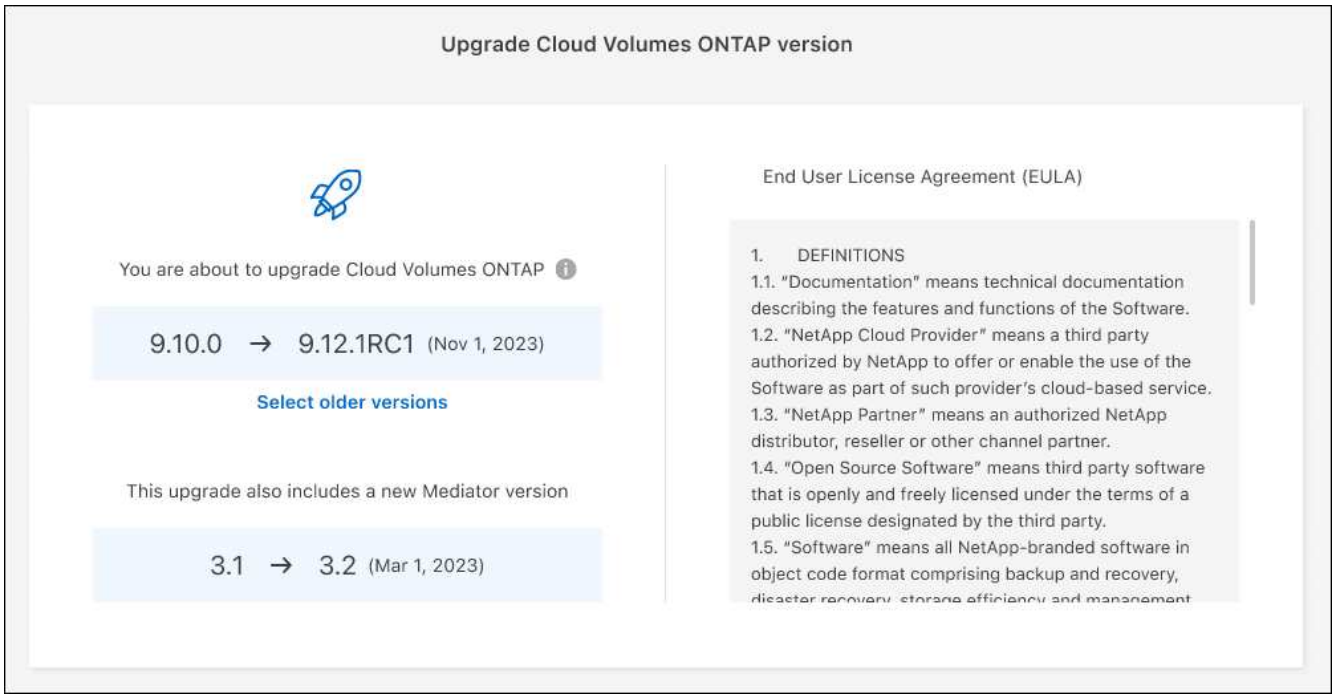
   タブの下のリンク。"]

3. 新しいバージョンが利用可能な場合は、*今すぐアップグレード！*をクリックします

   BlueXPの通知を通じてCloud Volumes ONTAPをアップグレードするには、NetApp Support Siteアカウントが必要です。

4. [Upgrade Cloud Volumes ONTAP （EULAのアップグレード）]ページで、EULAを読み、*[I read and approve the EULA]*を選択します。
5. [* アップグレード] をクリックします。

Upgrade Cloud Volumes ONTAPページでは、デフォルトでアップグレード可能な最新のCloud Volumes ONTAPバージョンが選択されます。可能な場合は、*[古いバージョンを選択]*をクリックして、以前のバージョンのCloud Volumes ONTAPをアップグレード対象として選択できます。
を参照してください "サポートされるアップグレードパスのリスト" をクリックし、Cloud Volumes ONTAPの現在のバージョンに基づいて適切なアップグレードパスを選択します。



ページのスクリーンショット。"]

6. アップグレードのステータスを確認するには、[設定]アイコンをクリックして*[タイムライン]*を選択します。

結果

BlueXP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、作業環境に対して操作を実行できます。

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。

URL にあるイメージからアップグレードします

Cloud Volumes ONTAP ソフトウェアイメージをコネクタまたはHTTPサーバに配置し、BlueXPからソフトウェアのアップグレードを開始できます。このオプションは、BlueXP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に使用できます。

作業を開始する前に

- Cloud Volumes ONTAP システムでボリュームやアグリゲートの作成などのBlueXP処理を実行中でないことを確認してください。
- ONTAP イメージのホストにHTTPSを使用する場合は、SSL認証の問題が原因でアップグレードが失敗する可能性がありますが、これは証明書がないことが原因です。回避策 は、ONTAP とBlueXP間の認証に使用するCA署名証明書を生成してインストールします。

手順を追った操作手順については、ネットアップのナレッジベースを参照してください。

"ネットアップの技術情報アーティクル：「How to configure BlueXP as an HTTPS server to host upgrade images"

手順

1. オプション： Cloud Volumes ONTAP ソフトウェアイメージをホストできる HTTP サーバを設定します。

   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 サーバにファイルを配置する必要があります。

2. Cloud Volumes ONTAP に独自のセキュリティグループを使用する場合は、アウトバウンドルールで HTTP 接続を許可し、 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てください。

   事前定義された Cloud Volumes ONTAP セキュリティグループは、デフォルトでアウトバウンド HTTP 接続を許可します。

3. からソフトウェアイメージを取得します "NetApp Support Site"。
4. ソフトウェアイメージを、ファイルの提供元となるコネクタまたは HTTP サーバ上のディレクトリにコピーします。

   2つのパスを使用できます。正しいパスはコネクタのバージョンによって異なります。

   - `/opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/`
   - `/opt/application/netapp/cloudmanager/ontap/images/`

5. BlueXPの作業環境で、をクリックします。 （楕円アイコン）*をクリックし、 Update Cloud Volumes ONTAP *をクリックします。
6. [Update Cloud Volumes ONTAP version]ページで、URLを入力し、*[Change Image]*をクリックします。

   上の図のパスにあるコネクタにソフトウェアイメージをコピーした場合は、次の URL を入力します。

   \http：//<Connector-private-IP-address><image-file-name>

   URLでは、* image-file-name *は「cot.image.9.13.1P2.tgz」の形式に従う必要があります。

7. [* Proceed](続行) をクリックして確定します

結果

BlueXP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。

Google Cloud NAT ゲートウェイを使用しているときのダウンロードエラーを修正します

コネクタは、 Cloud Volumes ONTAP のソフトウェアアップデートを自動的にダウンロードします。設定で Google Cloud NAT ゲートウェイを使用している場合、ダウンロードが失敗することがあります。この問題を修正するには、ソフトウェアイメージを分割するパーツの数を制限します。この手順は、BlueXP APIを使用して実行する必要があります。

ステップ

1. 次の JSON を本文として /occm/config に PUT 要求を送信します。

```
{
  "maxDownloadSessions": 32
}
```

maxDownloadSessions の値は 1 または 1 より大きい任意の整数です。値が 1 の場合、ダウンロードされたイメージは分割されません。

32 は値の例です。使用する値は、 NAT の設定と同時に使用できるセッションの数によって異なります。

"/occm/config API 呼び出しの詳細を確認してください"。

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 PAYGO システムに含まれていますが、最初にシステムをネットアップに登録してサポートをアクティブ化する必要があります。

アップグレードするには、ネットアップに PAYGO システムを登録する必要があります いずれかの方法を使用して ONTAP ソフトウェアをインストールします "このページで説明します"。

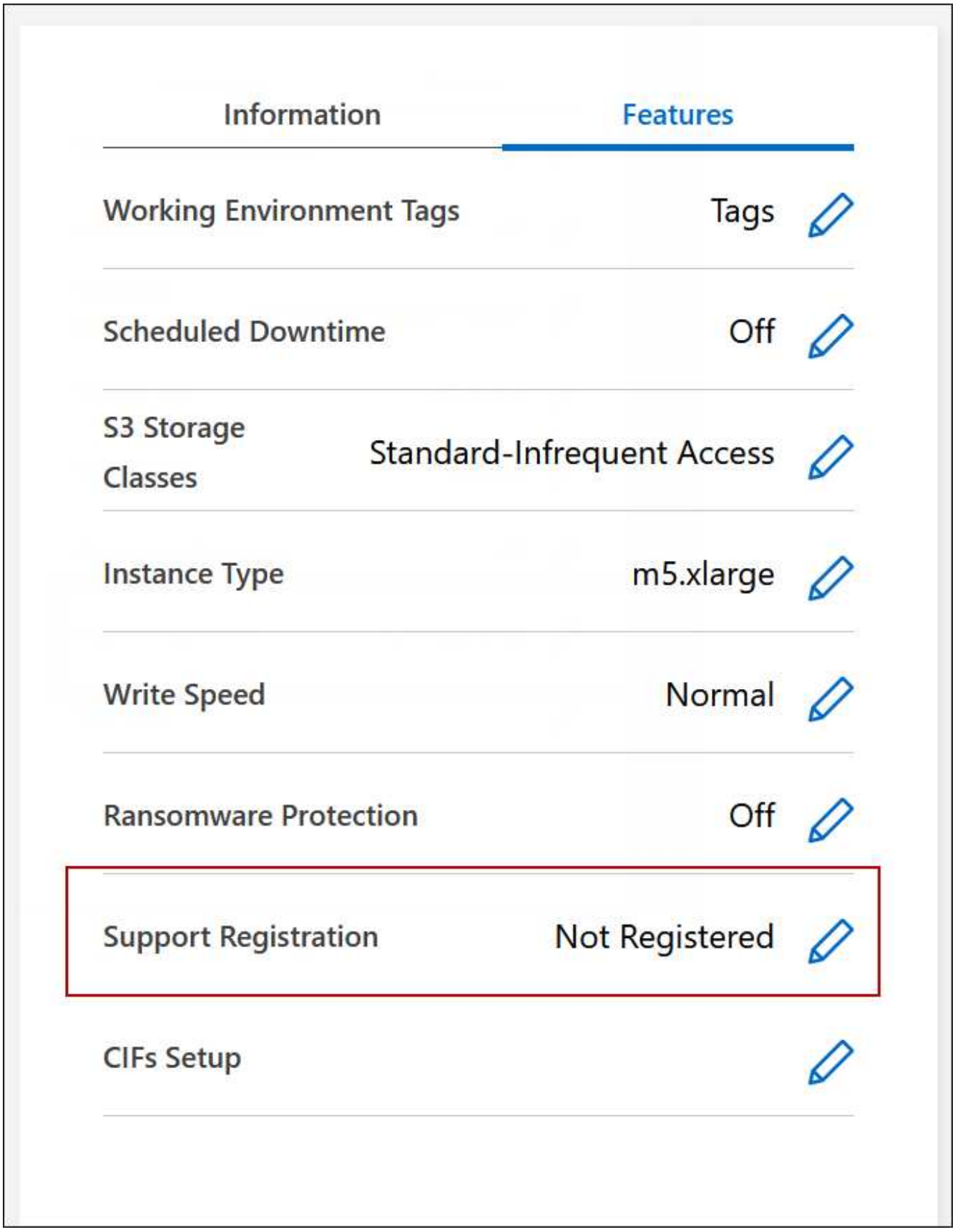
サポートに登録されていないシステムでも、新しいバージョンが利用可能になったときにBlueXPに表示されるソフトウェア更新通知を受け取ります。ただし、ソフトウェアをアップグレードする前に、システムを登録する必要があります。

手順

1. NetApp Support Site アカウントをBlueXPにまだ追加していない場合は、「アカウント設定」に移動して追加します。

   "NetApp Support Siteのアカウントを追加する方法について説明します"。

2. Canvas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. [概要]タブで、[機能]パネルをクリックし、*[サポート登録]*の横にある鉛筆アイコンをクリックします。



4. NetApp Support Siteのアカウントを選択し、 * 登録 * をクリックします。

結果

BlueXPを使用すると、システムがネットアップに登録されます。

Cloud Volumes ONTAP の状態の管理

Cloud Volumes ONTAP を停止してBlueXPから起動することで、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。この操作を手動で行う代わりに、システムを自動的にシャットダウンして特定の時刻に再起動するようにBlueXPを設定できます。

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場合、アクティブなデータ転送が進行中のときはシャットダウンを延期します。

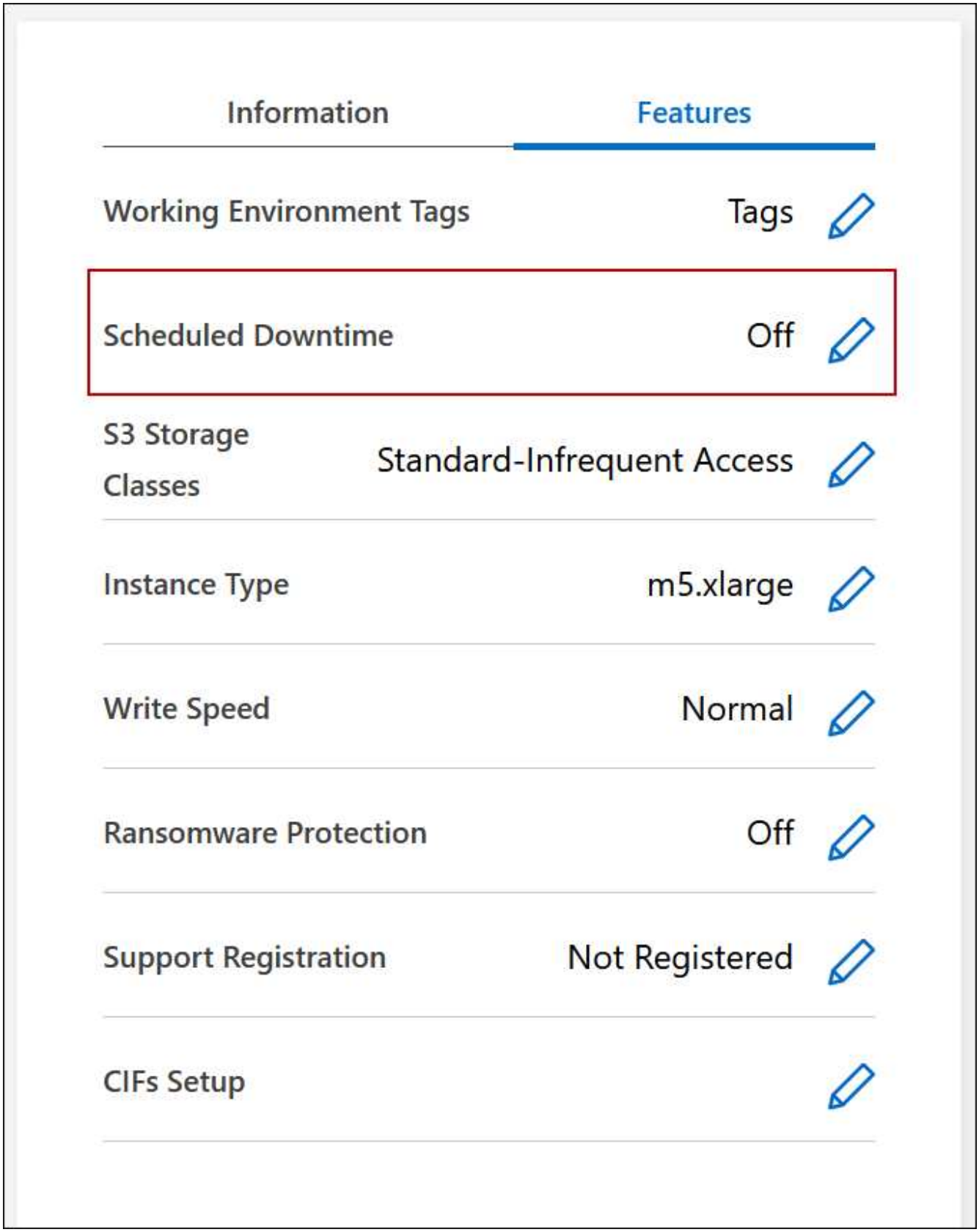
  転送が完了すると、BlueXPによってシステムがシャットダウンされます。

- 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。
- スケジュールされたシャットダウンによって Cloud Volumes ONTAP をオフにすると、ブートディスクとルートディスクのスナップショットは作成されません。

  スナップショットは、次のセクションで説明するように、手動シャットダウンを実行した場合にのみ自動的に作成されます。

手順

1. [Canvas]ページで、目的の作業環境をダブルクリックします。
2. [Overview]タブで、[Features]パネルをクリックし、* Scheduled downtime *の横にある鉛筆アイコンをクリックします。



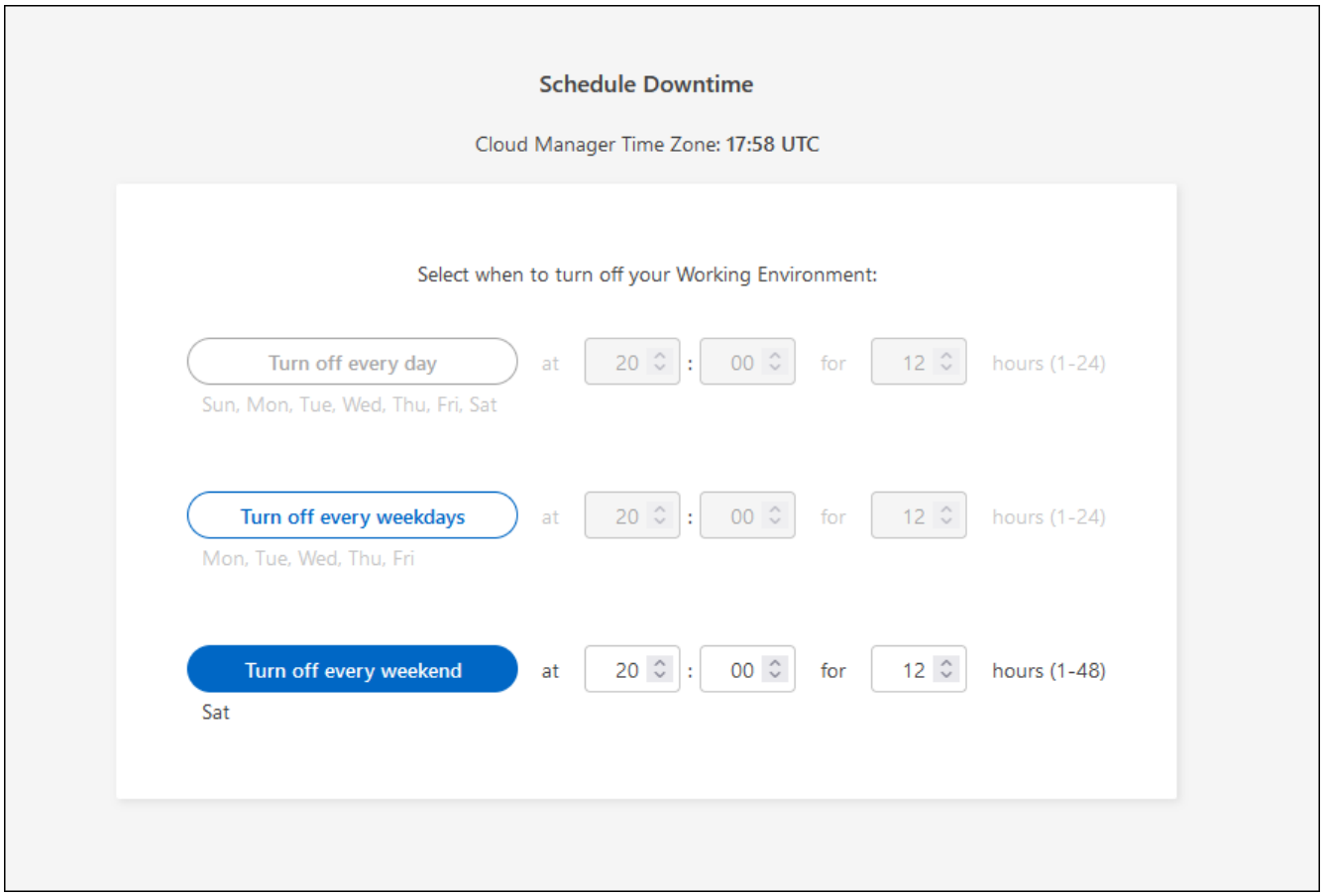
3. シャットダウンスケジュールを指定します。

   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、毎週土曜日の午後20時にシステムをシャットダウンするように設定したスケジュールを示しています（午後8時）12時間。BlueXPは毎週月曜日の午前0時にシステムを再起動します



画面を示しています。"]

4. [保存（ Save ）] をクリックします。

結果

スケジュールが保存されます。Features（機能）パネルの下の対応するScheduled downtime（スケジュールされたダウンタイム）行項目に「On（オン）」

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。

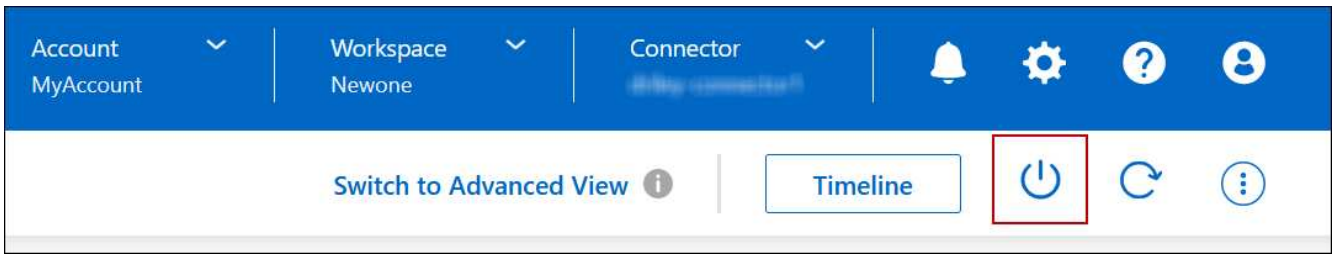
コストを削減するため、BlueXPは定期的にルートディスクと起動ディスクの古いスナップショットを削除します。ルートディスクとブートディスクの両方に対して、最新の 2 つの Snapshot のみが保持されます。

このタスクについて

HAペアを停止すると、BlueXP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。

   スナップショットは、リブート時に自動的に作成されます。

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。

を使用して NTP サーバを指定します "BlueXP API" または、ユーザインターフェイスからアクセスできます "CIFS サーバを作成"。

システムの書き込み速度を変更する

BlueXPを使用すると、Cloud Volumes ONTAP で通常の書き込み速度または高速の書き込み速度を選択できます。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。

高速の書き込み速度は、すべてのタイプのシングルノードシステムと一部のHAペア構成でサポートされています。でサポートされている構成を表示します "Cloud Volumes ONTAP リリースノート"

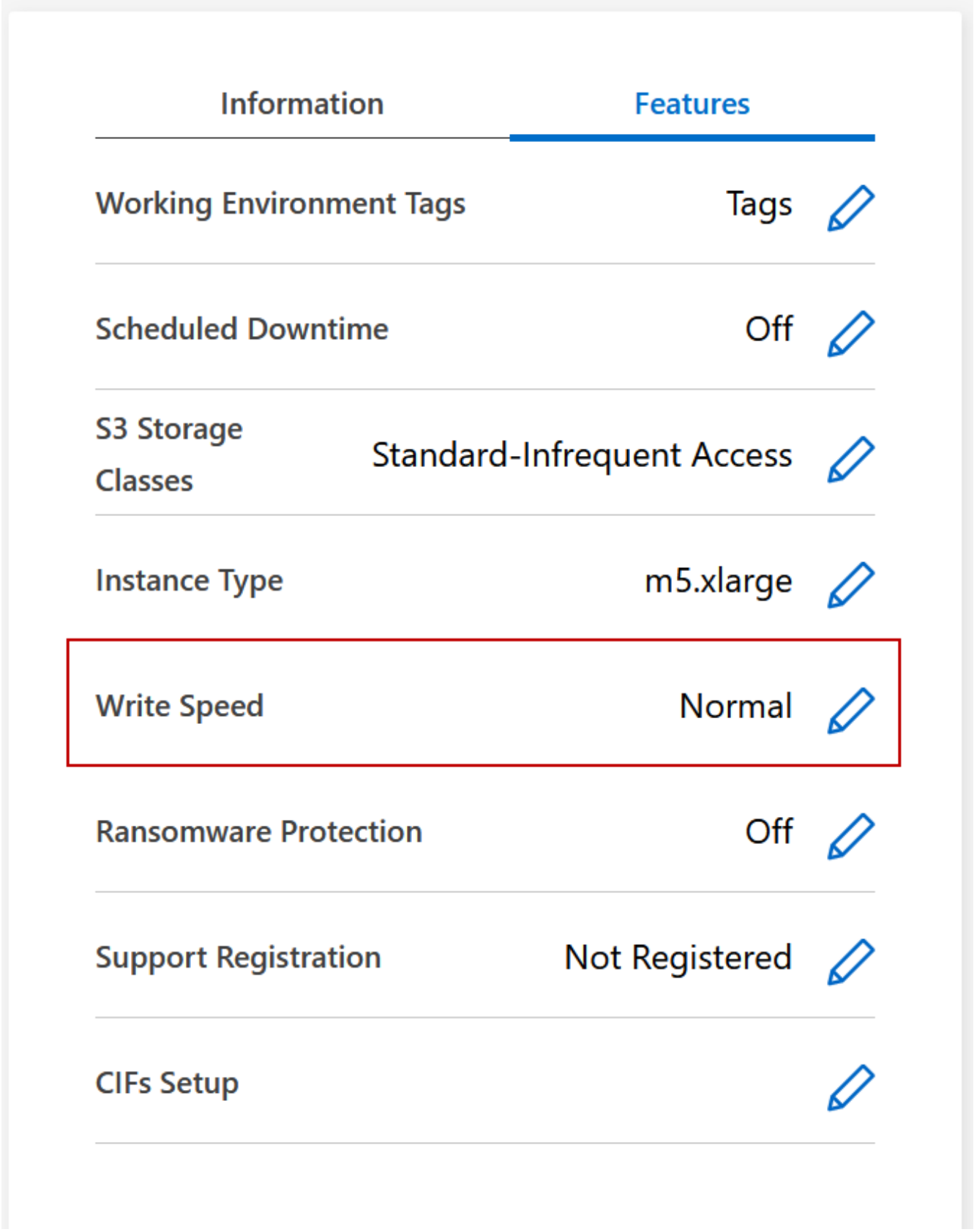
書き込み速度を変更する前に、次のことを確認してください "通常の設定と高い設定の違いを理解する"。

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 システムが再起動される点に注意してください。これはシステムの停止を伴うプロセスであり、システム全体のダウンタイムが必要となります。

手順

1. Canvasページで、書き込み速度に設定するシステムの名前をダブルクリックします。
2. [概要]タブで、[機能]パネルをクリックし、*[書き込み速度]*の横にある鉛筆アイコンをクリックします。



3. 「 * 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。

高速*書き込み速度オプションは、Google Cloudバージョン9.13.0以降のCloud Volumes ONTAP HAペアでサポートされます。

4. をクリックし、確認メッセージを確認して[承認]*をクリックします。

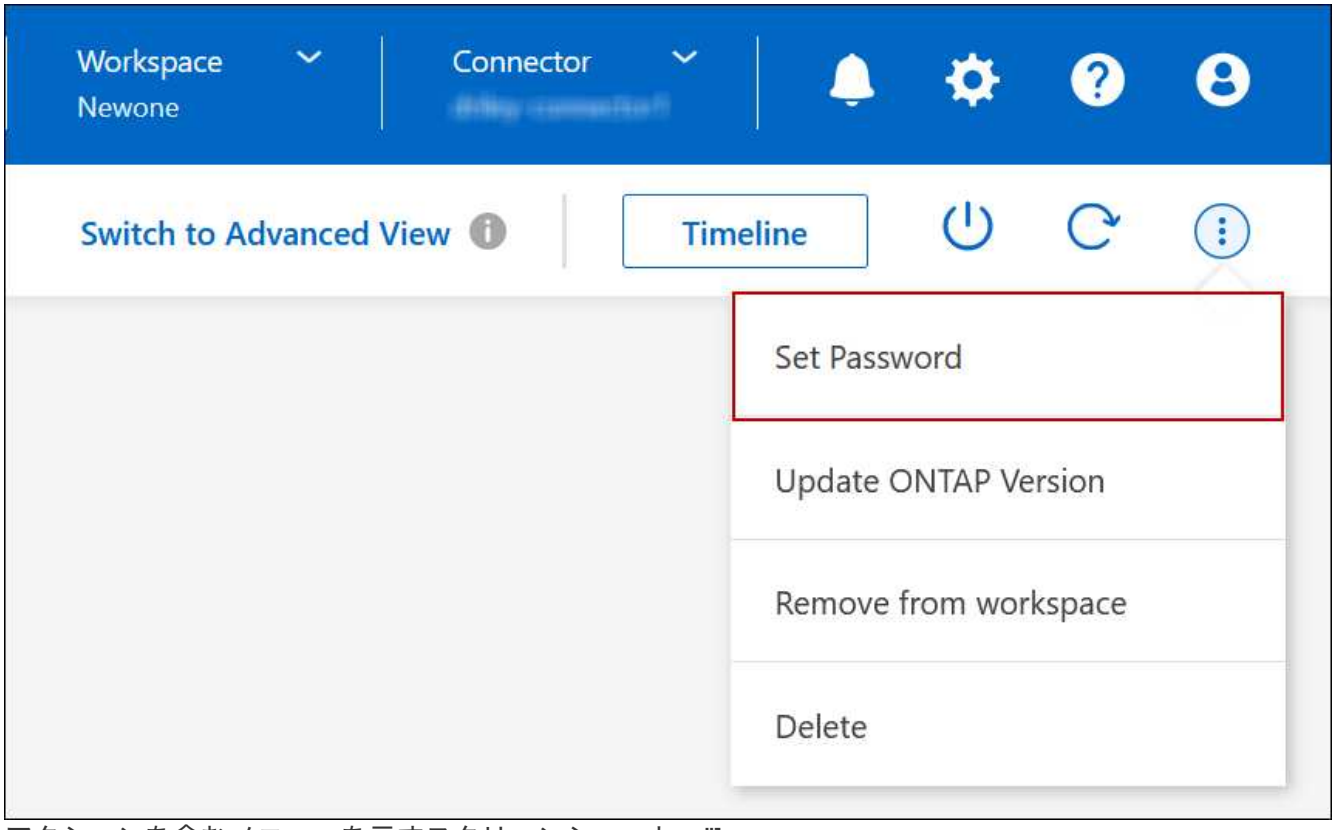
Cloud Volumes ONTAP のパスワードを変更します

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、このアカウントのパスワードをBlueXPから変更できます。

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BlueXPに反映されません。その結果、BlueXPはインスタンスを正しく監視できません。

手順

1. [Canvas]ページで、Cloud Volumes ONTAP 作業環境の名前をダブルクリックします。
2. BlueXPコンソールの右上にある楕円アイコンをクリックし、*[パスワードの設定]*を選択します。



アクションを含むメニューを示すスクリーンショット。"]

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。

システムを追加、削除、または削除します

既存の**Cloud Volumes ONTAP** システムを**BlueXP**に追加する

既存のCloud Volumes ONTAP システムを検出し、BlueXPに追加できます。これは、新しいBlueXPシステムを導入した場合に可能性があります。

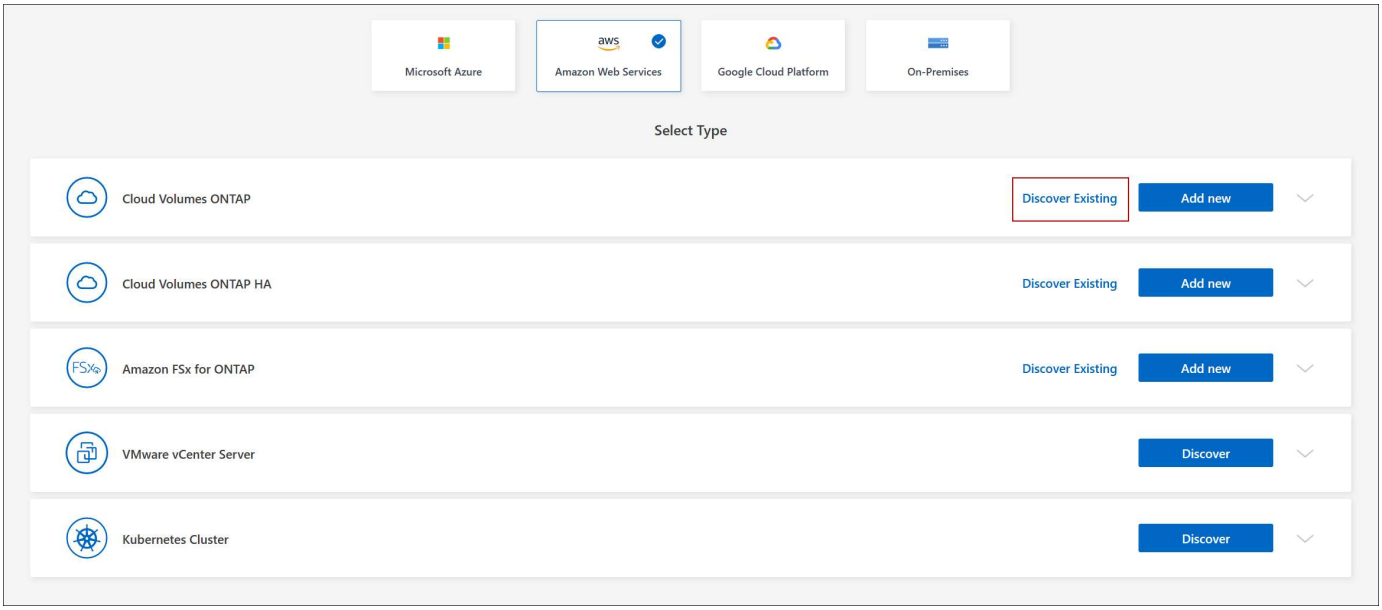
作業を開始する前に

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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、 * 作業環境の追加 * をクリックします。
3. 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。
4. Cloud Volumes ONTAP システムのタイプを選択します。
5. 既存のシステムを検出するには、リンクをクリックしてください。

[+]



1. [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。
2. [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 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 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 作業環境を削除すると'BlueXPから削除されますCloud Volumes ONTAP システムは削

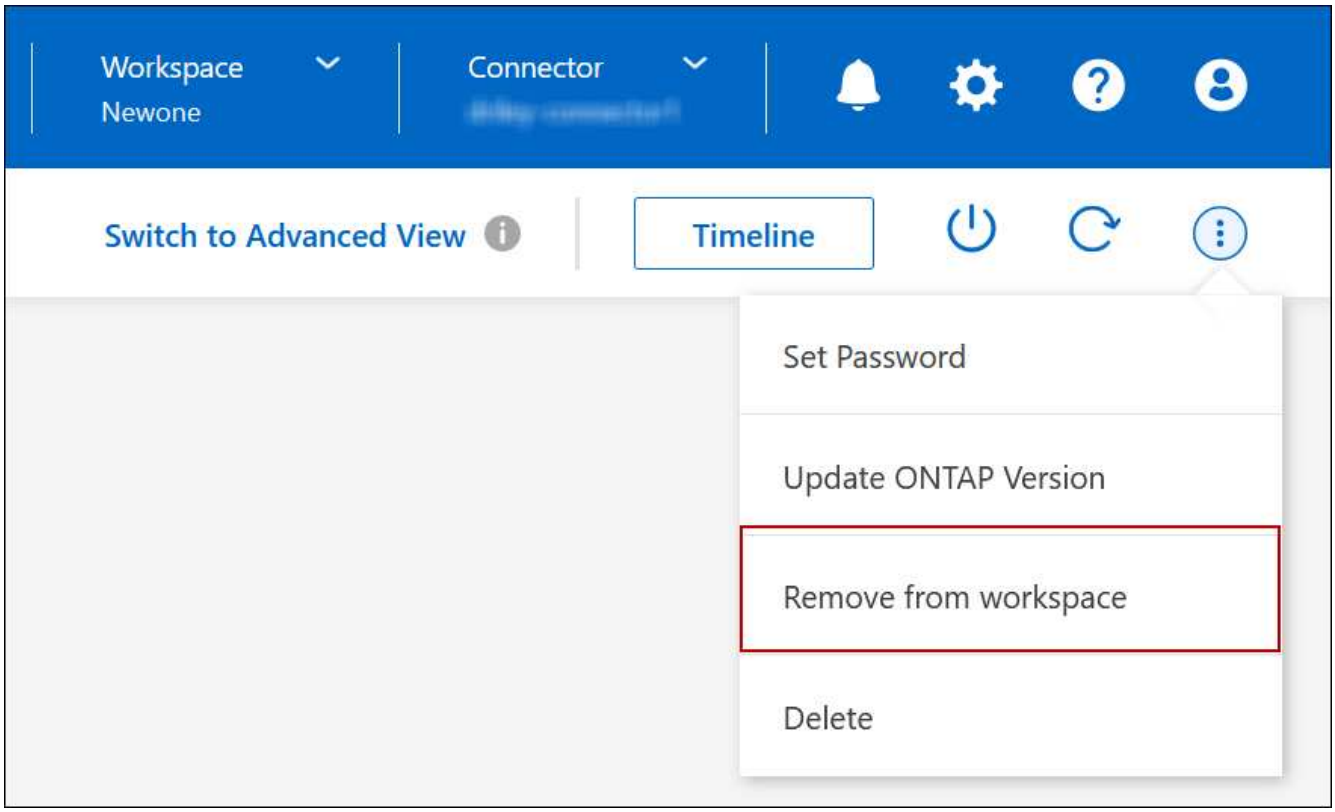
除されません。作業環境は後で再検出できます。

BlueXPから作業環境を削除すると'次の操作を実行できます

- 作業環境を別のワークスペースで再検出します
- 別のBlueXP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. [Canvas]ページで、削除する作業環境をダブルクリックします。
2. BlueXPコンソールの右上にある楕円アイコンをクリックし、*[ワークスペースから削除]*を選択します。



オプションを示すスクリーンショット。"]

3. [ワークスペースからのレビュー]ウィンドウで、*[削除]*をクリックします。

結果

BlueXPは作業環境を削除しますこの作業環境は、 Canvas ページからいつでも再検出できます。

Cloud Volumes ONTAP システムを削除する

クラウドプロバイダのコンソールからではなく、Cloud Volumes ONTAP システムを必ずBlueXPから削除してください。たとえば、クラウドプロバイダ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BlueXPから削除する必要があります。

作業環境を削除すると'BlueXPはCloud Volumes ONTAP 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

BlueXPのバックアップとリカバリのバックアップやBlueXP分類のインスタンスなど、他のサービスで管理されるリソースは、作業環境を削除しても削除されません。手動で削除する必要があります。そうしないと、これらのリソースの料金が引き続き請求されます。

クラウドプロバイダにCloud Volumes ONTAP を導入すると、BlueXPはインスタンスでの終端保護を有効にします。このオプションを使用すると、偶発的な終了を防止できます

手順

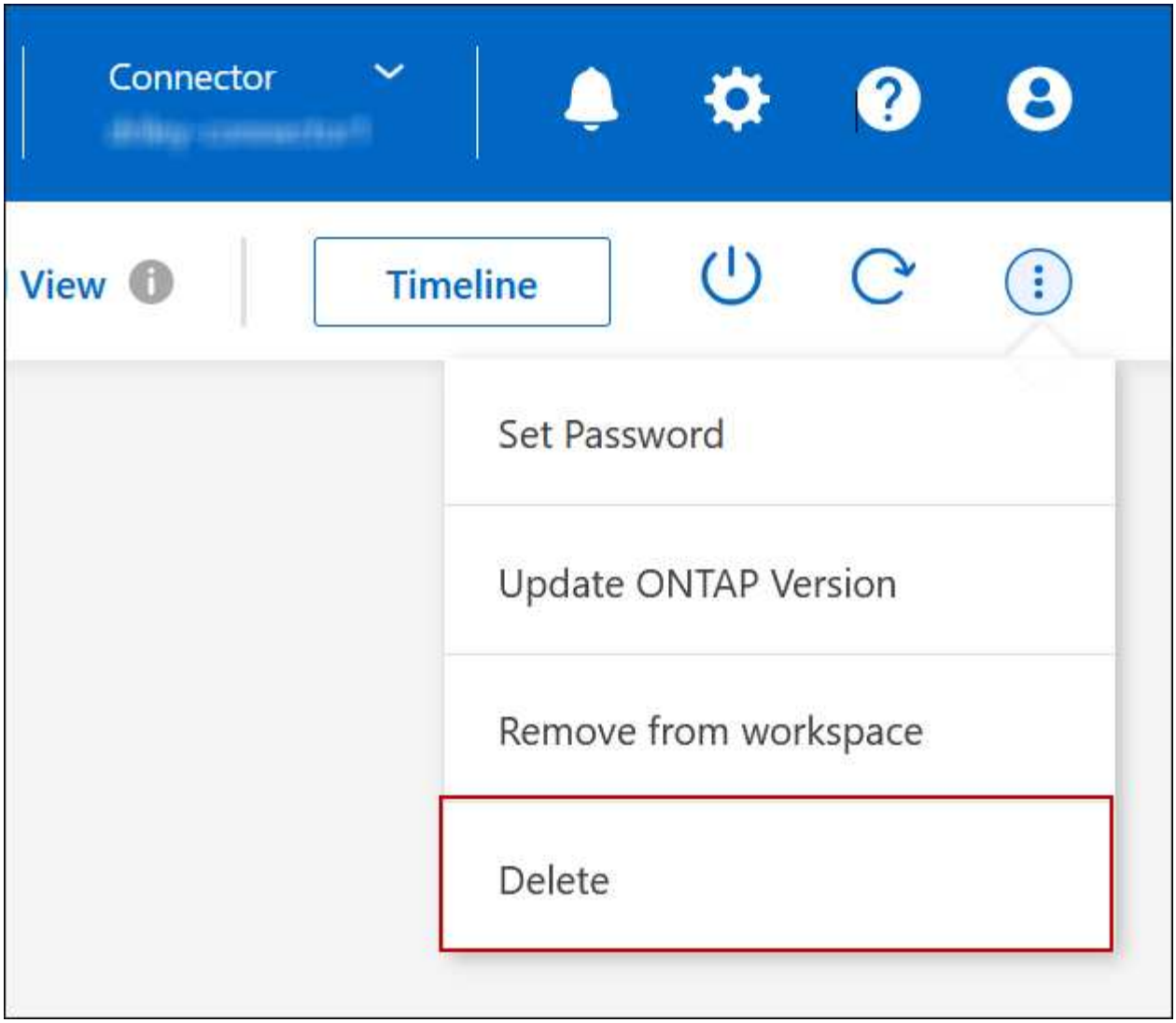
1. 作業環境でBlueXPのバックアップとリカバリを有効にした場合は、バックアップデータが引き続き必要かどうかを確認し、実行します "必要に応じて、バックアップを削除します"。

   BlueXPのバックアップとリカバリは、設計上Cloud Volumes ONTAP から独立しています。Cloud Volumes ONTAP システムを削除しても、BlueXPのバックアップとリカバリではバックアップが自動的に削除されません。また、システムの削除後にバックアップを削除する機能は現在UIでサポートされていません。

2. この作業環境でBlueXPの分類を有効にし、他の作業環境でこのサービスを使用していない場合は、サービスのインスタンスを削除する必要があります。

   "BlueXP分類インスタンスの詳細については、こちらをご覧ください"。

3. Cloud Volumes ONTAP 作業環境を削除します。
   a. キャンバスページで、削除する Cloud Volumes ONTAP 作業環境の名前をダブルクリックします。
   b. BlueXPコンソールの右上にある楕円アイコンをクリックし、*[削除]*を選択します。



c. [Delete Working Environment]ウィンドウで、作業環境の名前を入力し、*[Delete]*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。

AWSの管理

Cloud Volumes ONTAP の EC2 インスタンスタイプを変更します

AWS 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タイプから選択できます。インスタンスタイプは、ニーズに合わせ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にいつでも変更できます。

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"

- インスタンスタイプを変更すると、 AWS のサービス料金に影響する可能性があります。

- 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。

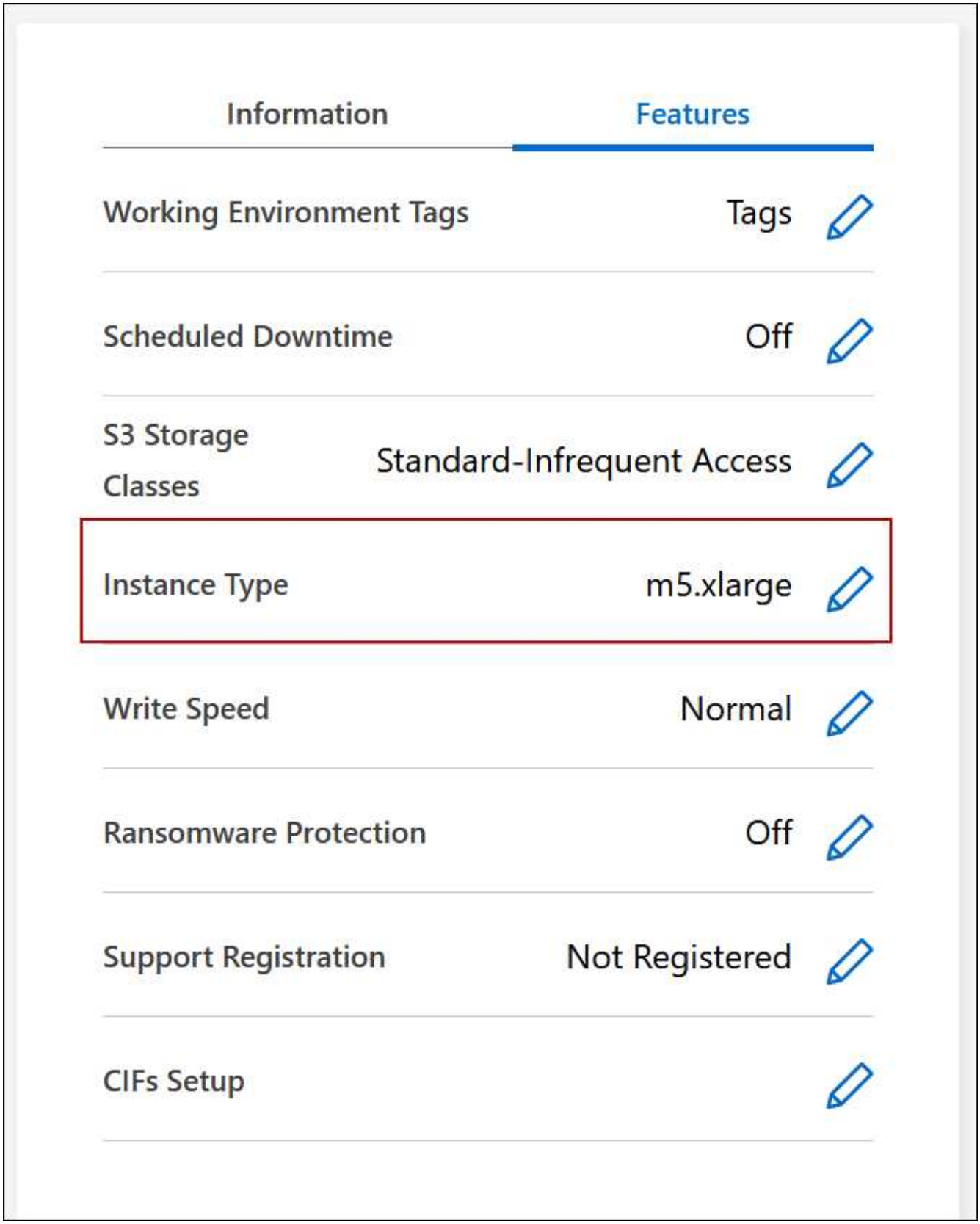
> テイクオーバーを開始してギブバックを待機することで、BlueXPは一度に1つのノードを正常に変更します。ネットアップの QA チームは、このプロセスでファイルの書き込みと読み取りの両方をテストしたため、クライアント側で問題は発生しませんでした。接続が変更されると、 I/O レベルでの再試行が表示されますが、アプリケーションレイヤはこれらの NFS / CIFS 接続の「再配線」の省略形を使用しています。

参照

AWSでサポートされるインスタンスタイプの一覧については、を参照してください "サポートされているEC2インスタンス"。

手順

1. [Canvas]ページで、作業環境を選択します。
2. [Overview]タブで、[Features]パネルをクリックし、*[Instance type]*の横にある鉛筆アイコンをクリックします。



a. ノードベースのPAYGOライセンスを使用している場合は、*[ライセンスタイプ]*の横にある鉛筆のアイコンをクリックして、別のライセンスとインスタンスタイプを選択することもできます。

3. インスタンスタイプを選択し、変更の影響を理解していることを確認するチェックボックスを選択して、*[変更]*をクリックします。

結果

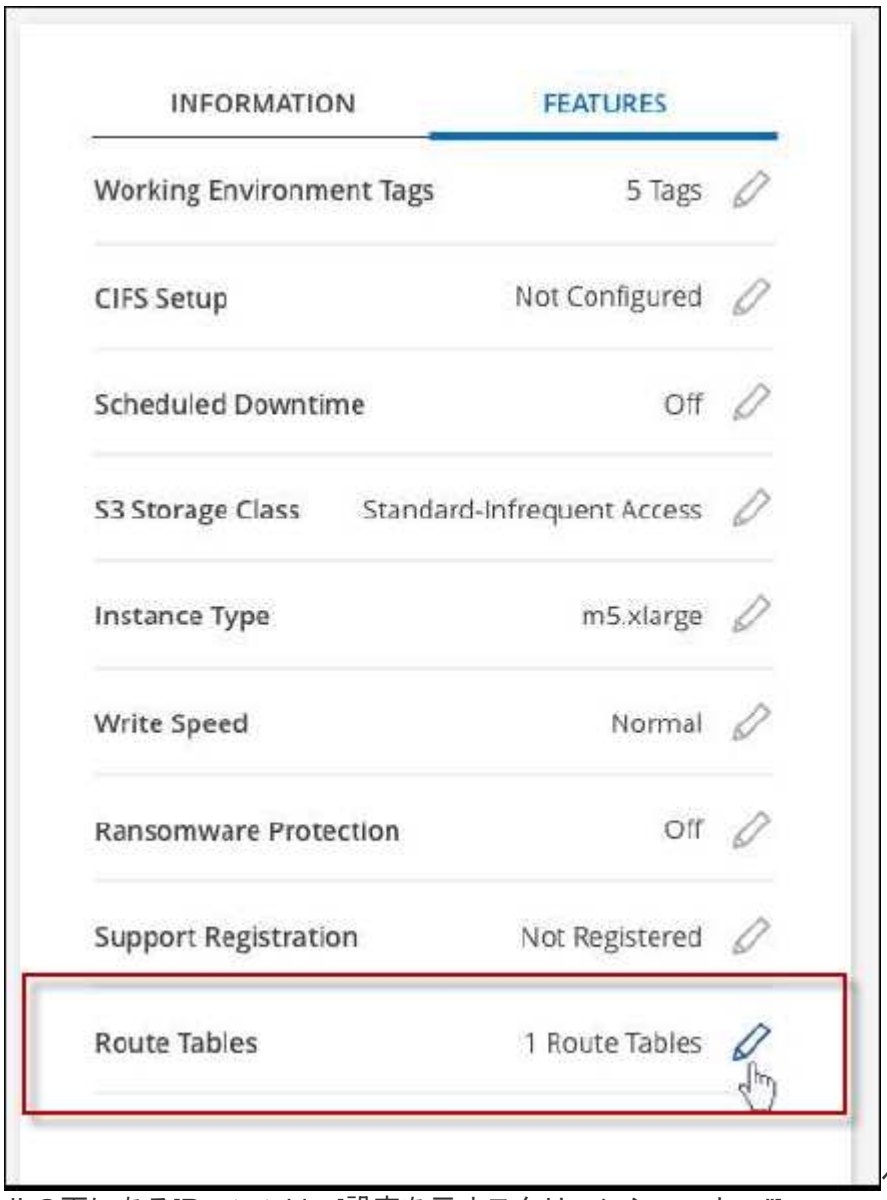
Cloud Volumes ONTAP が新しい設定でリブートします。

複数の **AZ** にまたがる **HA** ペア用のルーティングテーブルを変更します

複数の AWS アベイラビリティゾーン（ AZ ）に導入されている 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. [Canvas]ページで、作業環境を選択します。
2. [概要]タブで、[機能]パネルをクリックし、*[ルートテーブル]*の横にある鉛筆アイコンをクリックします。



ページの右上にある[Features]パネルの下にある[Route tables]設定を示すスクリーンショット。"]

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

BlueXPは、ルーティングテーブルを変更するAWS要求を送信します。

Azureの管理

Cloud Volumes ONTAP の Azure VM タイプを変更します

Microsoft Azure で Cloud Volumes ONTAP を起動する際には、いくつかの種類の VM を選択できます。ニーズに合わせ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 VM 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"

- VM タイプを変更すると、 Microsoft Azure のサービス料金に影響する可能性があります。
- Cloud Volumes ONTAP が再起動されます。

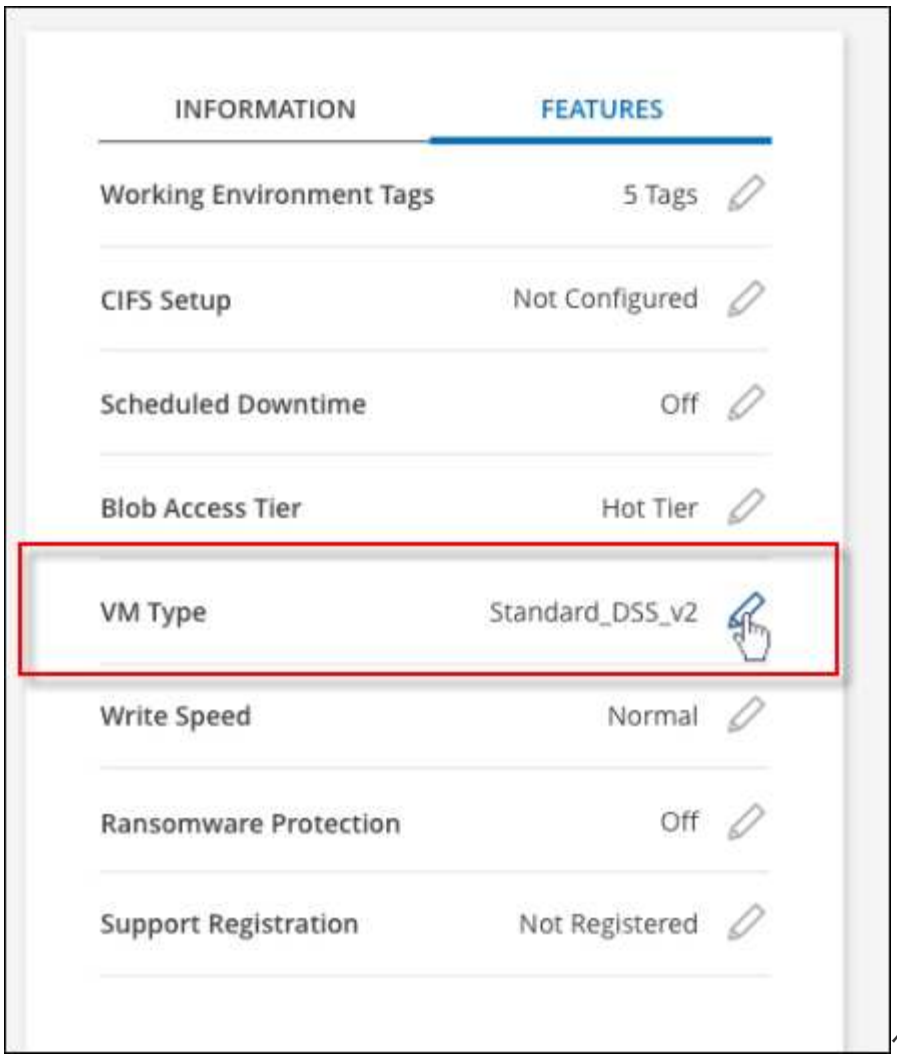
  シングルノードシステムの場合、 I/O は中断されます。

  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。

テイクオーバーを開始してギブバックを待機することで、BlueXPは一度に1つのノードを正常に変更します。ネットアップの QA チームは、このプロセスでファイルの書き込みと読み取りの両方をテストしたため、クライアント側で問題は発生しませんでした。接続が変更されると、 I/O レベルでの再試行が表示されますが、アプリケーションレイヤはこれらの NFS / CIFS 接続の「再配線」の省略形を使用しています。

手順

1. [Canvas]ページで、作業環境を選択します。
2. [Overview]タブで、[Features]パネルをクリックし、*[VM type]*の横にある鉛筆のアイコンをクリックします。



ページの右上にある[Features]パネルに表示されるVMタイプの設定を示すスクリーンショット。"]

a. ノードベースのPAYGOライセンスを使用している場合は、*[ライセンスタイプ]*の横にある鉛筆のアイコンをクリックして、別のライセンスとVMタイプを選択することもできます。

3. VMタイプを選択し、変更の影響を理解していることを確認するチェックボックスを選択し、*[変更]*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。

AzureのCloud Volumes ONTAP HAペアでのCIFSロックの無効化

アカウント管理者は、BlueXPの設定を有効にして、Azureメンテナンスイベント中のCloud Volumes ONTAP ストレージギブバックの問題を回避できます。この設定を有効にすると、 Cloud Volumes ONTAP は CIFS ロックを拒否し、アクティブな CIFS セッションをリセットします。

このタスクについて

Microsoft Azure では、仮想マシンに対して定期的なメンテナンスイベントをスケジュールします。Cloud Volumes ONTAP HA ペアでメンテナンスイベントが発生すると、 HA ペアでストレージのテイクオーバーが開始されます。このメンテナンスイベントの間にアクティブな CIFS セッションがあると、 CIFS ファイルが

ロックされてストレージのギブバックができなくなる可能性があります。

この設定を有効にすると、 Cloud Volumes ONTAP でロックが拒否され、アクティブな CIFS セッションがリセットされます。その結果、これらのメンテナンスイベントの間も HA ペアでストレージのギブバックが完了します。

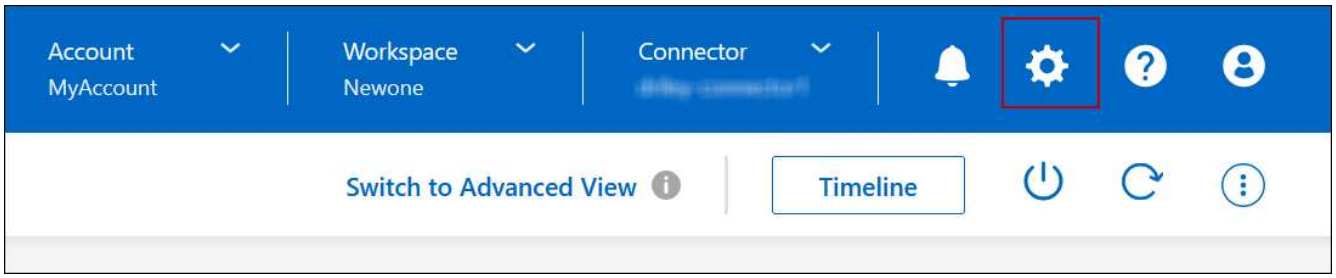
> このプロセスは、 CIFS クライアントの処理を中断する可能性があります。CIFS クライアントからコミットされていないデータは失われる可能性があります。

必要なもの

BlueXP設定を変更する前にコネクタを作成する必要があります。 "詳細をご確認ください"。

手順

1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[コネクタの設定]を選択します。



2. [* Azure*] で、 [* Azure CIFS locks for Azure HA working environments *] をクリックします。
3. チェックボックスをクリックして機能を有効にし、 * 保存 * をクリックします。

Azure Private Linkまたはサービスエンドポイントを使用する

Cloud Volumes ONTAP は、関連付けられたストレージアカウントへの接続にAzure Private Linkを使用します。必要に応じて、Azure Private Linkを無効にし、サービスエンドポイントを使用することができます。

概要

BlueXPでは、Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間の接続用にAzure Private Linkがデフォルトで有効になっています。Azure Private Linkは、Azureのエンドポイント間の接続を保護し、パフォーマンスを向上させます。

必要に応じて、Azureプライベートリンクの代わりにサービスエンドポイントを使用するようにCloud Volumes ONTAP を設定できます。

どちらの構成でも、BlueXPは常にCloud Volumes ONTAP とストレージアカウント間の接続に対するネットワークアクセスを制限します。ネットワークアクセスは、Cloud Volumes ONTAP が導入されているVNetおよびコネクタが導入されているVNetに限定されます。

代わりに**Azure Private Link**を無効にし、サービスエンドポイントを使用してください

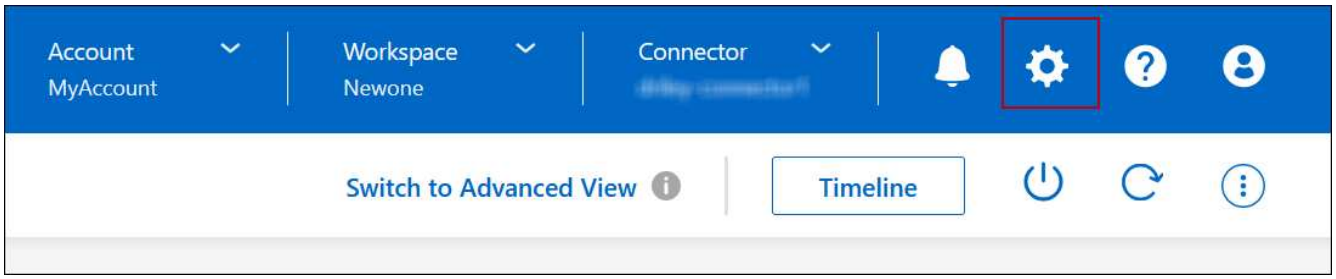
ビジネスで必要な場合は、BlueXPの設定を変更して、Azureプライベートリンクの代わりにサービスエンドポイントを使用するようにCloud Volumes ONTAP を設定できます。この設定を変更すると、新しく作成した環境 Cloud Volumes ONTAP システムに変更が適用されます。サービスエンドポイントは、でのみサポートされ

ます "Azureリージョンペア" コネクタとCloud Volumes ONTAP VNetの間。

コネクタは、管理対象の Cloud Volumes ONTAP システムまたはにある Azure リージョンと同じ Azure リージョンに導入する必要があります "Azure リージョンペア" Cloud Volumes ONTAP システム用。

手順

1. BlueXPコンソールの右上にある[設定]アイコンをクリックし、[コネクタの設定]を選択します。



2. [**Azure**] で、 [* Azure プライベートリンクを使用する *] をクリックします。
3. Cloud Volumes ONTAP とストレージアカウント間のプライベートリンク接続 * の選択を解除します。
4. [保存（ Save ）] をクリックします。

完了後

Azure Private Linksを無効にし、コネクタがプロキシサーバーを使用している場合は、ダイレクトAPIトラフィックを有効にする必要があります。

"コネクタで直接APIトラフィックを有効にする方法について説明します"

Azureプライベートリンクを使用する

ほとんどの場合、Cloud Volumes ONTAP でAzureプライベートリンクを設定するために必要な作業はありません。BlueXPはAzureプライベートリンクを管理しています。ただし、既存のAzureプライベートDNSゾーンを使用する場合は、構成ファイルを編集する必要があります。

カスタム**DNS**の要件

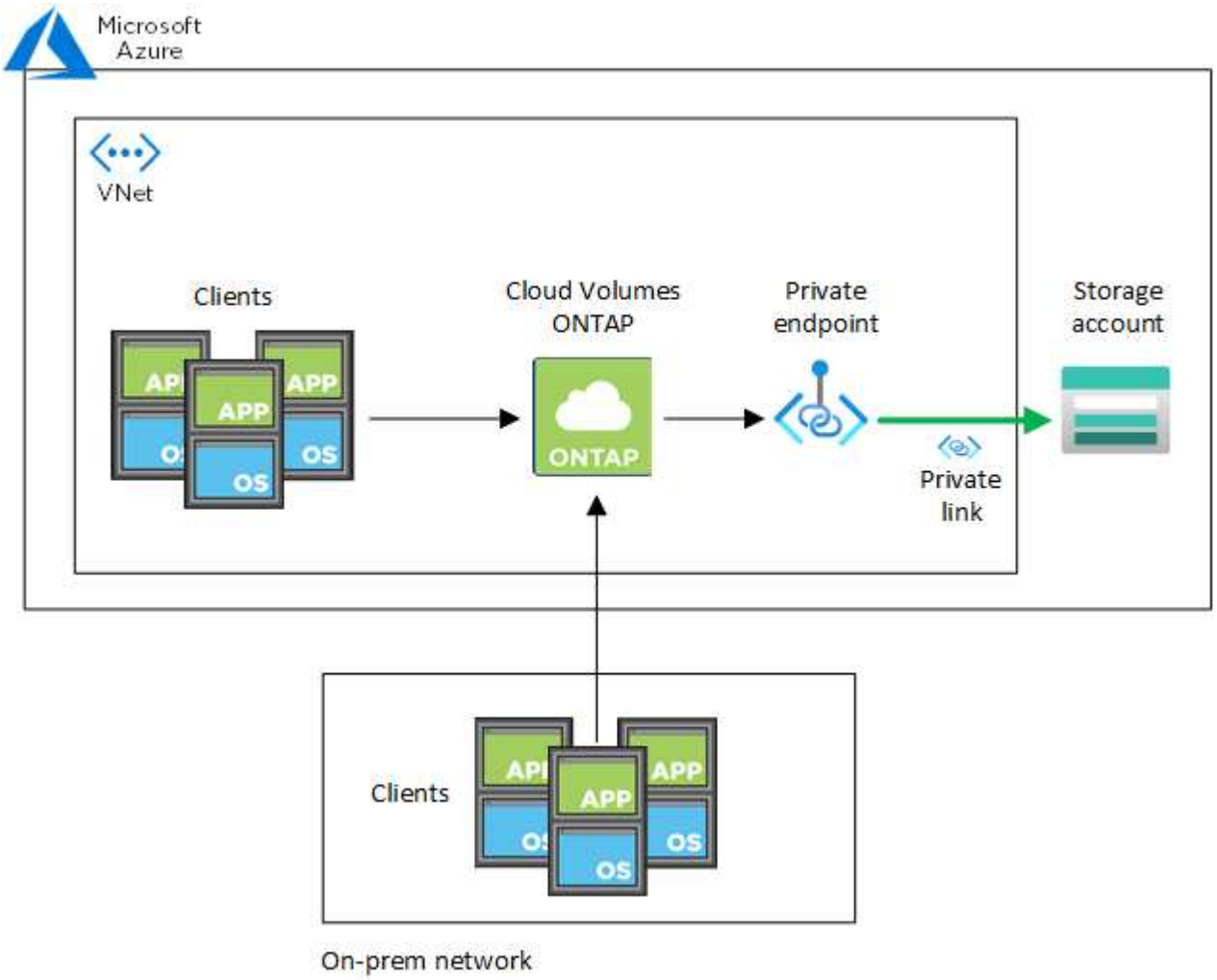
必要に応じて、カスタムDNSを使用する場合は、カスタムDNSサーバからAzureプライベートDNSゾーンに対する条件付きフォワーダを作成する必要があります。詳細については、を参照してください "DNSフォワーダを使用するAzureのドキュメント"。

プライベートリンク接続の仕組み

BlueXPがAzureにCloud Volumes ONTAP を導入すると、リソースグループにプライベートエンドポイントが作成されます。プライベートエンドポイントは、Cloud Volumes ONTAP のストレージアカウントに関連付けられます。その結果、 Cloud Volumes ONTAP ストレージへのアクセスは、 Microsoft バックボーンネットワークを経由します。

VNet へのプライベート VPN 接続または ExpressRoute 接続を使用する場合、クライアントが Cloud Volumes ONTAP と同じ VNet 内、ピア VNet 内、またはオンプレミスネットワーク内にある場合、クライアントアクセスはプライベートリンクを経由します。

次の例は、同じ VNet 内およびプライベート VPN 接続または ExpressRoute 接続が確立されたオンプレミスネットワークから、プライベートリンクを介したクライアントアクセスを示しています。



コネクタシステムとCloud Volumes ONTAP システムが異なるVNetに導入されている場合は、コネクタが導入されているVNetとCloud Volumes ONTAP システムが導入されているVNet間にVNetピアリングを設定する必要があります。

Azureプライベート**DNS**の詳細を**BlueXP**に提供します

を使用する場合 "Azure プライベート DNS"では、各コネクタの構成ファイルを変更する必要があります。それ以外の場合、Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間のAzure Private Link 接続を有効にすることはできません。

DNS 名は Azure DNS の命名規則と一致している必要があります 要件 "Azure のドキュメントを参照"。

手順

1. コネクタホストに SSH 接続してログインします。
2. 次のディレクトリに移動します。 /opt/application/NetApp/cloudmanager/docx_occm/data
3. 「user-private-dns-zone-settings」パラメータに次のキーワードと値のペアを追加して、app.confを編集します。

```
"user-private-dns-zone-settings" : {
   "resource-group" : "<resource group name of the DNS zone>",
   "subscription" : "<subscription ID>",
   "use-existing" : true,
   "create-private-dns-zone-link" : true
}
```

パラメータは、「system-id」と同じレベルで入力する必要があります。

```
"system-id" : "<system ID>",
"user-private-dns-zone-settings" : {
```

subscriptionKeywordは、プライベートDNSゾーンがコネクタとは異なるサブスクリプションに存在する場合にのみ必要です。

4. ファイルを保存し、コネクタからログオフします。

   再起動は必要ありません。

障害発生時のロールバックを有効にする

BlueXPが特定のアクションの一部としてAzure Private Linkを作成できない場合、Azure Private Link接続なしで処理を完了します。このエラーは、新しい作業環境（シングルノードまたは HA ペア）の作成時、または HA ペアで次の操作が行われた場合に発生します。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、 32TiB を超える場合の新しいストレージアカウントの作成。

このデフォルトの動作は、BlueXPでAzure Private Linkの作成に失敗した場合にロールバックを有効にすることで変更できます。これにより、企業のセキュリティ規制を完全に遵守することができます。

ロールバックを有効にすると、アクションが停止し、アクションの一部として作成されたすべてのリソースがロールバックされます。

ロールバックは、APIまたはapp.confファイルを更新することで有効にできます。

- APIを使用したロールバックを有効にします。*

ステップ

1. を使用します `PUT /occm/config` 次の要求本文を指定したAPI呼び出し：

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

   ◦ app.confを更新してロールバックを有効にします*

手順

1. コネクタホストに SSH 接続してログインします。

2. 次のディレクトリに移動します。 /opt/application/NetApp/cloudmanager/docx_occm/data
3. 次のパラメータと値を追加してapp.confを編集します。

```
 "rollback-on-private-link-failure": true
. ファイルを保存し、コネクタからログオフします。
```

再起動は必要ありません。

リソースグループを移動しています

Cloud Volumes ONTAP ではAzureリソースグループの移動がサポートされていますが、ワークフローはAzureコンソールでのみ実行されます。

同じAzureサブスクリプション内で、あるリソースグループからAzure内の別のリソースグループに作業環境を移動することができます。異なるAzureサブスクリプション間でのリソースグループの移動はサポートされていません。

手順

1. 作業環境を* Canvas *から削除します。

   作業環境を削除する方法については、を参照してください "Cloud Volumes ONTAP の動作環境を削除しています"。

2. Azureコンソールでリソースグループ移動を実行する。

   移動を完了するには、を参照してください "Microsoft Azureのドキュメントで、リソースを新しいリソースグループまたはサブスクリプションに移動する"。

3. Canvas *で、作業環境を確認します。
4. 作業環境の情報で新しいリソースグループを探します。

結果

新しいリソースグループには、作業環境とそのリソース（VM、ディスク、ストレージアカウント、ネットワークインターフェイス、Snapshot）が含まれます。

Google Cloudの管理

Cloud Volumes ONTAP の Google Cloud マシンタイプを変更します

Google Cloud で Cloud Volumes ONTAP を起動する際には、複数のマシン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"

- マシンタイプを変更すると、 Google Cloud サービス料金に影響する可能性があります。
- Cloud Volumes ONTAP が再起動されます。

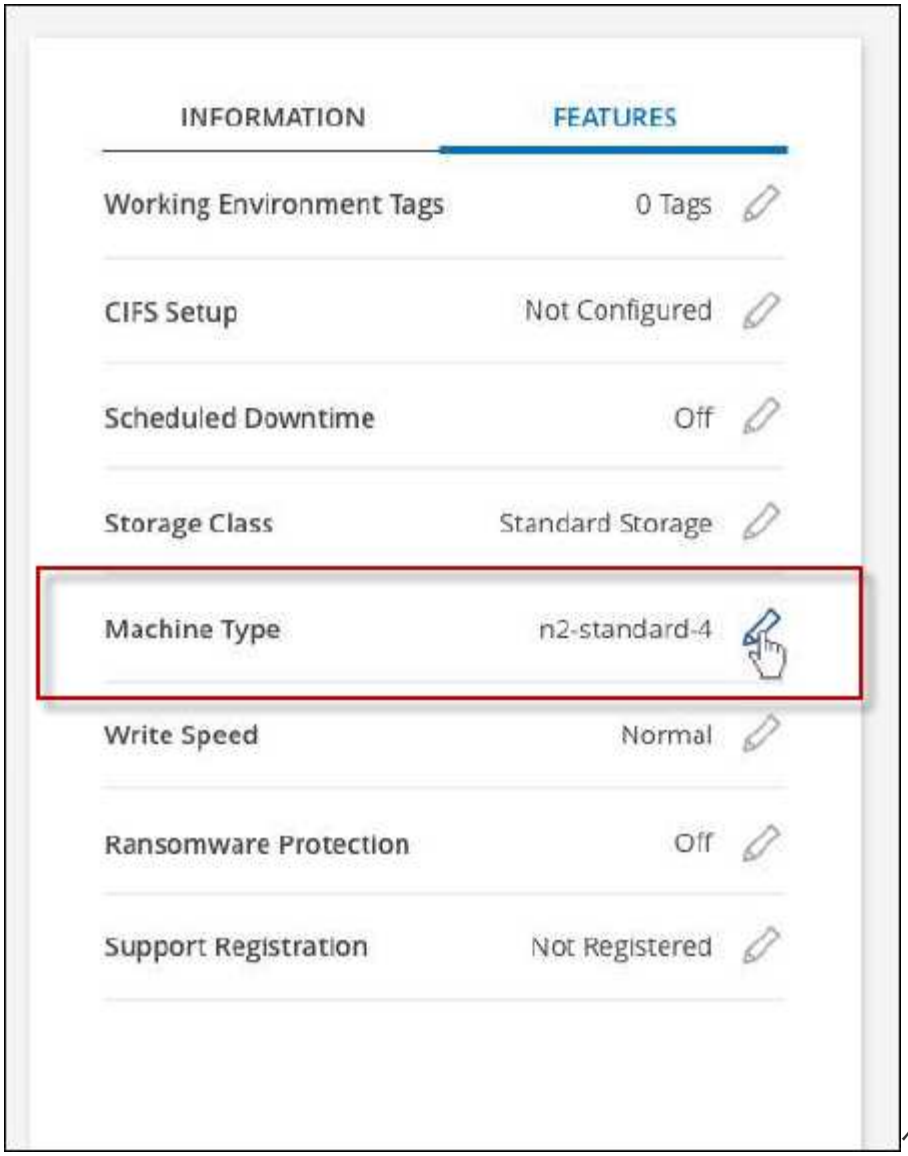
  シングルノードシステムの場合、 I/O は中断されます。

  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。

テイクオーバーを開始してギブバックを待機することで、BlueXPは一度に1つのノードを正常に変更します。ネットアップの QA チームは、このプロセスでファイルの書き込みと読み取りの両方をテストしたため、クライアント側で問題は発生しませんでした。接続が変更されると、 I/O レベルでの再試行が表示されますが、アプリケーションレイヤはこれらの NFS / CIFS 接続の「再配線」の省略形を使用しています。

手順

1. [Canvas]ページで、作業環境を選択します。
2. [概要]タブで、[機能]パネルをクリックし、*[マシンタイプ]*の横にある鉛筆アイコンをクリックします。



ページの右上にある[Features]パネルの下にある[Machine type]設定を示すスクリーンショット。"]

a. ノードベースのPAYGOライセンスを使用している場合は、*[ライセンスタイプ]*の横にある鉛筆のアイコンをクリックして、別のライセンスとマシンタイプを選択することもできます。

3. 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、*[変更]*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。

拡張ビューを使用して**Cloud Volumes ONTAP** を管理します

Cloud Volumes ONTAP の高度な管理が必要な場合は、ONTAP システムに付属の管理インターフェイスであるONTAP System Managerを使用して実行できます。BlueXPにはSystem Managerインターフェイスが搭載されているので、高度な管理のためにBlueXPを残す必要はありません。

この拡張ビューはプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化

する予定です。製品内のチャットでご意見をお寄せください。

機能

BlueXPの詳細ビューでは、次の管理機能を使用できます。

- 高度なストレージ管理

  整合グループ、共有、qtree、クォータ、およびStorage VMの管理

- ネットワーク管理

  IPspace、ネットワークインターフェイス、ポートセット、およびイーサネットポートを管理します。

- イベントとジョブ

  イベントログ、システムアラート、ジョブ、および監査ログを表示します。

- 高度なデータ保護

  Storage VM、LUN、および整合グループを保護する。

- ホスト管理

  SANイニシエータグループとNFSクライアントを設定します。

サポートされている構成

System Managerを使用した高度な管理は、標準のクラウドリージョンでCloud Volumes ONTAP 9.10.0以降でサポートされます。

GovCloudリージョンまたはアウトバウンドのインターネットアクセスがないリージョンでは、System Managerの統合はサポートされません。

制限

System Managerインターフェイスに表示されるいくつかの機能は、Cloud Volumes ONTAP ではサポートされません。

- BlueXPの階層化

  Cloud Volumes ONTAP では、BlueXP階層化サービスはサポートされていません。ボリュームを作成するときは、BlueXPの標準ビューからデータをオブジェクトストレージに階層化するように直接設定する必要があります。

- 階層

  アグリゲートの管理（ローカル階層とクラウド階層を含む）はSystem Managerではサポートされていません。アグリゲートは、BlueXPのStandard Viewから直接管理する必要があります。

- ファームウェアのアップグレード

Cloud Volumes ONTAP では、[クラスタ]>[設定*]ページからの自動ファームウェア更新はサポートされていません。

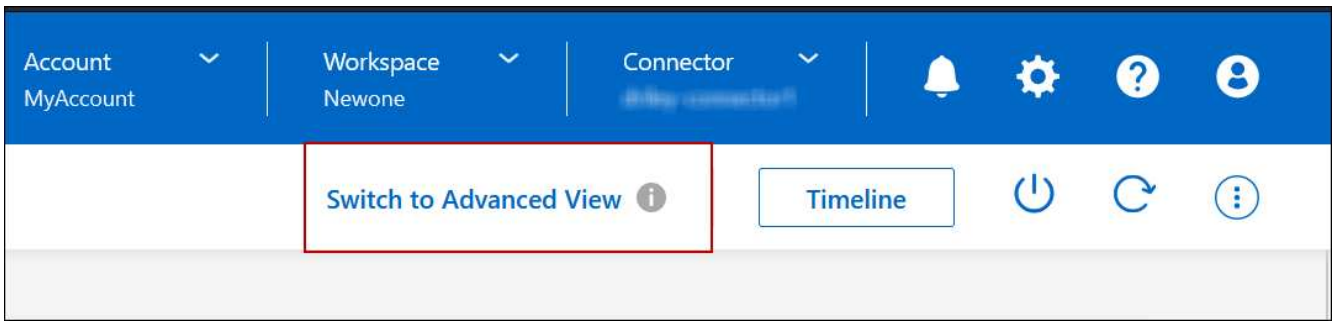
また、System Managerからのロールベースアクセス制御はサポートされていません。

開始方法

Cloud Volumes ONTAP 作業環境を開き、詳細ビューオプションをクリックします。

手順

1. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
2. キャンバスページで、Cloud Volumes ONTAP システムの名前をダブルクリックします。
3. 右上の*[拡張表示に切り替える]をクリックします。



4. 確認メッセージが表示されたら、そのメッセージを読み、*閉じる*をクリックします。
5. System Managerを使用してCloud Volumes ONTAP を管理する。
6. 必要に応じて、[標準表示に切り替える]をクリックして、BlueXPを使用した標準管理に戻ります。

System Managerの使用方法に関するヘルプ

Cloud Volumes ONTAP でSystem Managerを使用する際にサポートが必要な場合は、を参照してください "ONTAP のドキュメント" を参照してください。役立つリンクをいくつか紹介します。

- "ボリュームとLUNの管理"
- "Network Management の略"
- "データ保護"

CLIからCloud Volumes ONTAP を管理します

Cloud Volumes ONTAP CLI では、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 を使い慣れている場合は、 CLI の使用を推奨します。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、クラウドプロバイダネットワーク内のジャンプホストからSSHを使用する場合などです。

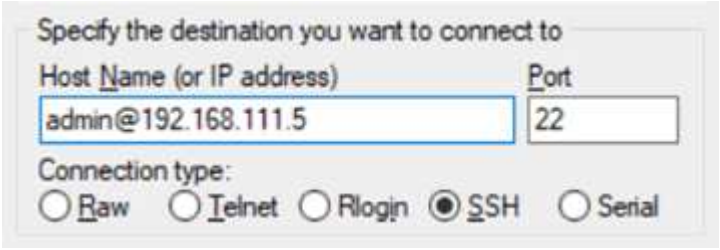
複数の AZS に導入されている場合、 Cloud Volumes ONTAP HA 構成では、クラスタ管理インターフェイスにフローティング IP アドレスが使用されます。これは、外部ルーティングが使用できないことを意味します。同じルーティングドメインの一部であるホストから接続する必要があります。

手順

1. BlueXP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. 左側のナビゲーションメニューから、* Storage > Canvas *を選択します。
   b. キャンバスページで、 Cloud Volumes ONTAP システムを選択します。
   c. 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::>
```

システムの健全性とイベント

AutoSupport のセットアップを確認します

AutoSupport は、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。デフォルトでは、各ノードで AutoSupport が有効になっており、 HTTPS 転送プロトコルを使用してテクニカルサポートにメッセージを送信できます。AutoSupport がこれらのメッセージを送信できることを確認することをお勧めします。

必要な設定手順は、 Cloud Volumes ONTAP がアウトバウンドインターネットに接続されていることを確認することだけです。詳細については、クラウドプロバイダのネットワーク要件を参照してください。

AutoSupport の要件

Cloud Volumes ONTAP ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健常性をプロアクティブに監視し、ネットアップテクニカルサポートにメッセージを送信します。

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

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するように設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で_ inbound_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で_OUTBOUND接続を許可する必要もあります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、 AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください "ONTAP のドキュメント：「 AutoSupport のセットアップ"。

AutoSupport 構成のトラブルシューティングを行います

アウトバウンド接続が使用できず、BlueXPがコネクタをプロキシサーバとして使用するようにCloud Volumes ONTAP システムを設定できない場合は、「<作業環境名> is unable to send AutoSupport messages」というBlueXPから通知が届きます。

ネットワークの問題が原因でこのメッセージが表示される可能性が高いです。

この問題に対処するには、次の手順を実行します。

手順

1. CLIからシステムを管理できるように、Cloud Volumes ONTAP システムにSSH接続します。

   "Cloud Volumes ONTAP にSSH接続する方法について説明します"。

2. AutoSupport サブシステムの詳細なステータスを表示します。

   ```
   autosupport check show-details
   ```

   次のような応答が返されます。

```
    Category: smtp
          Component: mail-server
             Status: failed
             Detail: SMTP connectivity check failed for destination:
                     mailhost. Error: Could not resolve host -
'mailhost'
            Corrective Action: Check the hostname of the SMTP server

    Category: http-https
        Component: http-put-destination
            Status: ok
            Detail: Successfully connected to:
                    <https://support.netapp.com/put/AsupPut/>.

          Component: http-post-destination
             Status: ok
             Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

    Category: on-demand
          Component: ondemand-server
             Status: ok
             Detail: Successfully connected to:
                     https://support.netapp.com/aods/asupmessage.

    Category: configuration
            Component: configuration
                Status: ok
                Detail: No configuration issues found.
    5 entries were displayed.
```

http-httpsカテゴリのステータスが「ok」の場合は、AutoSupport が正しく設定されていて、メッセージを送信できることを意味します。

3. ステータスがOKでない場合は、各Cloud Volumes ONTAP ノードのプロキシURLを確認します。

```
autosupport show -fields proxy-url
```

4. プロキシURLパラメータが空の場合は、コネクタをプロキシとして使用するようにCloud Volumes ONTAP を設定します。

```
autosupport modify -proxy-url http://<connector private ip>:3128
```

5. AutoSupport のステータスを再度確認します。

```
autosupport check show-details
```

6. このステータスがFAILEDの場合は、Cloud Volumes ONTAP とポート3128のコネクタの間に接続が確立されていることを確認します。
7. 接続が確立されていることを確認したあともステータスIDに障害が発生している場合は、コネクタにSSHで接続します。

   "ConnectorのLinux VMへの接続の詳細については、を参照してください"

8. に進みます `/opt/application/netapp/cloudmanager/docker_occm/data/`
9. プロキシ構成ファイルを開く `squid.conf`

   ファイルの基本構造は次のとおりです。

```
        http_port 3128
        acl localnet src 172.31.0.0/16
        acl azure_aws_metadata dst 169.254.169.254

        http_access allow localnet
        http_access deny azure_aws_metadata
        http_access allow localhost
        http_access deny all
```

   localnet srcの値は、Cloud Volumes ONTAP システムのCIDRです。

10. Cloud Volumes ONTAP システムのCIDRブロックがファイルで指定された範囲にない場合は、値を更新するか、次のように新しいエントリを追加します。

    `acl cvonet src <cidr>`

    この新しいエントリを追加する場合は、許可エントリも追加することを忘れないでください。

    `http_access allow cvonet`

    次に例を示します。

```
        http_port 3128
        acl localnet src 172.31.0.0/16
        acl cvonet src 172.33.0.0/16
        acl azure_aws_metadata dst 169.254.169.254

        http_access allow localnet
        http_access allow cvonet
        http_access deny azure_aws_metadata
        http_access allow localhost
        http_access deny all
```

11. 設定ファイルを編集したら、sudoとしてプロキシコンテナを再起動します。

```
docker restart squid
```

12. Cloud Volumes ONTAP のCLIに戻って、Cloud Volumes ONTAP からAutoSupport メッセージを送信できることを確認します。

```
autosupport check show-details
```

EMSの設定

イベント管理システム（EMS）は、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 のドキュメント：EMS の設定の概要"。

概念

Cloud Volumes ONTAP ライセンス

Cloud Volumes ONTAP には、いくつかのライセンスオプションがあります。それぞれのオプションで、ニーズに合った消費モデルを選択できます。

ライセンスの概要

新規のお客様は、次のライセンスオプションを利用できます。

容量単位のライセンス
: ネットアップアカウントで複数のCloud Volumes ONTAP システムをプロビジョニングした容量分だけ料金が発生追加のクラウドデータサービスを購入できます。

Keystoneサブスクリプション
: ニーズに合わせて拡張できるサブスクリプションベースのサービス。 HA ペア向けのシームレスなハイブリッドクラウドエクスペリエンスを提供します。

以前のノード単位のライセンスモデルは、ライセンスを購入済みの既存のお客様や、アクティブな Marketplace サブスクリプションを所有しているお客様には引き続き提供されます。

以降のセクションでは、これらの各オプションについて詳しく説明します。

ライセンスがないと、ライセンスされた機能の使用はサポートされません。

容量単位のライセンス

容量ベースのライセンスパッケージを使用すると、TiB分の容量に対してCloud Volumes ONTAP の料金を支払うことができます。このライセンスはネットアップアカウントに関連付けられており、ライセンスで十分な容量が使用可能であれば、ライセンスに対して複数のシステムを充電することができます。

たとえば、 20TiB のライセンスを 1 つ購入して 4 つの Cloud Volumes ONTAP システムを導入し、各システムに 5TiB のボリュームを割り当てて合計 20TiB にするとします。そのアカウントに導入されている各 Cloud Volumes ONTAP システムのボリュームで容量を使用できます。

容量ベースのライセンスは、 a_packag_ の形式で用意されています。Cloud Volumes ONTAP システムを導入する際には、ビジネスニーズに応じて、複数のライセンスパッケージから選択できます。

パッケージ

Cloud Volumes ONTAP で使用できる容量ベースのパッケージは次のとおりです。

フリーミアム

Cloud Volumes ONTAP のすべての機能をネットアップから無償で提供（クラウドプロバイダの料金がまだ適用されます）。

- ライセンスや契約は必要ありません。

- ネットアップによるサポートは含まれていません。
- Cloud Volumes ONTAP システムあたりのプロビジョニング可能な容量は 500GiB に制限されています。
- ネットアップのアカウント 1 つにつき、最大 10 台の Cloud Volumes ONTAP システムを任意のクラウドプロバイダで使用できます。
- Cloud Volumes ONTAP システム用にプロビジョニングされた容量が500GiBを超えると、BlueXPはシステムをEssentialsパッケージに変換します。

  システムがEssentialsパッケージに変換されるとすぐに、が表示されます 最低料金 適用されます。

  プロビジョニングされた容量が 500GiB 未満の他のシステムは、 Freemium （ Freemium 製品を使用して導入されている場合）に残ります。

最適化

プロビジョニングされた容量とI/O処理の料金は別途お支払いください。

- Cloud Volumes ONTAP のシングルノードまたはHA
- 充電は、ストレージと使用量（I/O）という2つのコストコンポーネントに基づいています。

  データレプリケーション（SnapMirror）やNDMPに関連するI/Oは料金に含まれません。

- Azure Marketplaceでは、従量課金制または年間契約として提供されています
- Google Cloud Marketplaceでは、従量課金制サービスまたは年間契約として提供されます
- 選択したVMタイプでサポートされます：
- Azureの場合：E4s_v3、E4ds_v4、DS4_v2、DS13_v2、E8s_v3、およびE8ds_v4
- Google Cloudの場合：n2-standard-4、n2-standard-8
- ネットアップのクラウドデータサービスを追加コストで利用できます

Essentialsをクリックします

さまざまな構成で Cloud Volumes ONTAP の容量に基づいて料金が発生します。

- Cloud Volumes ONTAP 構成を選択します。
  - シングルノードまたは HA システム
  - ディザスタリカバリ（ DR ）用のファイルストレージとブロックストレージまたはセカンダリデータ
- ネットアップのクラウドデータサービスを追加コストで利用できます

プロフェッショナル

バックアップの数に制限はなく、あらゆる種類のCloud Volumes ONTAP 構成で容量ごとに料金が発生します。

- Cloud Volumes ONTAP 構成のライセンスを提供します

  プライマリボリュームとセカンダリボリュームの容量を同じ速度で課金する、シングルノードまたはHA

- BlueXPのバックアップとリカバリを使用したボリュームバックアップは無制限ですが、Professionalパッケージを使用するCloud Volumes ONTAP システムのみが対象です
- ネットアップのクラウドデータサービスを追加コストで利用できます

Edge Cache（エッジキャッシュ）

Cloud Volume Edge Cacheのライセンスを提供します。

- 分散型企業向けのビジネス継続性とデータ保護を備えたプロフェッショナルパッケージと同じ機能を提供します
- 設置面積の小さいWindows VMを使用して、各場所でインテリジェントなエッジキャッシングを実現します
- 3台のTiBを購入するごとに、1つのエッジノードを使用します
- Azure Marketplaceでは、従量課金制または年間契約として提供されています
- Google Cloud Marketplaceでは、従量課金制サービスまたは年間契約として提供されます

"Cloud Volume Edgeキャッシュがビジネスにどのように役立つかをご確認ください"

消費モデル

容量ベースのライセンスパッケージには、次の消費モデルがあります。

- * BYOL *：ネットアップから購入したライセンス。任意のクラウドプロバイダでCloud Volumes ONTAP を導入する際に使用できます。

[+]
BYOLではOptimizedパッケージとEdge Cacheパッケージは使用できません。

- * PAYGO *：クラウドプロバイダの市場から1時間ごとのサブスクリプション。
- * Annual *：クラウドプロバイダの市場から年間契約。

次の点に注意してください。

- ネットアップからライセンスを購入した場合（ BYOL ）は、クラウドプロバイダが提供する PAYGO のサブスクリプションも必要です。

  ライセンスは常に最初に請求されますが、次の場合は、マーケットプレイスで 1 時間ごとの料金が請求されます。

  - ライセンス容量を超えた場合
  - ライセンスの期間が終了する場合
- 市場から年間契約を結んでいる場合、導入する Cloud Volumes ONTAP システムにはその契約が適用されます。BYOL と年間市場契約を組み合わせることはできません。
- 中国のリージョンでは、BYOLを使用するシングルノードシステムのみがサポートされます。

パッケージの変更

導入後、容量ベースのライセンスを使用するCloud Volumes ONTAP システムのパッケージを変更できます。

たとえば、Essentialsパッケージを含むCloud Volumes ONTAP システムを導入した場合、ビジネスニーズの変化に応じて、そのシステムをProfessionalパッケージに変更できます。

"充電方法を変更する方法について説明します"。

価格設定

価格設定の詳細については、を参照してください "NetApp BlueXPのWebサイト"。

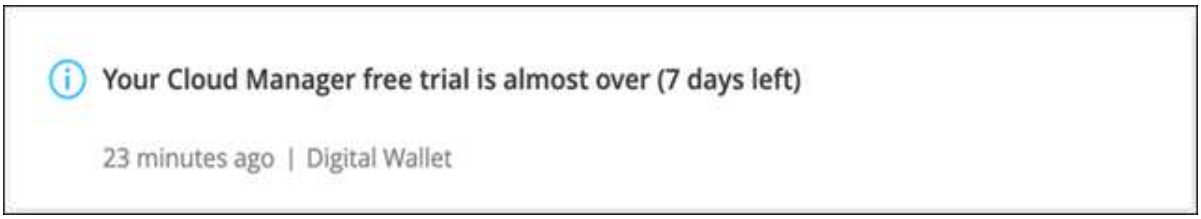
無償トライアルを利用できます

30 日間の無償トライアルをクラウドプロバイダのマーケットプレイスで従量課金制サブスクリプションで利用できます。この無償トライアルには、Cloud Volumes ONTAP とBlueXPのバックアップとリカバリ機能が含まれています。トライアルは、市場で提供サービスに登録すると開始されます。

インスタンスや容量の制限はありません。Cloud Volumes ONTAP システムは必要な数だけ導入でき、必要な容量を30日間無償で割り当てることができます。無料トライアルは、30日後に1時間ごとの有料サブスクリプションに自動的に変換されます。

Cloud Volumes ONTAP のソフトウェアライセンス料金は1時間ごとに発生しませんが、クラウドプロバイダからインフラ料金が請求されます。

無料トライアルが開始されたとき、7日間残っているとき、残りの1日があるときに、BlueXPに通知が届きます。例：



サポートされている構成

容量ベースのライセンスパッケージは Cloud Volumes ONTAP 9.7 以降で利用できます。

容量制限

このライセンスモデルでは、個々の Cloud Volumes ONTAP システムでディスクとオブジェクトストレージへの階層化によって、最大 2 PiB の容量をサポートします。

ライセンス自体にに関しては、最大容量制限はありません。

システムの最大数

容量単位のライセンスを使用する場合、Cloud Volumes ONTAP システムの最大数はネットアップアカウントあたり20個に制限されます。a_system_は、Cloud Volumes ONTAP HAペア、Cloud Volumes ONTAP シングルノードシステム、またはユーザが作成した追加のStorage VMです。デフォルトのStorage VMはカウントされません。これにより、環境 のすべてのライセンスモデルが制限されます。

たとえば、次の3つの作業環境があるとします。

- 1つのStorage VMを含むシングルノードのCloud Volumes ONTAP システム（Cloud Volumes ONTAP の導

入時に作成されるデフォルトのStorage VM）

この作業環境は1つのシステムとしてカウントされます。

- 2つのStorage VMを含むシングルノードのCloud Volumes ONTAP システム（デフォルトのStorage VMと、作成した追加のStorage VM 1台）

  この作業環境は、シングルノードシステム用と追加のStorage VM用の2つのシステムとしてカウントされます。

- 3つのStorage VMを含むCloud Volumes ONTAP HAペア（デフォルトのStorage VMと、作成した追加のStorage VM 2つ）

  この作業環境は、HAペア用と追加のStorage VM用の2つという3つのシステムとしてカウントされます。

合計6つのシステムです。その後、アカウントに14台のシステムを追加するためのスペースを確保します。

20台以上のシステムを必要とする大規模な導入環境の場合は、アカウント担当者または営業チームにお問い合わせください。

"ネットアップアカウントの詳細については、こちらをご覧ください"。

充電に関するメモ

以下の詳細は、課金が容量ベースのライセンスとどのように連携するかを理解するのに役立ちます。

最低料金

プライマリ（読み取り/書き込み）ボリュームが1つ以上あるStorage VMをデータ提供する場合は、最小4TiBの料金が発生します。プライマリボリュームの合計が4TiBを下回った場合、BlueXPはそのStorage VMに4TiBの最小料金を適用します。

まだボリュームをプロビジョニングしていない場合は、最小料金は適用されません。

Essentialsパッケージの場合、4TiBの最小容量料金は、セカンダリ（データ保護）ボリュームのみを含むStorage VMには適用されません。たとえば、1TiBのセカンダリデータが格納されたStorage VMがある場合、その1TiBのデータに対してのみ課金されます。Essentials以外のパッケージタイプ（Optimized、Professional、Edge Cache）では、ボリュームタイプに関係なく、最小容量4TiBが適用されます。

年齢が高すぎます

BYOL の容量を超えた場合やライセンスの有効期限が切れた場合は、マーケットプレイスのサブスクリプションに基づいて 1 時間あたりの料金が高すぎることを意味します。

Essentials パッケージ

Essentialsパッケージでは、導入タイプ（HAまたはシングルノード）とボリュームタイプ（プライマリまたはセカンダリ）ごとに課金されます。たとえば、_Essentials HA_に は、_Essentials Secondary HA_と は異なる価格が設定されています。

Essentialsライセンスをネットアップから購入した場合（BYOL）、その導入環境およびボリュームタイプでライセンスされている容量を超えた場合、BlueXPデジタルウォレットは、より高い価格のEssentialsライセンス（お持ちの場合）に対して追加料金を請求します。これは、市場に課金する前に、前払い済みの容量として

購入済みの使用可能容量を最初に使用するためです。市場に課金することで、月額料金が加算されます。

次に例を示します。Essentialsパッケージには、次のライセンスがあるとします。

- 500TiBのコミット済み容量を含む500TiBのセカンダリHA_License
- 100TiBのコミット済み容量のみを含む500TiB _ Essentialsシングルノードライセンス

セカンダリボリュームを含むHAペアにはもう1つの50TiBがプロビジョニングされます。BlueXPデジタルウォレットは、その50TiBをPAYGOに課金する代わりに、_Essentials Single Node_licenseに対して50TiBの超過料金を請求します。このライセンスは_Essentials Secondary HA_より も価格が高くなりますが、PAYGOの価格よりも安いです。

BlueXPデジタルウォレットでは、_Essentials Single Node_licenseに対して請求される50TiBが表示されます。

Storage VMs

- データ提供用の Storage VM （ SVM ）を追加する場合、追加のライセンスコストは発生しませんが、データ提供用 SVM ごとの容量は 4TiB になります。
- ディザスタリカバリ用 SVM は、プロビジョニングされた容量に基づいて料金が発生します。

HA ペア

HA ペアの場合、ノードのプロビジョニング済み容量に対してのみ料金が発生します。パートナーノードに同期ミラーリングされるデータには料金は発生しません。

FlexCloneボリュームとFlexCache ボリューム

- FlexClone ボリュームで使用される容量に対する料金は発生しません。
- ソースおよびデスティネーションの FlexCache ボリュームはプライマリデータとみなされ、プロビジョニング済みスペースに基づいて料金が発生します。

開始方法

容量単位のライセンスの取得方法については、以下をご覧ください。

- "AWSでCloud Volumes ONTAP のライセンスを設定"
- "AzureでCloud Volumes ONTAP のライセンスをセットアップする"
- "Google CloudでCloud Volumes ONTAP のライセンスを設定します"

Keystoneサブスクリプション

成長に合わせて拡張できるサブスクリプションベースのサービス。運用コストの消費モデルを希望するお客様に、設備投資やリースを先行するお客様にシームレスなハイブリッドクラウドエクスペリエンスを提供します。

課金は、Keystoneサブスクリプションに含まれる1つ以上のCloud Volumes ONTAP HAペアのコミット済み容量に基づいて行われます。

各ボリュームのプロビジョニング済み容量は集計され、Keystoneサブスクリプションのコミット済み容量と

定期的に比較されます。超過した容量はKeystoneサブスクリプションのバーストとして課金されます。

"NetApp Keystoneの詳細については、こちらをご覧ください"。

サポートされている構成

KeystoneサブスクリプションはHAペアでサポートされます。現時点では、このライセンスオプションはシングルノードシステムではサポートされていません。

容量制限

個々の Cloud Volumes ONTAP システムでは、ディスクとオブジェクトストレージへの階層化によって、最大 2 PiB の容量をサポートしています。

開始方法

Keystoneサブスクリプションの利用を開始する方法をご確認ください。

- "AWSでCloud Volumes ONTAP のライセンスを設定"
- "AzureでCloud Volumes ONTAP のライセンスをセットアップする"
- "Google CloudでCloud Volumes ONTAP のライセンスを設定します"

ノードベースのライセンス

ノードベースのライセンスは、 Cloud Volumes ONTAP のライセンスをノード単位で付与することが可能になった旧世代のライセンスモデルです。このライセンスモデルは、新規のお客様にはご利用いただけません。また、無償トライアルもご利用いただけません。ノード単位の充電は、前述のキャパシティ単位の充電方法に置き換えられました。

既存のお客様は、ノードベースのライセンスを引き続き利用できます。

- アクティブなライセンスがある場合は、 BYOL をライセンスの更新のみに使用できます。
- 有効なマーケットプレイスサブスクリプションをお持ちの場合は、そのサブスクリプションを通じて引き続き課金をご利用いただけます。

ライセンスの変換

既存の Cloud Volumes ONTAP システムを別のライセンス方式に変換することはできません。現在のライセンス方式は、容量単位のライセンス、Keystoneサブスクリプション、ノード単位のライセンスの3つです。たとえば、システムをノードベースのライセンスから容量ベースのライセンスに変換することはできません（逆の場合も同様）。

別のライセンス方式に移行する場合は、ライセンスを購入し、そのライセンスを使用して新しい Cloud Volumes ONTAP システムを導入してから、その新しいシステムにデータをレプリケートできます。

システムをPAYGOからノード単位のライセンスからBYOLへ（逆も同様）に変換することはサポートされていません。新しいシステムを導入し、そのシステムにデータをレプリケートする必要があります。 "PAYGOとBYOLの違いを解説します"。

ストレージ

クライアントプロトコル

Cloud Volumes ONTAP は、iSCSI、NFS、SMB、NVMe-TCP、およびS3クライアントプロトコルをサポートします。

iSCSI

iSCSI は、標準のイーサネットネットワークで実行できるブロックプロトコルです。ほとんどのクライアントオペレーティングシステムには、標準のイーサネットポートで動作するソフトウェアイニシエータが搭載されています。

NFS

NFS は、 UNIX および Linux システム向けの従来のファイルアクセスプロトコルです。クライアントは、 NFSv3 、 NFSv4 、および NFSv4.1 プロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。ファイルアクセスは、 UNIX 形式の権限、 NTFS 形式の権限、またはその両方の組み合わせを使用して制御できます。

クライアントは、 NFS プロトコルと SMB プロトコルの両方を使用して同じファイルにアクセスできます。

SMB

SMB は、 Windows システム向けの従来のファイルアクセスプロトコルです。クライアントは、 SMB 2.0 、 SMB 2.1 、 SMB 3.0 、および SMB 3.1.1 の各プロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。NFS と同様に、複数の形式の権限の組み合わせがサポートされています。

S3

Cloud Volumes ONTAP は、スケールアウトストレージ用のオプションとしてS3をサポートしています。S3プロトコルをサポートすることで、Storage VM（SVM）のバケットに格納されたオブジェクトへのS3クライアントアクセスを設定できます。

"S3マルチプロトコルの仕組みを説明します"。
"ONTAP で S3 オブジェクトストレージサービスを設定および管理する方法について説明します"。

nvme-tcpが表示されます

Cloud Volumes ONTAP バージョン9.12.1以降を使用している場合、クラウドプロバイダではnvme-tcpがサポートされます。BlueXPには、NVMe-oF TCPの管理機能はありません。

ONTAP を使用したNVMeの設定の詳細については、を参照してください "NVMe用のStorage VMを設定する"。

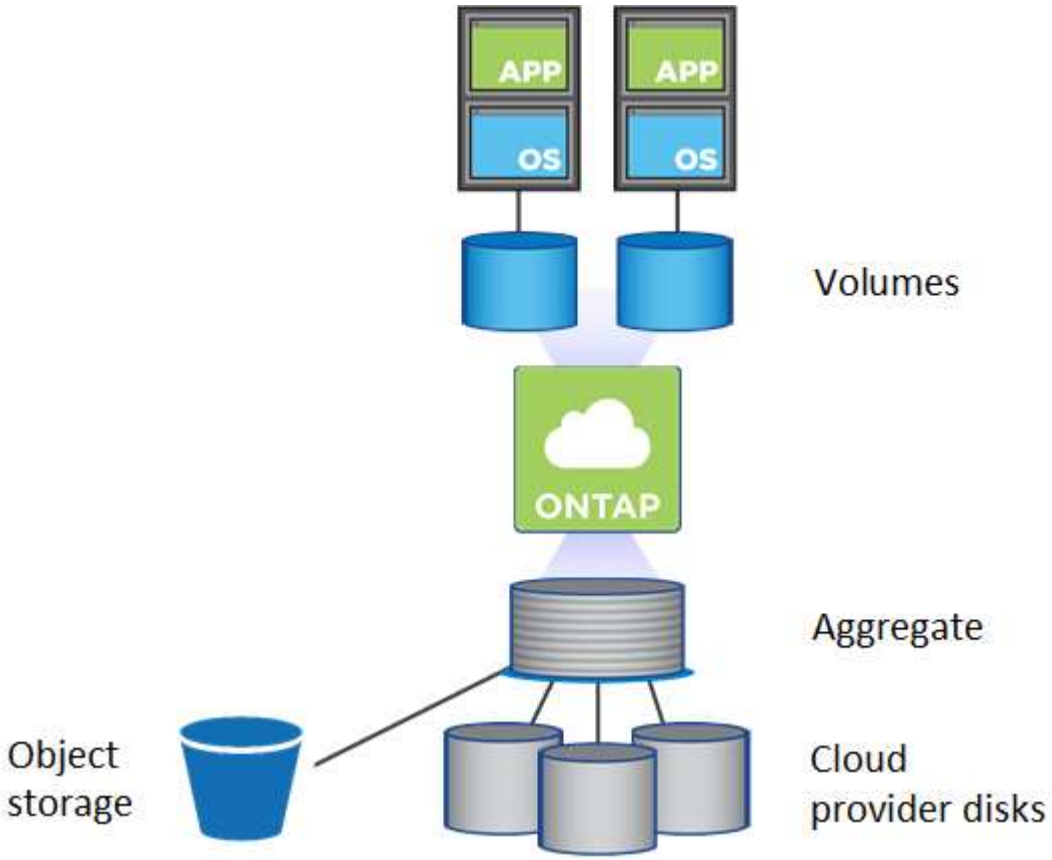
ディスクとアグリゲート

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。

すべてのディスクとアグリゲートは、BlueXP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。

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、BlueXPで500GiBのアグリゲートが作成された場合、使用可能な容量は442.94GiBです。

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。ただし、Amazon EBS Elastic Volumes機能をサポートする構成では、アグリゲートに最大8本のディスクを含めることがで

きます。 "Elastic Volumesのサポートに関する詳細情報"。

最大ディスクサイズは 16TiB です。

基盤となる EBS ディスクタイプは、汎用 SSD （ GP3 または gp2 ）、プロビジョニングされる IOPS SSD （ io1 ）、またはスループット最適化 HDD （ st1 ）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"。

スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

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 32TiB 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ペアは、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する次の2種類のディスクを使用します。

- *Premium*ページ*blobs*'最大ディスク・サイズ8TiB
- _管理対象ディスク_最大ディスクサイズは32TiBです

- 関連リンク *
- "Microsoft Azure のドキュメント：「 Azure managed disk types"
- "Microsoft Azure のドキュメント：「 Overview of Azure page blob"
- "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"

Google Cloudストレージ

Google Cloud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 64TiB です。

ディスクタイプは、 _Zonal SSD persistent disks _ 、 _Zonal Balanced persistent disks _ 、または _Zonal standard persistent disks _ のいずれかです。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のドキュメント：「Storage Options"
- "Google CloudでのCloud Volumes ONTAP のストレージ制限を確認します"

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。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。その他の RAID タイプはサポートされません。

ホットスペア

RAID0 は、冗長性を確保するためにホットスペアの使用をサポートしていません。

Cloud Volumes ONTAP インスタンスに接続された未使用のディスク（ホットスペア）の作成は不要な費用であり、必要に応じて追加のスペースをプロビジョニングすることができません。そのため、お勧めしません。

AWSのElastic Volumes

Cloud Volumes ONTAP アグリゲートでAmazon EBS Elastic Volumes機能がサポートされるため、パフォーマンスが向上し、容量が追加されます。また、必要に応じて基盤となるディスク容量が自動的に拡張されます。

利点

- ディスクの動的な拡張

  BlueXPは、Cloud Volumes ONTAP の実行中およびディスクの接続中に、ディスクのサイズを動的に増やすことができます。

- パフォーマンスの向上

  Elastic Volumesで有効になっているアグリゲートには、最大8本のディスクを割り当てて、2つのRAIDグ

ループで均等に利用することができます。この構成により、スループットとパフォーマンスが向上します。

- 大容量アグリゲート

  8本のディスクをサポートすることで、最大アグリゲート容量は128TiBになります。これらの制限は、Elastic Volumes機能が有効になっていないアグリゲートの場合、ディスクリミットの6つと最大96TiBを超えます。

  システムの合計容量制限は変わりません。

"Elastic Volumesの詳細については、AWSでご確認ください"

サポートされている構成

Amazon EBS Elastic Volumes機能は、特定のCloud Volumes ONTAP バージョンと特定のEBSディスクタイプでサポートされています。

Cloud Volumes ONTAP のバージョン

Elastic Volumes機能は、バージョン9.11.0以降で作成されたCloud Volumes ONTAP システムでサポートされます。この機能は、9.11.0より前に導入された既存のCloud Volumes ONTAP システムでは_サポートされません。

たとえば、Cloud Volumes ONTAP 9.9.0システムを作成したあとに、そのシステムをバージョン9.11.0にアップグレードした場合、Elastic Volumes機能はサポートされません。バージョン9.11.0以降を使用して導入した新しいシステムである必要があります。

EBSディスクタイプ

Elastic Volumes機能は、汎用SSD（GP3）またはプロビジョニングされたIOPS SSD（io1）を使用する場合、アグリゲートレベルで自動的に有効になります。Elastic Volumes機能は、他の種類のディスクを使用するアグリゲートではサポートされていません。

必要な**AWS**権限

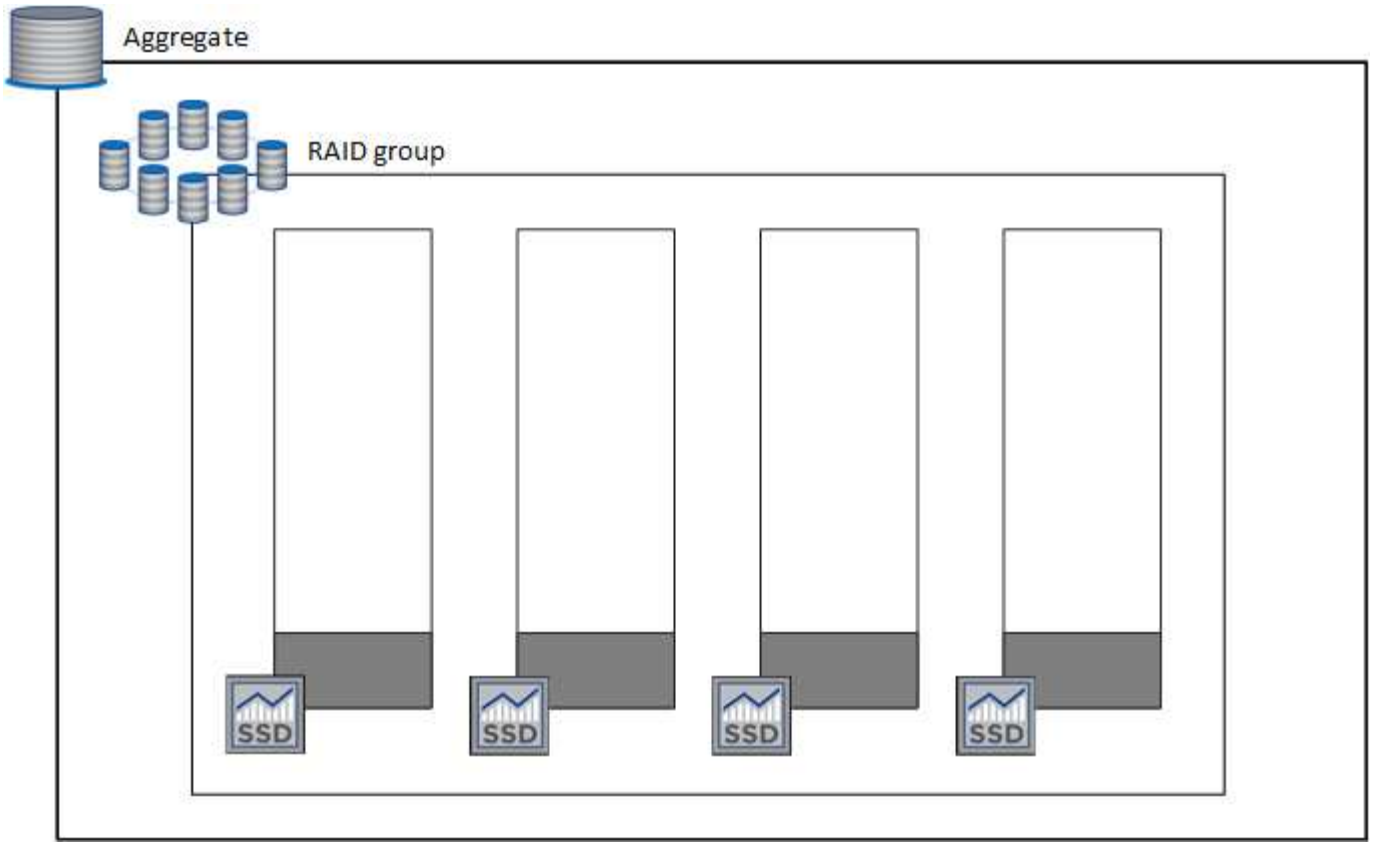
3.9.19リリース以降では、Cloud Volumes ONTAP アグリゲートでElastic Volumes機能を有効化して管理するために、Connectorで次の権限が必要になります。

- EC2: DescribeVolumesModifications (EC2 : DescribeVolumesMod
- EC2：ModifyVolume

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"

Elastic Volumesのサポートの仕組み

Elastic Volumes機能が有効になっているアグリゲートは、1つまたは2つのRAIDグループで構成されます。各RAIDグループには、同じ容量の同一ディスクが4本あります。それぞれ2.5TiBのディスクを4本含む10TiBのアグリゲートの例を次に示します。



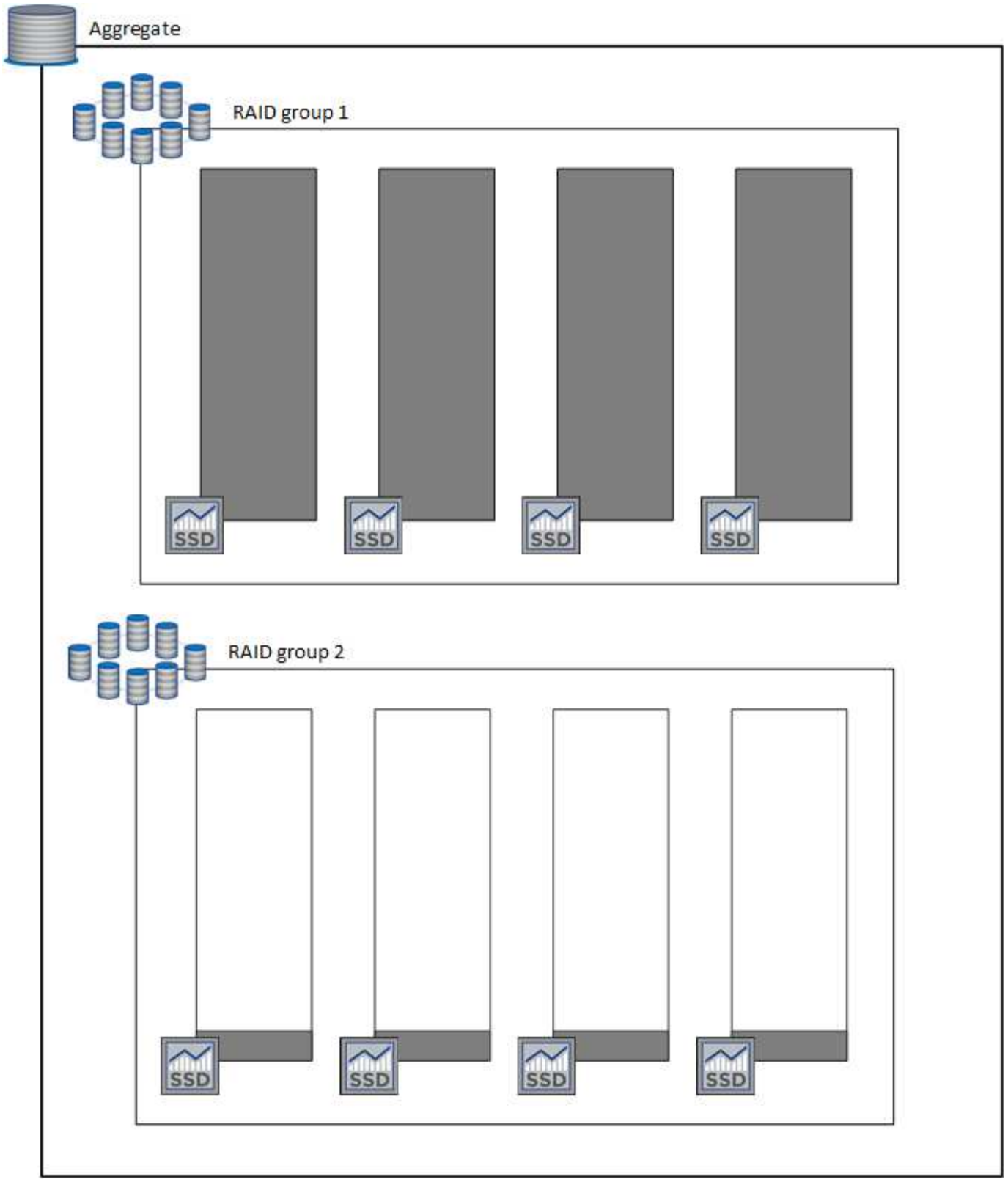
BlueXPでアグリゲートが作成されると、1つのRAIDグループから始まります。追加の容量が必要になった場合、BlueXPはRAIDグループ内のすべてのディスクの容量を同じ量だけ増やして、アグリゲートを拡張します。容量の増加は、最小256 GiBまたはアグリゲートのサイズの10%です。

たとえば、アグリゲートが1TiBの場合、各ディスクは250GiBです。アグリゲートの容量の10%は100GiBです。これは256GiBよりも小さいため、アグリゲートのサイズは256GiB以上（各ディスクで64GiB）増加します。

Cloud Volumes ONTAP システムの実行中およびディスクが接続されている間は、BlueXPによってディスクのサイズが増加します。変更はシステムの停止を伴わないものです。

アグリゲートが64TiB（各ディスクで16TiB）に達すると、BlueXPは容量を追加するために2つ目のRAIDグループを作成します。この2つ目のRAIDグループは、最初のRAIDグループと同様に機能します。つまり、同じ容量のディスクが4本あり、最大64TiBまで拡張できます。つまり、アグリゲートの最大容量は128TiBになります。

次に、2つのRAIDグループを含むアグリゲートの例を示します。最初のRAIDグループの容量が上限に達しており、2番目のRAIDグループのディスクには十分な空きスペースがあります。



ボリュームを作成したときの動作

GP3またはio1ディスクを使用するボリュームを作成すると、次のようにアグリゲート上にボリュームが作成されます。

- Elastic Volumesが有効になっている既存のGP3アグリゲートまたはio1アグリゲートがある場合、BlueXPはそのアグリゲートにボリュームを作成します。

- Elastic Volumesが有効になっているGP3アグリゲートまたはio1アグリゲートが複数ある場合、BlueXPは、最小限のリソースを必要とするボリュームをアグリゲート上に作成します。
- Elastic Volumesが有効になっていないGP3アグリゲートまたはio1アグリゲートだけがシステムに存在する場合、そのアグリゲートにボリュームが作成されます。

> このシナリオはほとんど発生しませんが、次の2つのケースが考えられます。
>
> - Elastic Volumes機能は、APIからアグリゲートを作成するときに明示的に無効にした。
> - ユーザインターフェイスから新しいCloud Volumes ONTAP システムを作成した場合、初期アグリゲートではElastic Volumes機能は無効になります。レビュー [制限] 詳細については、以下をご覧ください。

- 既存のアグリゲートに十分な容量がない場合は、Elastic Volumesを有効にしてアグリゲートが作成され、その新しいアグリゲートにボリュームが作成されます。

  アグリゲートのサイズは、要求されたボリュームサイズと10%の容量に基づいて決まります。

Capacity Management Mode （容量管理モード）

コネクタの容量管理モードは、他のタイプのアグリゲートと同様にElastic Volumesと連携します。

- 自動モードが有効な場合（デフォルト設定）、容量を追加する必要があると、BlueXPによってアグリゲートのサイズが自動的に拡張されます。
- 容量管理モードを手動に変更すると、追加の容量を購入する承認を求めるメッセージが表示されます。

"容量管理モードの詳細については、こちらをご覧ください"。

制限

アグリゲートのサイズの拡張には最大で6時間かかることがあります。この間、BlueXPはそのアグリゲートに容量を追加することはできません。

Elastic Volumesとの連携方法

Elastic Volumesは、BlueXPで次のように操作できます。

- GP3ディスクまたはio1ディスクを使用する場合は、初期アグリゲートでElastic Volumesが有効になっている新しいシステムを作成します

  "Cloud Volumes ONTAP システムの作成方法について説明します"

- Elastic Volumesが有効になっているアグリゲートに新しいボリュームを作成します

  GP3またはio1ディスクを使用するボリュームを作成すると、Elastic Volumesが有効になっているアグリゲートにボリュームが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 [ボリュームを作成したときの動作]。

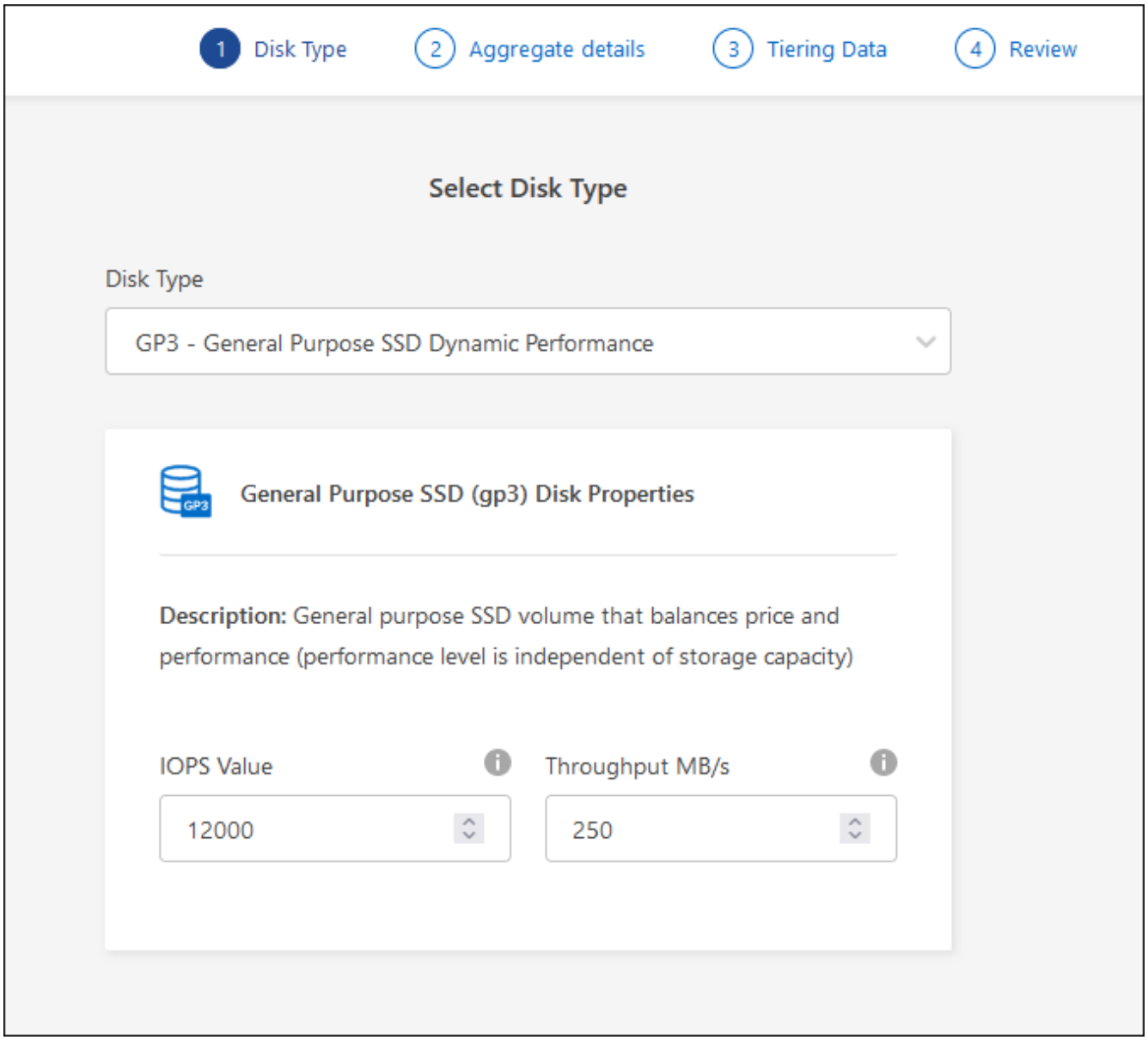
  "ボリュームを作成する方法について説明します"。

- Elastic Volumesが有効な新しいアグリゲートを作成します

Cloud Volumes ONTAP システムがバージョン9.11.0以降で作成されていれば、GP3ディスクまたはio1ディスクを使用する新しいアグリゲートでは、Elastic Volumesが自動的に有効になります。

アグリゲートを作成すると、アグリゲートの容量サイズを確認するプロンプトが表示されます。これは、ディスクサイズとディスク数を選択する他の設定とは異なります。

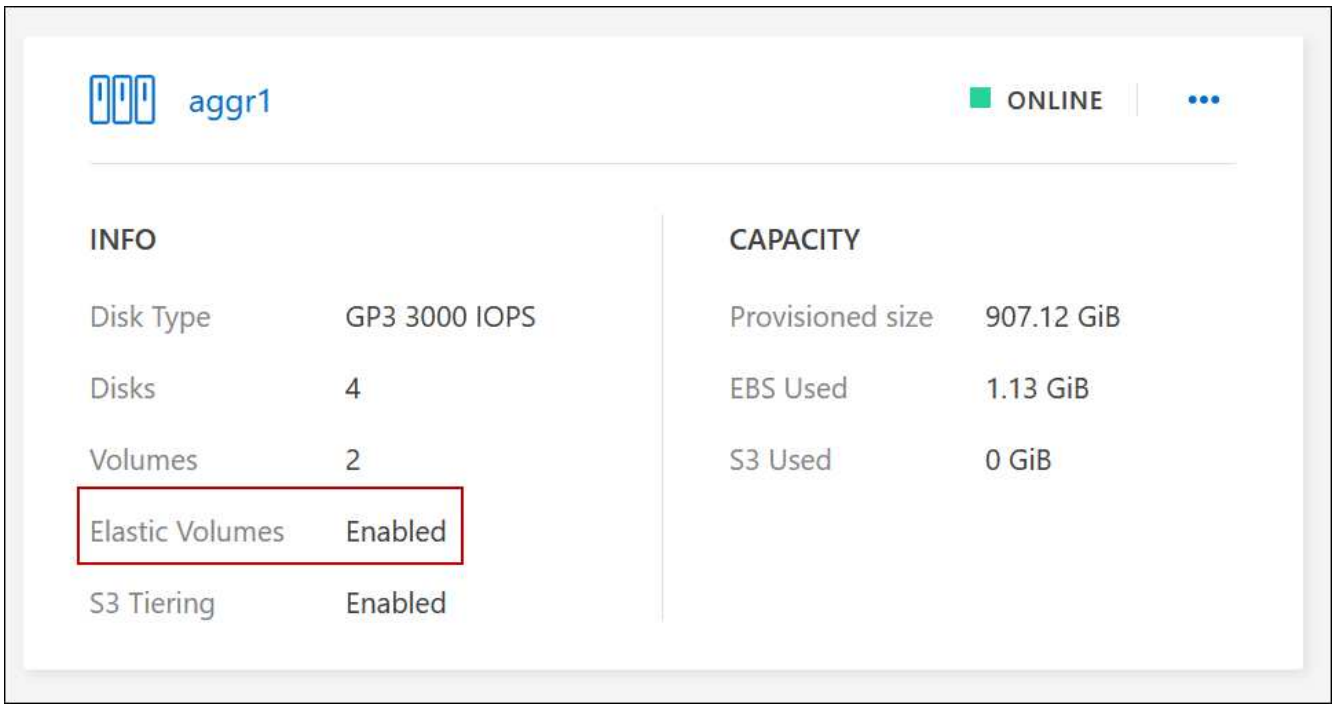
次のスクリーンショットは、GP3ディスクで構成される新しいアグリゲートの例を示しています。



"アグリゲートの作成方法を確認できます"。

- Elastic Volumesが有効になっているアグリゲートを特定します

Advanced Allocationページに移動すると、アグリゲートでElastic Volumes機能が有効になっているかどうかを確認できます。次の例では、aggr1でElastic Volumesが有効になっています。



- アグリゲートに容量を追加します

  BlueXPでは必要に応じて自動的にアグリゲートに容量が追加されますが、手動で容量を増やすことができます。

  "アグリゲートの容量を増やす方法について説明します"。

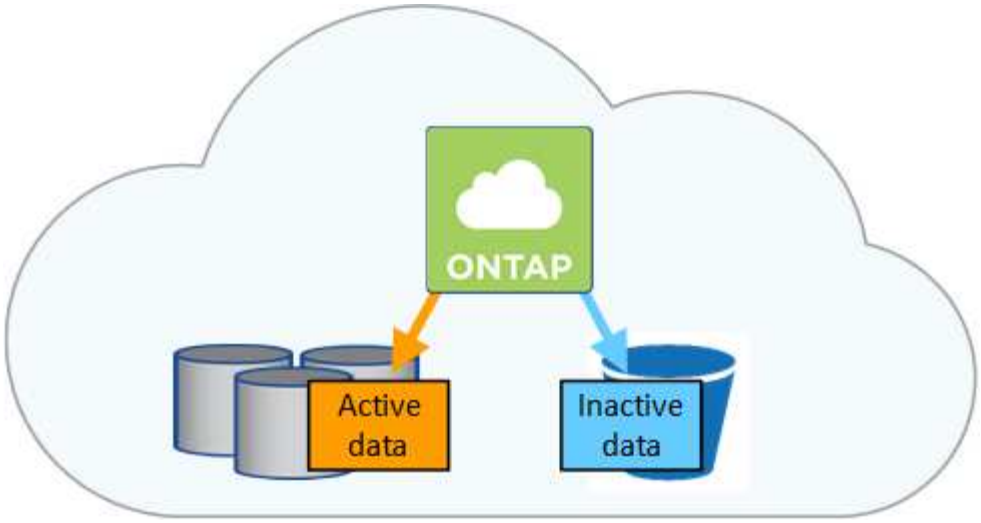
- Elastic Volumesが有効になっているアグリゲートにデータをレプリケートします

  移行先のCloud Volumes ONTAP システムがElastic Volumesをサポートしている場合、Elastic Volumeが有効になっているアグリゲートに移行先ボリュームが配置されます（GP3ディスクまたはio1ディスクを選択している場合）。

  "データレプリケーションの設定方法について説明します"

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。



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。

高パフォーマンス階層

パフォーマンス階層には、汎用 SSD （ GP3 または gp2 ）またはプロビジョニングされる IOPS SSD （ io1 ）を使用できます。

スループット最適化 HDD （ st1 ）を使用している場合、オブジェクトストレージへのデータの階層化は推奨されません。

大容量階層

Cloud Volumes ONTAP システムは、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。

BlueXPでは、作業環境ごとに1つのS3バケットが作成され、fabric-pool-_cluster unique identifier_という名前が付けられています。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。

BlueXPはS3バケットを作成する際、次のデフォルト設定を使用します。

- ストレージクラス：Standard
- デフォルトの暗号化：無効
- Block public access：すべてのパブリックアクセスをブロックします
- オブジェクトの所有権：ACLが有効
- バケットのバージョン管理：無効
- オブジェクトロック：無効

ストレージクラス

AWS の階層化データのデフォルトのストレージクラスは *Standard* です。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。

アクセス頻度の低いデータがない場合は、ストレージクラスを次のいずれかに変更することで、ストレージコストを削減できます。*Intelligent Tiering* _、_*one-Zone*低頻度アクセス、*Standard* -低頻度アクセス、または_S3 Glacier Instant Retrieval。ストレージクラスを変更すると、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行されます。

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、ストレージクラス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"。

作業環境の作成時にストレージクラスを選択し、あとでいつでも変更できます。ストレージクラスの変更の詳細については、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"。

データ階層化のストレージクラスは、システム全体に適用されます。ボリューム単位ではありません。

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。

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、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。

BlueXPでは、Cloud Volumes ONTAP の作業環境ごとに1つのコンテナを持つ新しいストレージアカウントが作成されます。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。

BlueXPでは、次の設定でストレージアカウントが作成されます。

- アクセス層：ホット
- パフォーマンス：標準
- 冗長性：ローカル冗長ストレージ（LRS）
- アカウント：StorageV2（汎用v2）
- REST API処理にはセキュアな転送が必要：有効
- ストレージアカウントキーへのアクセス：有効
- TLSの最小バージョン：バージョン1.2
- インフラストラクチャの暗号化:無効

ストレージアクセス階層

Azure の階層化データのデフォルトのストレージアクセス階層は、 _hot_tier です。ホット階層は、大容量階層でアクセス頻度が高いデータに最適です。

大容量階層のアクセス頻度の低いデータにアクセスする予定がない場合は、_cool_storage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。ストレージ階層をクールに変更すると、アクセス頻度の低い大容量階層のデータがクールなストレージ階層に直接移動します。

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、ストレージ階層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"。

作業環境の作成時にストレージ階層を選択し、あとでいつでも変更できます。ストレージ階層の変更の詳細については、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"。

データ階層化のためのストレージアクセス階層は、システム全体に適用されます。ボリューム単位ではありません。

Google Cloudのデータ階層化

Google Cloud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

パフォーマンス階層には、 SSD 永続ディスク、分散型永続ディスク、標準の永続ディスクがあります。

大容量階層

Cloud Volumes ONTAP システムは、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。

BlueXPは'各作業環境用にバケットを作成し'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。

BlueXPでバケットを作成すると、次のデフォルト設定が使用されます。

- 場所の種類：地域
- ストレージクラス：Standard
- public access：オブジェクトACLに依存します
- アクセスコントロール：きめ細かな設定
- 保護：なし
- データの暗号化：Googleで管理されるキー

ストレージクラス

階層化データのデフォルトのストレージクラスは、 *Standard Storage_class* です。データへのアクセス頻度が低い場合は、 *_Nearline Storage_or_Coldline Storage* に変更することでストレージコストを削減できます。ストレージクラスを変更すると、アクセス頻度の低いデータは選択したクラスに直接移動します。

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、ストレージクラスを変更する前にこの点を考慮する必要があります。 "Google Cloud Storage のストレージクラスの詳細については、こちらをご覧ください"。

作業環境の作成時にストレージ階層を選択し、あとでいつでも変更できます。ストレージクラスの変更の詳細については、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"。

データ階層化のストレージクラスは、システム全体に適用されます。ボリューム単位ではありません。

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。クーリング期間は、データがアグリゲートに書き込まれると開始されます。

最小クーリング期間とデフォルトのアグリゲートしきい値を 50% に変更できます（詳細については後述します）。 "冷却期間を変更する方法について説明します" および "しきい値を変更する方法について説明します"。

BlueXP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から選択できます。

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。

すべて

すべてのデータ（メタデータを除く）はすぐにコールドとしてマークされ、オブジェクトストレージにできるだけ早く階層化されます。ボリューム内の新しいブロックがコールドになるまで、 48 時間待つ必要はありません。「すべて」のポリシーが設定される前のボリュームにあるブロックは、コールドになるまで 48 時間かかります。

読み取られた場合、クラウド階層のコールドデータブロックはコールドのままで、パフォーマンス階層に書き戻されません。このポリシーは ONTAP 9.6 以降で使用できます。

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。その場合は、データ保護ボリュームに*Backup*ポリシーが適用されます。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、冷却時間が長くなります。

Cloud Volumes ONTAP をオフにすると、システムを再起動するまで各ブロックの温度が維持されます。たとえば、システムの電源をオフにしたときにブロックの温度が 5 であっても、システムの電源をオンにしたときの温度は 5 のままです。

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

BlueXPでは、Cloud Volumes ONTAP ストレージをシンプルかつ高度に管理できます。

すべてのディスクとアグリゲートは、BlueXP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

BlueXPを使用すると、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 用のストレージのプロビジョニングを簡単に行うことができます。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。BlueXPでは、インスタンスを起動するとき、および追加のボリュームをプロビジョニングする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、BlueXPは次の3つのうちいずれかの処理を行います。

- 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。

[+]
Elastic VolumesをサポートするAWSのアグリゲートの場合は、BlueXPでRAIDグループ内のディスクのサイズも拡張されます。 "Elastic Volumesのサポートに関する詳細情報"。

- 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。

BlueXPでは、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、いくつかの要因によっ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 Volumes ONTAP 用の新しいアグリゲートをAWSで作成すると、システムのアグリゲートの数が増えるにつれて、アグリゲートのディスクサイズが徐々に拡張されます。BlueXPは、AWSが許容す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、BlueXPでは、次のようなディスクサイズが選択される場合があります。

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.	500GiB	3TiB
4.	1TiB	6TiB
6.	2TiB	12TiB

この動作は、Amazon EBS Elastic Volumes機能をサポートするアグリゲートには適用されません。Elastic Volumesが有効になっているアグリゲートは、1つまたは2つのRAIDグループで構成されます。各RAIDグループには、同じ容量の同一ディスクが4本あります。 "Elastic Volumesのサポートに関する詳細情報"。

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

BlueXPでは、アグリゲートを自分で管理する代わりに、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、BlueXPがストレージ容量の決定を通知するかどうか、またはBlueXP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。

この動作は、コネクタの_Capacity Management Mode_onによって決定されます。容量管理モードは、そのコネクタで管理されているすべてのCloud Volumes ONTAP システムに影響します。別のコネクタがある場合は、別の方法で設定できます。

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、自動的に新しいディスクが購入されます。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などを実行します。

次の例は、このモードの動作を示しています。

- アグリゲートの容量がしきい値に達し、ディスクの容量が増えても、BlueXPはそのアグリゲート用の新しいディスクを自動的に購入するため、ボリュームを継続して拡張することができます。

  BlueXPは15分ごとに空き容量の比率をチェックし'追加のディスクを購入する必要があるかどうかを判断します

[+]
Elastic VolumesをサポートするAWSのアグリゲートの場合は、BlueXPでRAIDグループ内のディスクのサイズも拡張されます。 "Elastic Volumesのサポートに関する詳細情報"。

- アグリゲートが容量のしきい値に達し、かつ他のディスクをサポートできない場合は、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ボリュームが自動的に移動されます。

  ボリュームに新しいアグリゲートを作成すると、そのボリュームのサイズに対応するディスクサイズが選択されます。

  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、スペースをクラウドプロバンスに戻すことはできません。

- アグリゲートにボリュームが12時間以上格納されていない場合、BlueXPはそのアグリゲートを削除します。

容量の自動管理による **LUN** の管理

BlueXPの自動容量管理はLUNには適用されませんBlueXPでLUNを作成すると'自動拡張機能が無効になります

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、容量の決定が必要になったときに「Action Required」メッセージが表示されます。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。

詳細はこちら。

"容量管理モードを変更する方法について説明します"。

書き込み速度

BlueXPを使用すると'ほとんどのCloud Volumes ONTAP 構成で通常の書き込み速度または高速の書き込み速度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

通常の書き込み速度を選択した場合、データはディスクに直接書き込まれます。データをディスクに直接書き込んだ場合、計画外のシステム停止が発生した場合や、計画外のシステム停止が発生した場合のデータ損失の可能性を低減します（ HA ペアのみ）。

デフォルトでは、通常の書き込み速度が使用されます。

高速の書き込み速度

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、クラウドプロバイダが提供するストレージのパフォーマンスが整合ポイントの処理時間に影響する可能性があります。

高速書き込みを使用する場合

高速の書き込みパフォーマンスが求められるワークロードで、計画外のシステム停止が発生した場合や、計画外のシステム停止（ HA ペアのみ）が伴うカスケード障害が発生した場合のデータ損失リスクに対処できる場合は、高速の書き込み速度を使用することを推奨します。

高速書き込みを使用する場合の推奨事項

高速の書き込み速度を有効にする場合は、アプリケーションレイヤでの書き込み保護を確保するか、またはデータ損失が発生した場合にアプリケーションで許容されるようにする必要があります。

AWS で **HA** ペアを使用した場合の高速の書き込み速度

AWS の HA ペアで高速の書き込み速度を有効にする場合は、複数の Availability Zone （ AZ ；アベイラビリティゾーン）環境と単一の AZ 環境の保護レベルの違いを理解しておく必要があります。複数の AZ に HA ペアを導入すると、耐障害性が向上し、データ損失の可能性を軽減できます。

"AWS の HA ペアについて詳しくは、こちらをご覧ください"。

高速の書き込み速度をサポートする構成

すべての Cloud Volumes ONTAP 構成で高速書き込みがサポートされるわけではありません。デフォルトで

は、これらの構成では通常の書き込み速度が使用されます。

AWS

シングルノードシステムを使用する場合、 Cloud Volumes ONTAP では、すべてのインスタンスタイプで高速な書き込み速度がサポートされます。

9.8 リリース以降では、 Cloud Volumes ONTAP でサポートされているほぼすべての EC2 インスタンスタイプを使用する場合、 HA ペアでの高速書き込みがサポートされます。ただし、 m5.xlarge と r5.xlarge は除きます。

"Cloud Volume が提供する Amazon EC2 インスタンスの詳細については、こちらをご覧ください ONTAP はをサポートします"。

Azure

シングルノードシステムを使用する場合、 Cloud Volumes ONTAP では、すべての種類の VM で高速な書き込み速度がサポートされます。

HA ペアを使用する場合、 Cloud Volumes ONTAP では 9.8 リリース以降、複数の種類の VM で高速の書き込み速度がサポートされます。にアクセスします "Cloud Volumes ONTAP リリースノート" をクリックして、高速の書き込み速度をサポートする VM タイプを確認します。

Google Cloud

シングルノードシステムを使用する場合、 Cloud Volumes ONTAP では、すべての種類のマシンで高速な書き込み速度がサポートされます。

HAペアを使用する場合、Cloud Volumes ONTAP 9.13.0リリース以降では、いくつかのタイプのVMで高速の書き込み速度がサポートされます。にアクセスします "Cloud Volumes ONTAP リリースノート" をクリックして、高速の書き込み速度をサポートする VM タイプを確認します。

"Cloud の Google Cloud マシンタイプの詳細をご覧ください Volume ONTAP はをサポートします"。

書き込み速度を選択する方法

を作成するときに、書き込み速度を選択できます 新しい作業環境を構築できます "既存のシステムの書き込み速度を変更する"。

データ損失が発生した場合の予測

高速の書き込み速度が原因でデータ損失が発生した場合、Event Management System（EMS；イベント管理システム）で次の2つのイベントが報告されます。

- Cloud Volumes ONTAP 9.12.1以降

```
 NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0～9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
 ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8〜9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect.
```

この場合、Cloud Volumes ONTAP をブートして、ユーザの手を煩わせることなくデータを提供できるようにする必要があります。

データ損失が発生した場合のデータアクセスの停止方法

データ損失について懸念がある場合、データ損失時にアプリケーションの実行を停止し、データ損失の問題に適切に対処したあとでデータアクセスを再開するには、 CLI から NVFAIL オプションを使用してこの目標を達成します。

をクリックして **NVFAIL** オプションを有効にします

```
vol modify -volume <vol-name> -nvfail on
```

をクリックして **NVFAIL** 設定を確認します

```
vol show -volume <vol-name> -fields nvfail
```

NVFAIL オプションを無効にする場合

```
vol modify -volume <vol-name> -nvfail off
```

データ損失が発生した場合、 NVFAIL が有効になっている NFS または iSCSI ボリュームは、データ処理を停止する必要があります（ステートレスプロトコルである CIFS への影響はありません）。詳細については、を参照してください "NFS ボリュームまたは LUN へのアクセスに対する NVFAIL の影響"。

をクリックして **NVFAIL** 状態を確認します

```
vol show -fields in-nvfailed-state
```

データ損失の問題に適切に対処したら、 NVFAIL 状態を解消でき、ボリュームへのデータアクセスが可能になります。

をクリックして **NVFAIL** 状態を解消します

```
vol modify -volume <vol-name> -in-nvfailed-state false
```

Flash Cache

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おり、Cloud Volumes ONTAP はパフォーマンスを向上させるために_Flash Cache _として使用します。トークン更新テストの行を追加しています。

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。

サポートされている構成

Flash Cacheは、特定のCloud Volumes ONTAP 構成でサポートされています。でサポートされている構成を表示します "Cloud Volumes ONTAP リリースノート"

制限

- Cloud Volumes ONTAP 9.12.0までの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。Cloud Volumes ONTAP 9.12.1を導入またはアップグレードする場合、圧縮を無効にする必要はありません。

  BlueXP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 "CLI を使用してデータ圧縮を無効にします"。

- 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。

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。クラウド WORM ストレージには SnapLock テクノロジが採用されており、 WORM ファイルはファイルレベルで保護されます。

WORM ストレージの仕組み

WORM ストレージにコミットされたファイルは、保持期間が過ぎたあとも変更することはできません。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。

充電中

WORM ストレージの充電は、合計プロビジョニング容量に基づいて 1 時間ごとに行われます。

WORMのライセンスは、従量課金制または年間契約の条件でのみ利用できます。クラウドプロバイダのマー

ケットプレイスから購入できます。WORMは、ノードベースと容量ベースの両方のライセンスモデルをサポートしています。

Cloud Volumes ONTAPのWORMストレージにはBYOLライセンスは使用できません。

Cloud Volumes ONTAP 9.10.1以降では、次の充電動作について理解しておく必要があります。

- ONTAP 9.10.1以降では、WORMボリュームとWORM以外のボリュームを同じアグリゲートに配置できるようになりました。
- Cloud Volumes ONTAP 作業環境の作成時にWORMを有効にすると、BlueXPで作成したすべてのボリュームでWORMが有効になります。ただし、ONTAP CLIまたはSystem Managerを使用して、WORMを無効にしたボリュームを作成できます。これらのボリュームはWORM状態のままです。
- 作業環境の作成時にWORMを有効にしないと、BlueXPで作成したすべてのボリュームでWORMが無効になります。これらのボリュームのWORMレートでは課金されません。

"WORM ストレージの価格設定については、こちらをご覧ください"

WORM ストレージのアクティブ化

WORMストレージをアクティブ化する方法は、使用しているCloud Volumes ONTAP のバージョンによって異なります。

バージョン9.10.1以降

Cloud Volumes ONTAP 9.10.1以降では、ボリュームレベルでWORMを有効または無効にすることができます。

新しいCloud Volumes ONTAP 作業環境を作成する場合は、WORMストレージを有効または無効にするように求められます。

- 作業環境の作成時にWORMストレージを有効にすると、BlueXPで作成したすべてのボリュームでWORMが有効になります。ただし、System ManagerまたはCLIを使用して、WORMを無効にしたボリュームを作成できます。
- 作業環境の作成時にWORMストレージを無効にすると、BlueXP、System Manager、またはCLIで作成するすべてのボリュームでWORMが無効になります。作成時に有効にしなかったCloud Volumes ONTAP 作業環境でWORMを有効にする場合は、ネットアップサポートとのサポートチケットを作成する必要があります。

どちらのオプションを選択してもかまいません 充電の仕組みを理解する。

バージョン9.10.0以前

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。BlueXPで作成するすべてのボリュームでWORMが有効になっています。WORMストレージは個 々のボリュームで無効にすることはできません。

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ファイルを削除しています

privileged delete機能を使用して、保持期間中にWORMファイルを削除できます。

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とデータの階層化

Cloud Volumes ONTAP 9.8以降の新規システムを作成する場合は、データ階層化とWORMストレージの両方を有効にすることができます。WORMストレージによるデータ階層化を有効にすると、データをクラウドのオブジェクトストアに階層化できます。

データ階層化とWORMストレージの両方を有効にする場合は、次の点に注意してください。

- オブジェクトストレージに階層化されたデータには、ONTAP のWORM機能は含まれていません。WORMの機能をエンドツーエンドで維持するには、バケットの権限を正しく設定する必要があります。
- オブジェクトストレージに階層化されたデータはWORM機能を保持しません。つまり、バケットとコンテナへのフルアクセス権を持つ技術的には、ONTAP によって階層化されたオブジェクトをだれでも削除できます。
- Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

制限

- Cloud Volumes ONTAP の WORM ストレージは、「信頼されたストレージ管理者」モデルで機能します。WORM ファイルは書き換えから保護されますが、期限切れ前の WORM データがボリュームに含まれていた場合でも、クラスタ管理者はボリュームを削除できます。
- 信頼できるストレージ管理者モデルに加えて、 Cloud Volumes ONTAP の WORM ストレージも「信頼できるクラウド管理者」モデルで暗黙的に動作します。クラウド管理者は、クラウドプロバイダからクラウドストレージを直接削除するか、編集することで、有効期限が切れる前に WORM データを削除できました。

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。

HA コンポーネント

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。

メディエーター

AWS のメディエーターインスタンスの重要な詳細は、次のとおりです。

インスタンスタイプ
T2- マイクロ

ディスク
EBS 磁気ディスク × 1 （約 8GiB ）。

オペレーティングシステム
Debian 11.

Cloud Volumes ONTAP 9.10.0 以前では、 Debian 10 はメディエーターにインストールされていました。

アップグレード
Cloud Volumes ONTAP をアップグレードすると、必要に応じてメディエーターインスタンスも更新されます。

インスタンスへのアクセス
BlueXPからCloud Volumes ONTAP HAペアを作成すると、メディエーターインスタンスのキーペアを指定するように求められます。このキーペアは、を使用したSSHアクセスに使用できます `admin` ユーザ：

サードパーティのエージェント
サードパーティエージェントまたは VM 拡張機能は、メディエーターインスタンスではサポートされていません。

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。

ストレージのテイクオーバー、再同期、ギブバックは、すべてデフォルトで自動的に実行されます。ユーザによる操作は必要ありません。

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。
- Recovery Time Objective（RTO；目標復旧時間）は120秒です。
  システム停止が発生した場合、120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。

複数のアベイラビリティゾーン

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、BlueXP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。

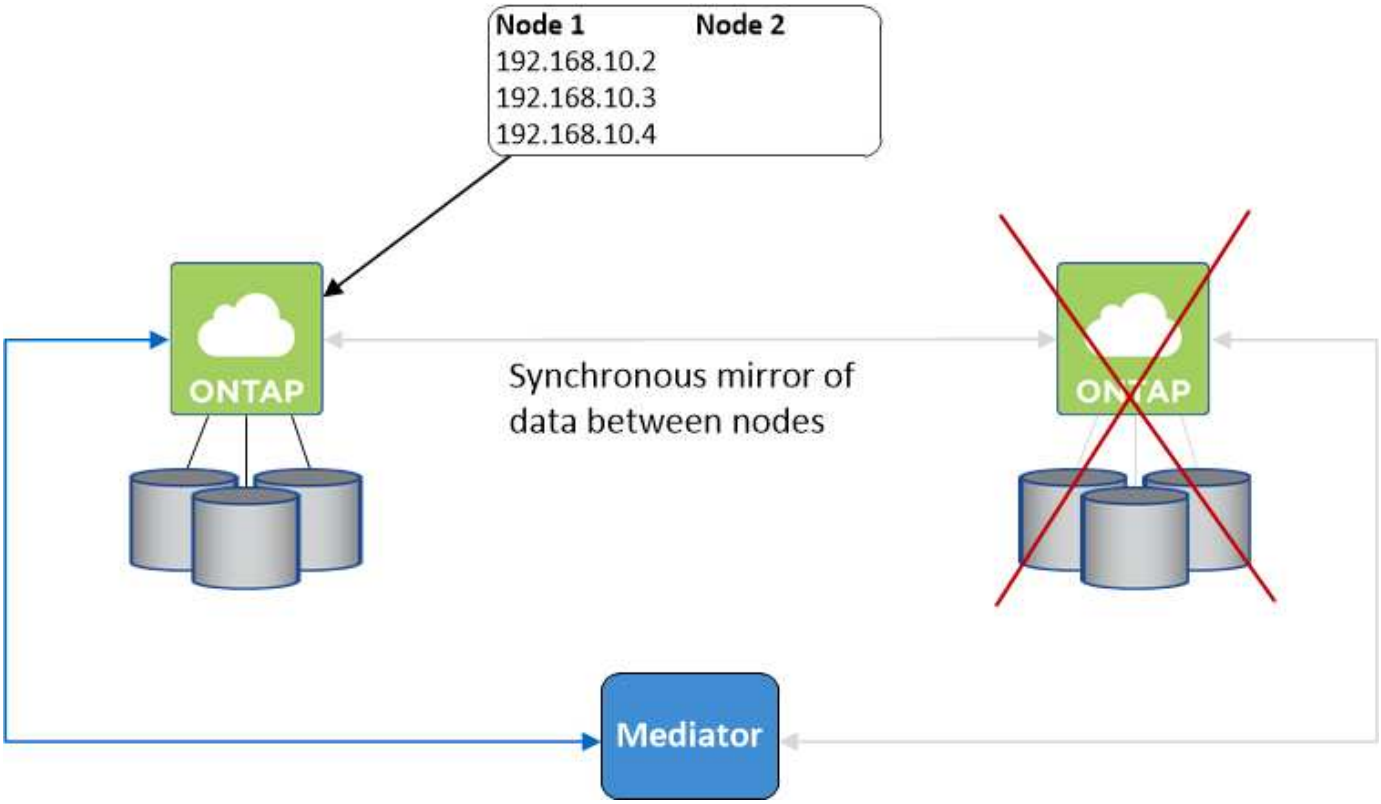
iSCSI のテイクオーバーとギブバック

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。

BlueXP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、*コマンドのマウント*をクリックします。

単一のアベイラビリティゾーン

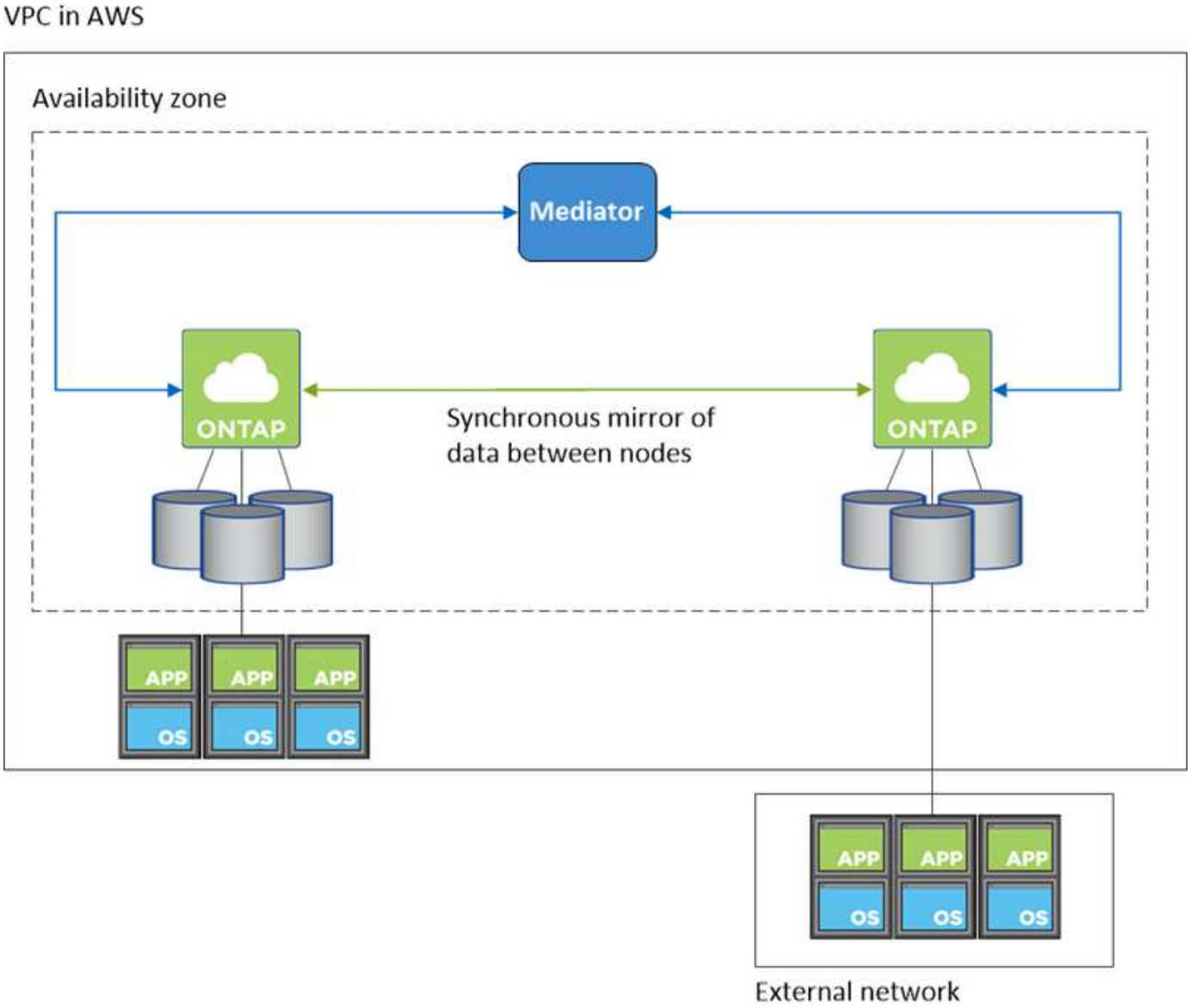
単一の可用性ゾーン（ AZ ）に HA 構成を導入すると、 Cloud Volumes ONTAP ノードを実行するインスタンスで障害が発生した場合でも、データの高可用性を確保できます。すべてのデータは、 vPC の外部からネイティブにアクセスできます。

BlueXPはを作成します "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。



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

新しいボリュームの作成時に追加のディスクが必要な場合、BlueXPは両方のノードに同じ数のディスクを割り当て、ミラーされたアグリゲートを作成し、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、BlueXPはノードごとに2つのディスクを割り当て、合計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、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/アクティブ構成として使用することも、アクティブ/パッシブ構成として使用することもできます。アクティブ/パッシブ構成では、パッシブノードが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、パッシブノードがデータ要求に応答します。

アクティブ/アクティブ構成は、ストレージシステムビューでBlueXPを使用している場合にのみセットアップできます。

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。

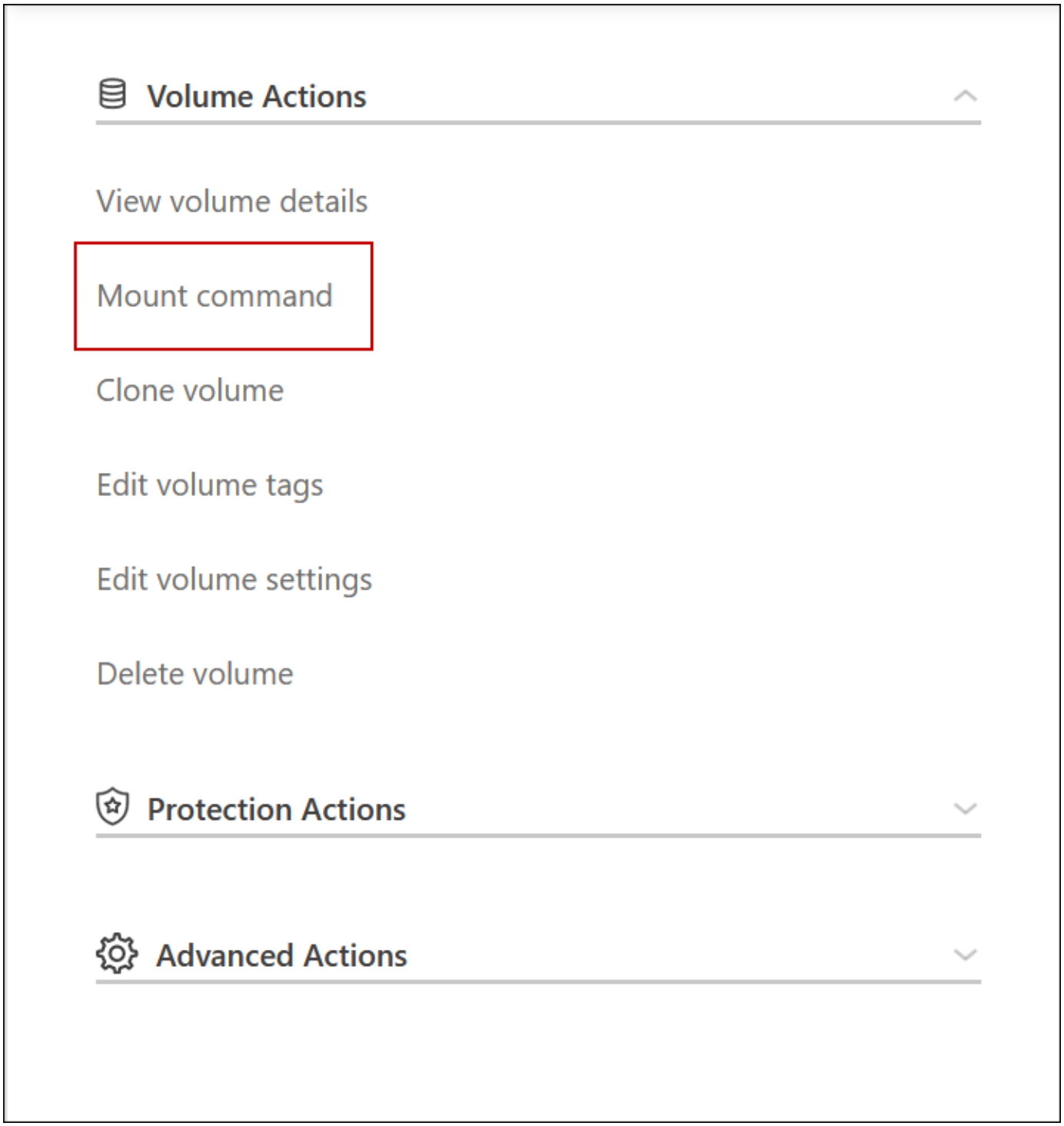
Cloud Volumes ONTAP のパフォーマンスの詳細については、を参照してください "パフォーマンス"。

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。

BlueXPの[Manage Volumes]パネルにある_Mount Command_Optionを使用すると、正しいIPアドレスを簡単に特定できます。

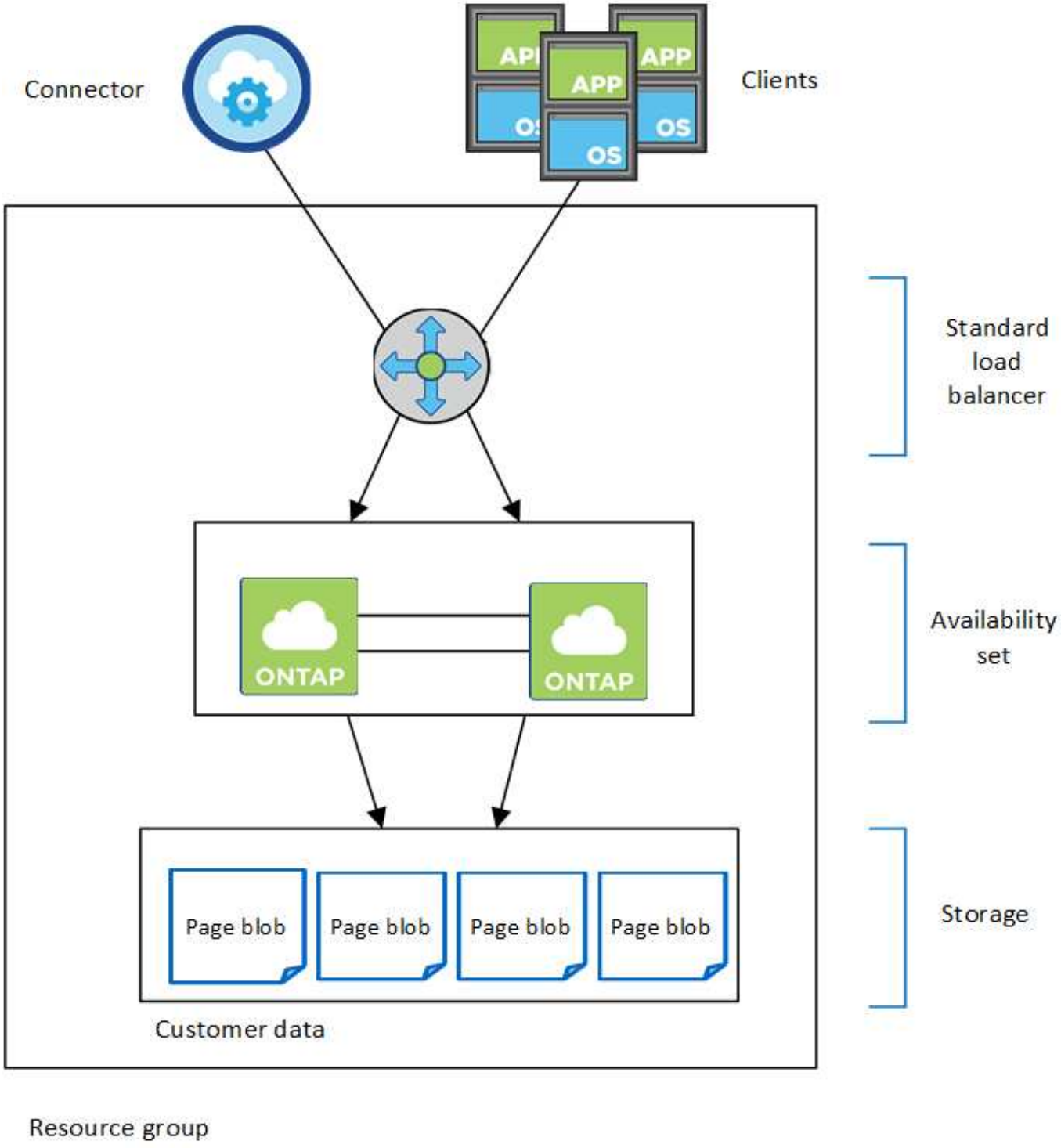


Azure のハイアベイラビリティペア

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ページBLOB構成には、次のコンポーネントが含まれています。



BlueXPによって導入されるAzureコンポーネントについては、次の点に注意してください。

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

Azure 可用性セットは、 Cloud Volumes ONTAP ノードを論理的にグループ化したものです。可用性セットを使用すると、ノードが異なる障害になっていることを確認し、ドメインを更新して冗長性と可用性を確保できます。 "可用性セットの詳細については、 Azure のドキュメントを参照してください"。

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。には追加のストレージも必要です "ブート、ルート、およびコアのデータ"。

ストレージアカウント

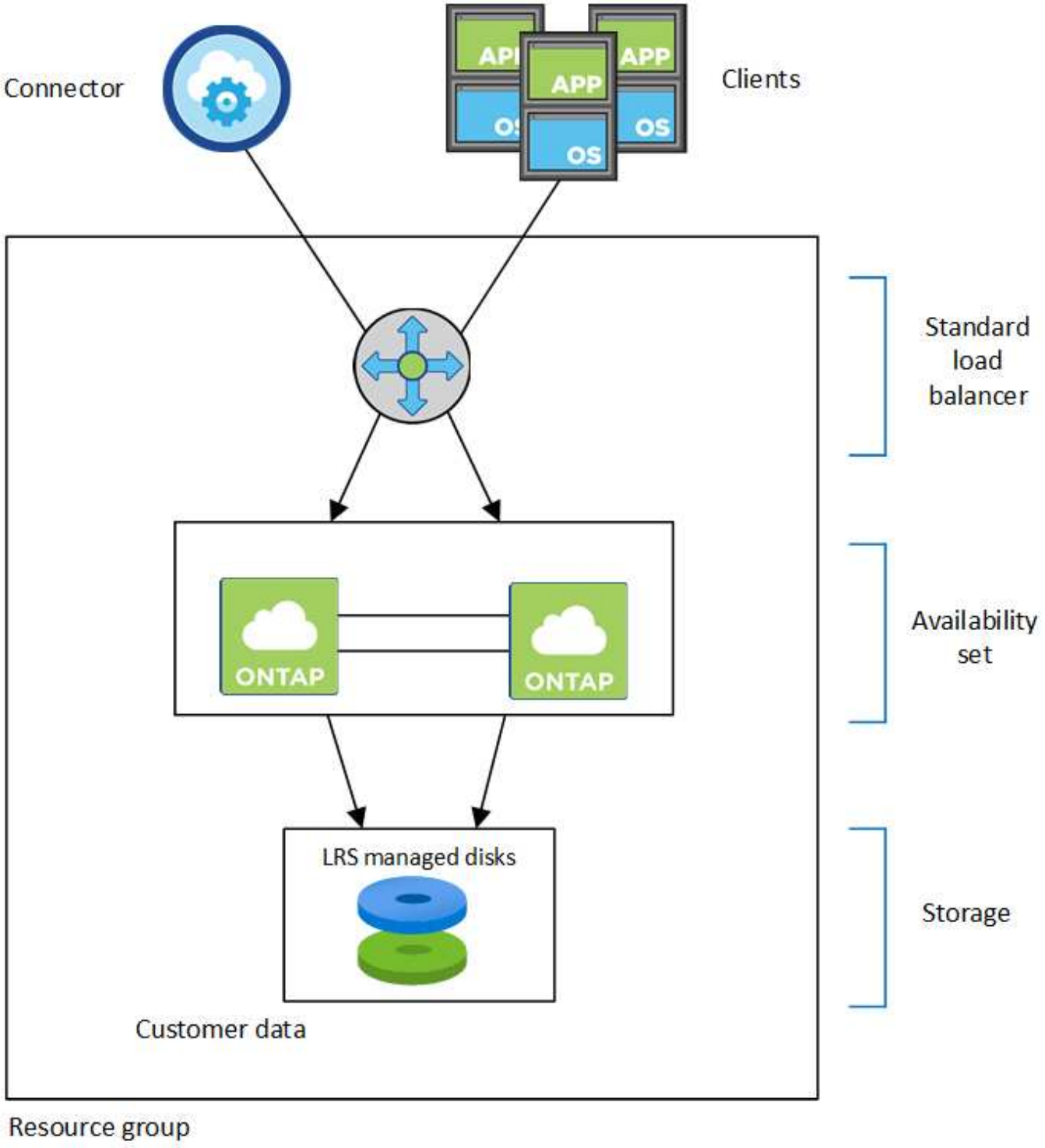
- 管理対象ディスクにはストレージアカウントが 1 つ必要です。
- ストレージ・アカウントあたりのディスク容量の上限に達しているため ' プレミアム・ストレージ・ページ・ブロブには 1 つ以上のストレージ・アカウントが必要です

  "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。
- Cloud Volumes ONTAP 9.7以降では、HAペア用にBlueXPで作成されるストレージアカウントは汎用v2のストレージアカウントです。
- 作業環境の作成時に、 Cloud Volumes ONTAP 9.7 HA ペアから Azure ストレージアカウントへの HTTPS 接続を有効にすることができます。このオプションを有効にすると、書き込みパフォーマンスに影響する可能性があります。作業環境の作成後に設定を変更することはできません。

共有管理対象ディスクを使用する**HA**シングルアベイラビリティゾーン構成

共有管理対象ディスク上で実行されるCloud Volumes ONTAP HAシングルアベイラビリティゾーン構成には、次のコンポーネントが含まれます。



BlueXPによって導入されるAzureコンポーネントについては、次の点に注意してください。

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

Azure 可用性セットは、 Cloud Volumes ONTAP ノードを論理的にグループ化したものです。可用性セットを使用すると、ノードが異なる障害になっていることを確認し、ドメインを更新して冗長性と可用性を確保できます。 "可用性セットの詳細については、 Azure のドキュメントを参照してください"。

ディスク

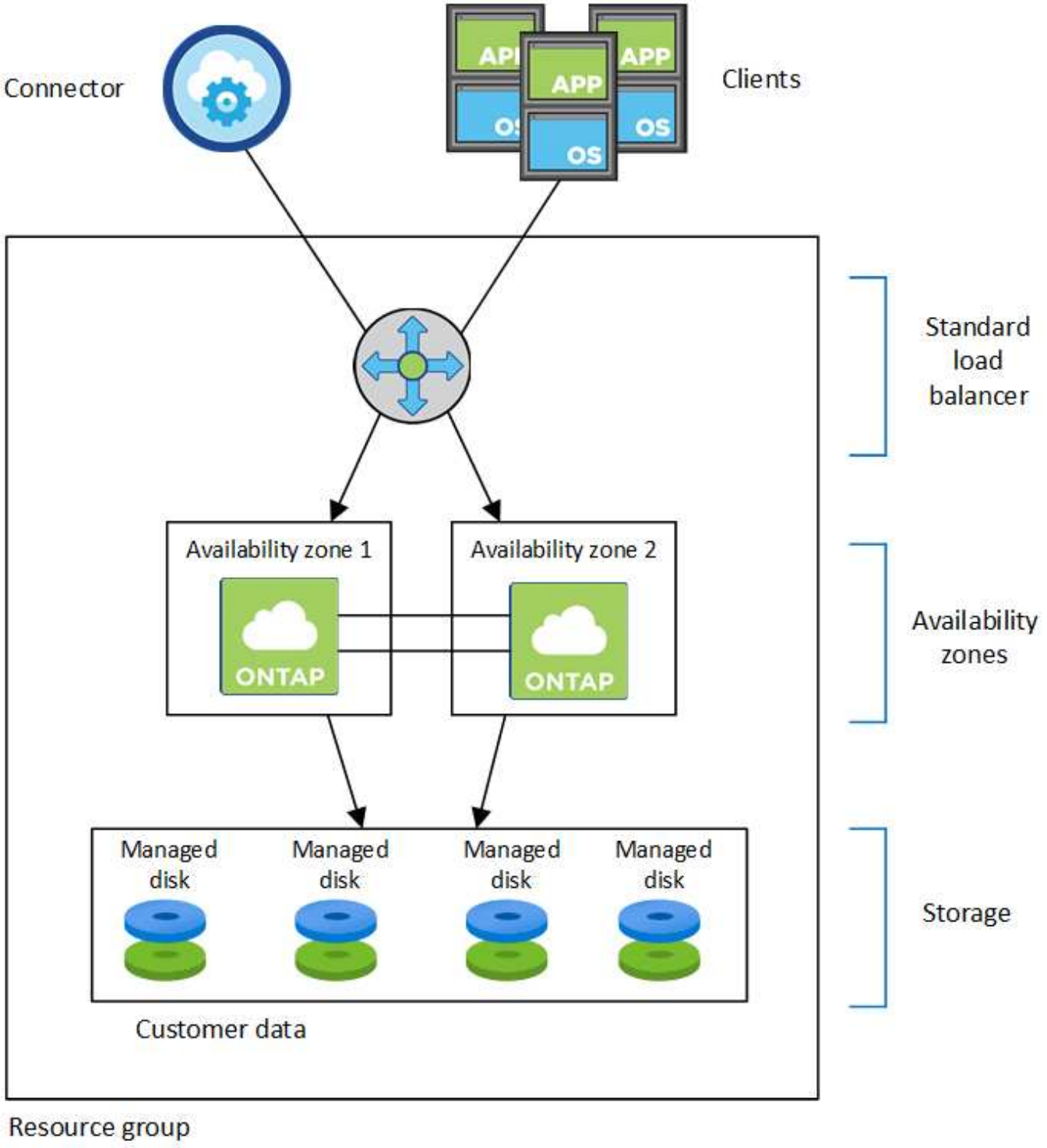
お客様のデータは、ローカル冗長ストレージ（LRS）管理対象ディスクに格納されています。各ノードがもう一方のノードのストレージにアクセスできます。には追加のストレージも必要です "ブート、ルート、パートナーのルート、コア、NVRAMの各データ"。

ストレージアカウント

ストレージアカウントは、診断ログの処理とBLOBストレージへの階層化を行うディスクベースの管理環境で使用されます。

HAの複数のアベイラビリティゾーン構成

AzureのCloud Volumes ONTAP HAマルチアベイラビリティゾーン構成には、次のコンポーネントが含まれています。



BlueXPによって導入されるAzureコンポーネントについては、次の点に注意してください。

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。

可用性ゾーン

2つのCloud Volumes ONTAP ノードが異なるアベイラビリティゾーンに導入されています。アベイラビリティゾーンを使用すると、各ノードが異なる障害ドメインに配置されます。 "Azureゾーン冗長ストレージの詳細については、Azureのドキュメントを参照してください"。

ディスク

お客様のデータは、ゾーン冗長ストレージ（ZRS）管理ディスクに格納されています。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。には追加のストレージも必要です "ブート、ルート、パートナールート、コアの各データ"。

ストレージアカウント

ストレージアカウントは、診断ログの処理とBLOBストレージへの階層化を行うディスクベースの管理環境で使用されます。

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。
- Recovery Time Objective（RTO；目標復旧時間）は120秒です。
  システム停止が発生した場合、120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。

ストレージのテイクオーバー、再同期、ギブバックは、すべてデフォルトで自動的に実行されます。ユーザによる操作は必要ありません。

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。

Google Cloud の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。Google Cloud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。

HA コンポーネント

Google Cloud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。

- 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。
- 1 つまたは 3 つのゾーン（推奨）。

  3 つのゾーンを選択すると、 2 つのノードとメディエーターが別々の Google Cloud ゾーンに配置されます。

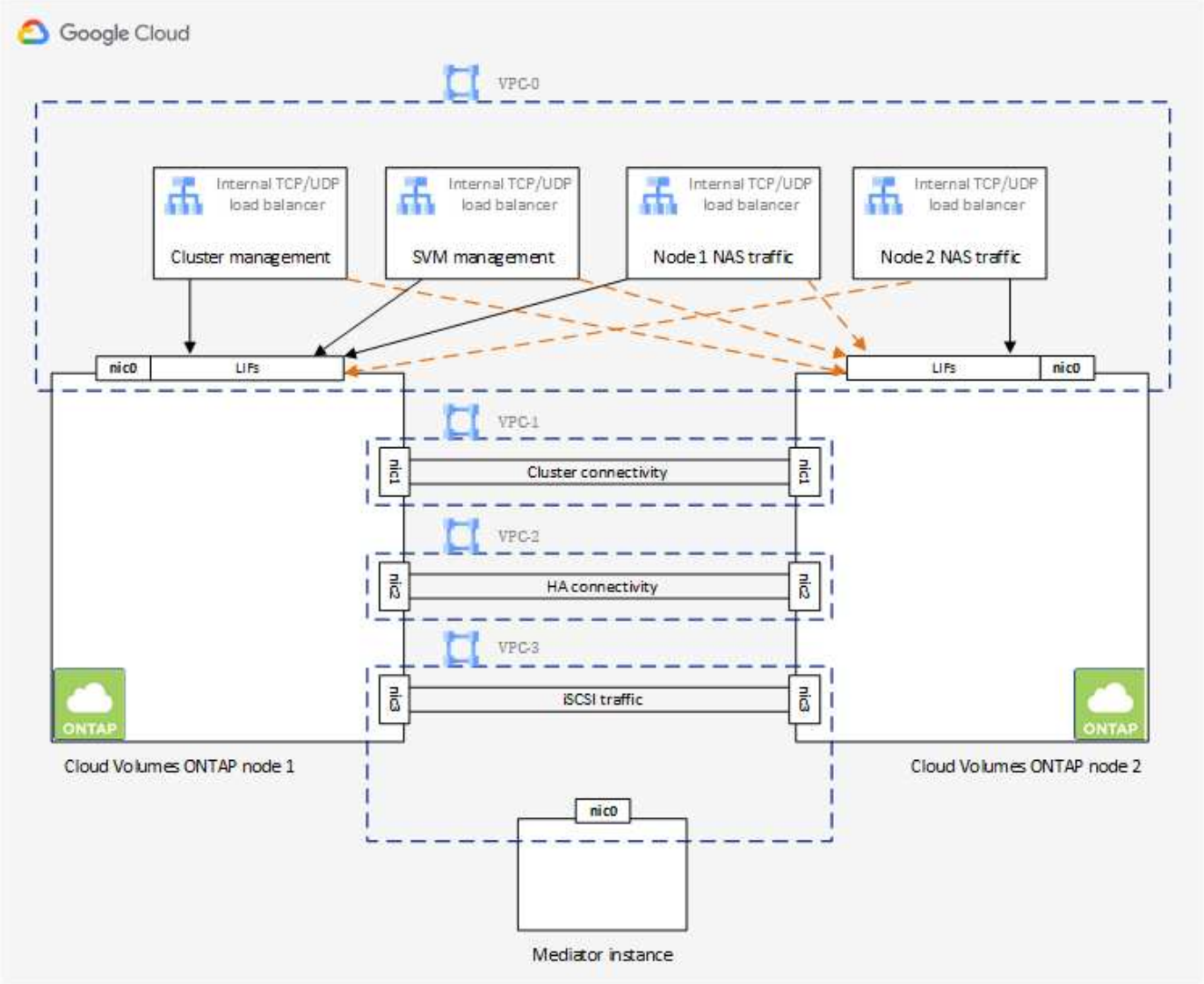
- 4 つの Virtual Private Cloud （ VPC ；仮想プライベートクラウド）

  GCP では各ネットワークインターフェイスが別々の VPC ネットワークに存在する必要があるため、構成では 4 つの VPC を使用します。

- Cloud Volumes ONTAP HA ペアへの着信トラフィックを管理する 4 つの Google Cloud 内部ロードバランサ（ TCP / UDP ）。

"ネットワーク要件について説明します"ロードバランサ、 VPC 、内部 IP アドレス、サブネットなどの詳細が含まれます。

次の概念図は、 Cloud Volumes ONTAP HA ペアとそのコンポーネントを示しています。



メディエーター

Google Cloud のメディエーターインスタンスの重要な詳細を次に示します。

インスタンスタイプ
: E2-micro（以前はF1-microインスタンスが使用されていました）

ディスク
: それぞれ10GiBの標準的な永続ディスク2本

オペレーティングシステム
: Debian 11.

> Cloud Volumes ONTAP 9.10.0 以前では、 Debian 10 はメディエーターにインストールされていました。

アップグレード
: Cloud Volumes ONTAP をアップグレードすると、必要に応じてメディエーターインスタンスも更新されま

す。

インスタンスへのアクセス

Debianの場合、デフォルトのクラウドユーザは `admin`。Google Cloudは、 `admin` ユーザーGoogle Cloud コンソールまたはgcloudコマンドラインを介してSSHアクセスが要求された場合。を指定できます `sudo` root権限を取得します。

サードパーティのエージェント

サードパーティエージェントまたは VM 拡張機能は、メディエーターインスタンスではサポートされていません。

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。

ストレージのテイクオーバー、再同期、ギブバックは、すべてデフォルトで自動的に実行されます。ユーザによる操作は必要ありません。

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。

- Recovery Time Objective（RTO；目標復旧時間）は120秒です。

  システム停止が発生した場合、120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

複数のゾーンまたは単一のゾーンに 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。

複数のゾーン（推奨）

3 つのゾーンに HA 構成を導入することで、ゾーン内で障害が発生した場合の継続的なデータ可用性を確保できます。書き込みパフォーマンスは、単一のゾーンを使用する場合に比べてわずかに低くなりますが、最小のパフォーマンスです。

シングルゾーン

Cloud Volumes ONTAP HA 構成では、単一のゾーンに導入する場合は分散配置ポリシーを使用します。このポリシーにより、 HA 構成がゾーン内の単一点障害から保護されます。障害の切り分けに別々のゾーンを使用する必要はありません。

この導入モデルでは、ゾーン間にデータ出力料金が発生しないため、コストが削減されます。

HA ペアでのストレージの動作

Cloud Volumes ONTAP クラスタとは異なり、 GCP の ONTAP HA ペアのストレージ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

新しいボリュームの作成時に追加のディスクが必要な場合、BlueXPは両方のノードに同じ数のディスクを割り当て、ミラーされたアグリゲートを作成し、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、BlueXPはノードごとに2つのディスクを割り当て、合計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。

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。

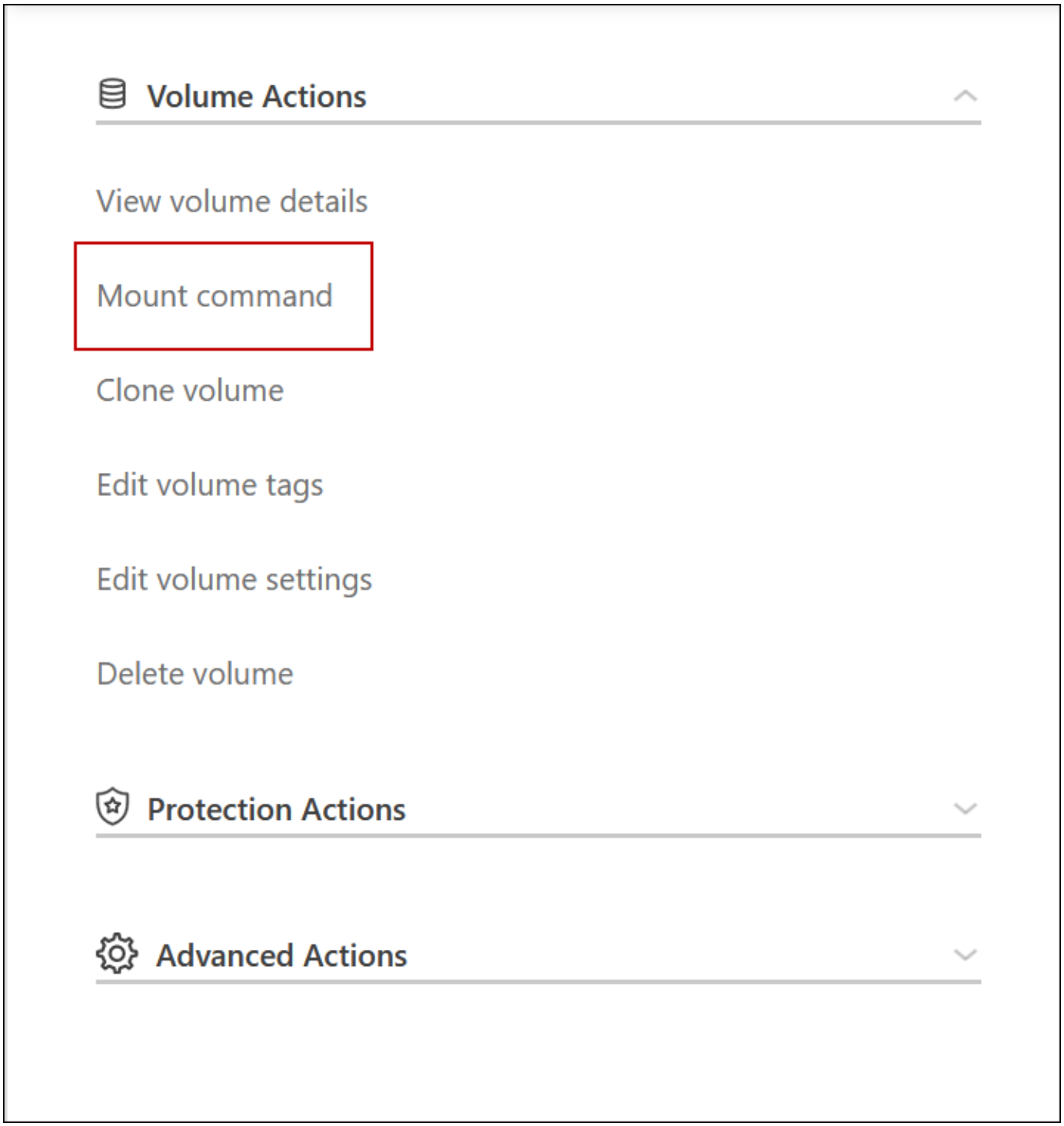
Cloud Volumes ONTAP のパフォーマンスの詳細については、を参照してください "パフォーマンス"。

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。

BlueXPの[Manage Volumes]パネルにある_Mount Command_Optionを使用すると、正しいIPアドレスを簡単に特定できます。



関連リンク

- "ネットワーク要件について説明します"
- "GCP の使用を開始する方法をご確認ください"

テイクオーバー中は操作を実行できません

HA ペアの一方のノードが利用できない場合は、もう一方のノードがパートナーに引き続きデータを提供します。これを _storage takeover _ と呼びます。storage giveback が

完了するまで、いくつかの操作は実行できません。

HAペアのノードが利用できない場合、BlueXPの作業環境の状態は_Degraded__です。

BlueXPストレージのテイクオーバーでは、次の操作を実行できません。

- サポート登録
- ライセンスの変更
- インスタンスまたは VM のタイプが変更された
- 書き込み速度の変更
- CIFSセットアップ
- 構成バックアップの場所を変更する
- クラスタのパスワードを設定しています
- ディスクとアグリゲートの管理（高度な割り当て）

これらの操作は、ストレージのギブバックが完了し、作業環境の状態が正常に戻ったあとで再度実行できます。

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。

- ネットアップの暗号化ソリューション（ NVE および NAE ）
- 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

ネットアップの暗号化ソリューションは、クラウドプロバイダがネイティブに暗号化することでハイパーバイザーレベルでデータを暗号化します。これにより、機密性の高いデータには二重の暗号化が必要になる場合があります。暗号化されたデータにアクセスすると、暗号化されていないデータがハイパーバイザーレベルで 2 回（クラウドプロバイダのキーを使用）暗号化されてから、ネットアップの暗号化ソリューションを再度使用して（外部キー管理ツールのキーを使用）暗号化されます。

ネットアップの暗号化ソリューション（ **NVE** および **NAE** ）

Cloud Volumes ONTAP はをサポートします "NetApp Volume Encryption （ NVE ）および NetApp Aggregate Encryption （ NAE ）"。NVE と NAE は、（ FIPS ） 140-2 に準拠したボリュームの保管データ暗号化を可能にするソフトウェアベースのソリューションです。NVE と NAE はいずれも AES 256 ビット暗号化を使用します。

- NVE は、一度に 1 ボリュームずつ保管データを暗号化する。各データボリュームには、一意の暗号化キーがあります。
- NAE は NVE の拡張機能です。 NVE は各ボリュームのデータを暗号化し、ボリュームはアグリゲート全体でキーを共有します。NAE では、アグリゲート内のすべてのボリュームの共通ブロックも重複排除できます。

NVE と NAE はどちらも外部キー管理機能でサポートされています。

新しいアグリゲートでは、外部キー管理ツールの設定後に NetApp Aggregate Encryption （ NAE ）がデフォルトで有効になります。NAE アグリゲートに含まれない新しいボリュームでは、 NetApp Volume Encryption （ NVE ）がデフォルトで有効になります（たとえば、外部キー管理ツールを設定する前に作成された既存のアグリゲートがある場合）。

サポートされているキー管理ツールをセットアップするだけで済みます。セットアップ手順については、を参照してください "ネットアップの暗号化ソリューション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）"。BlueXP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

データは、を使用して Azure の Cloud Volumes ONTAP で自動的に暗号化されます "Azure Storage Service Encryption の略" Microsoft が管理するキーを使用する場合：

必要に応じて、独自の暗号化キーを使用できます。 "Azure でお客様が管理するキーを使用するように Cloud Volumes ONTAP を設定する方法について説明します"。

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、データがディスクに書き込まれる前に常に暗号化されますが、BlueXP APIを使用して、_お客様が管理する暗号化キー_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。 "詳細はこちら。"。

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"。

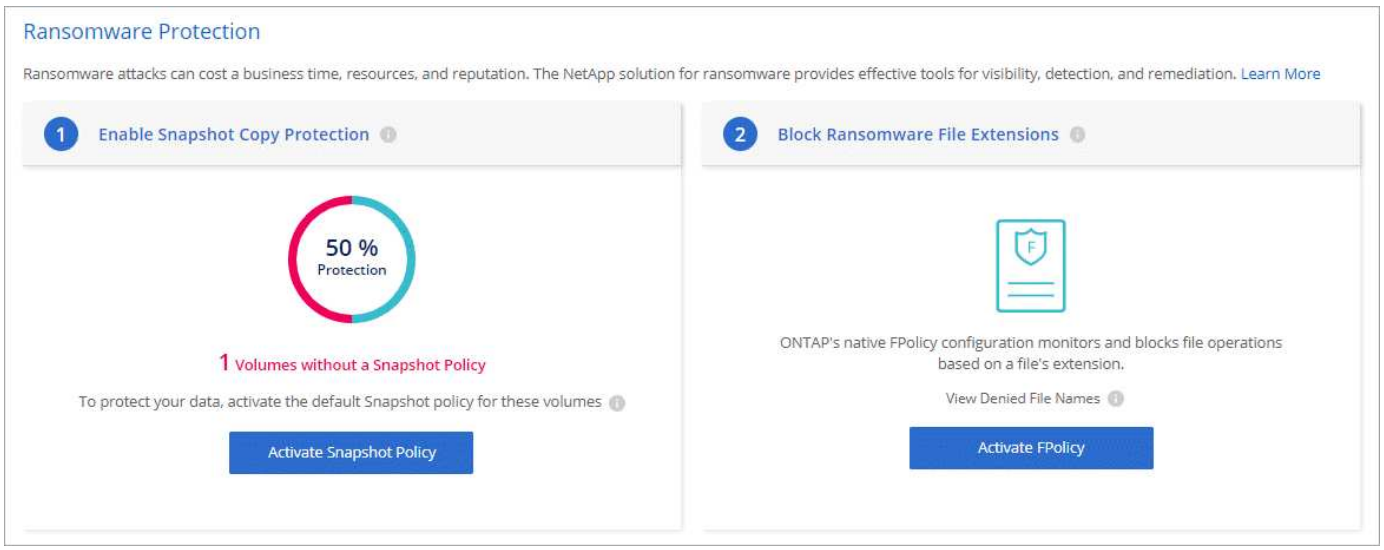
ランサムウェアからの保護

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。BlueXPを使用すると、NetApp解決策 for Ransomware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。

- BlueXPでは、Snapshotポリシーで保護されていないボリュームが特定され、それらのボリュームでデフォルトの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。

- BlueXPでは、ONTAPのFPolicy解決策 を有効にすることで、ランサムウェアの一般的な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。

パフォーマンスに関するテクニカルレポート

- Cloud Volumes ONTAP for AWS

"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

  "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"

- Cloud Volumes ONTAP for Google Cloud の略

  "ネットアップテクニカルレポート 4816 ：『 Performance Characterization of Cloud Volumes ONTAP for Google Cloud 』"

CPUパフォーマンス

Cloud Volumes ONTAP ノードは、クラウドプロバイダの監視ツールから高い利用率（ 90% 超）を示します。これは、 ONTAP が仮想マシンに提供されているすべての vCPU を、必要に応じて使用できるようにリザーブするためです。

詳細については、を参照してください "CLI を使用して ONTAP CPU 利用率を監視する方法に関するネットアップの技術情報アーティクルを参照してください"

ノードベースの BYOL のライセンス管理

ノードベース BYOL を使用する各 Cloud Volumes ONTAP システムには、アクティブなサブスクリプションを使用してシステムライセンスがインストールされている必要があります。BlueXPは、ライセンスを管理し、期限が切れる前に警告を表示することで、プロセスを簡素化します。

ノードベースのライセンスは、 Cloud Volumes ONTAP を使用するための旧世代の BYOL です。ノードベースのライセンスは、ライセンスの更新のみ可能です。

"Cloud Volumes ONTAP のライセンスオプションの詳細については、こちらをご覧ください"。

"ノードベースライセンスの管理方法については、こちらをご覧ください"。

BYOL システムのライセンス

ノードベースのライセンスは、単一のノードまたは HA ペアに対して最大 368 TiB の容量を提供します。

Cloud Volumes ONTAP BYOL システムでは、複数のライセンスを購入して、 368 TiB を超える容量を割り当てることができます。たとえば、 2 つのライセンスを購入して、 Cloud Volumes ONTAP に最大 736TiB の容量を割り当てることができます。また、 4 つのライセンスを購入して、最大 1.4 PiB までライセンスを取得することもできます。

シングルノードシステムまたは HA ペアに対して購入できるライセンスの数に制限はありません。

ディスク制限によって、ディスクだけを使用することで容量制限に達することがないことに注意してください。を使用すると、ディスク制限を超えることができます "使用頻度の低いデータをオブジェクトストレージに階層化します"。ディスクの制限については、を参照してください "ストレージの制限については、『 Cloud

Volumes ONTAP リリースノート』を参照してください"。

新しいシステムのライセンス管理

ノードベースのBYOLシステムを作成すると、ライセンスのシリアル番号とNetApp Support Site アカウントを入力するように求められます。BlueXPでは、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。

"NetApp Support Site アカウントをBlueXPに追加する方法について説明します"。

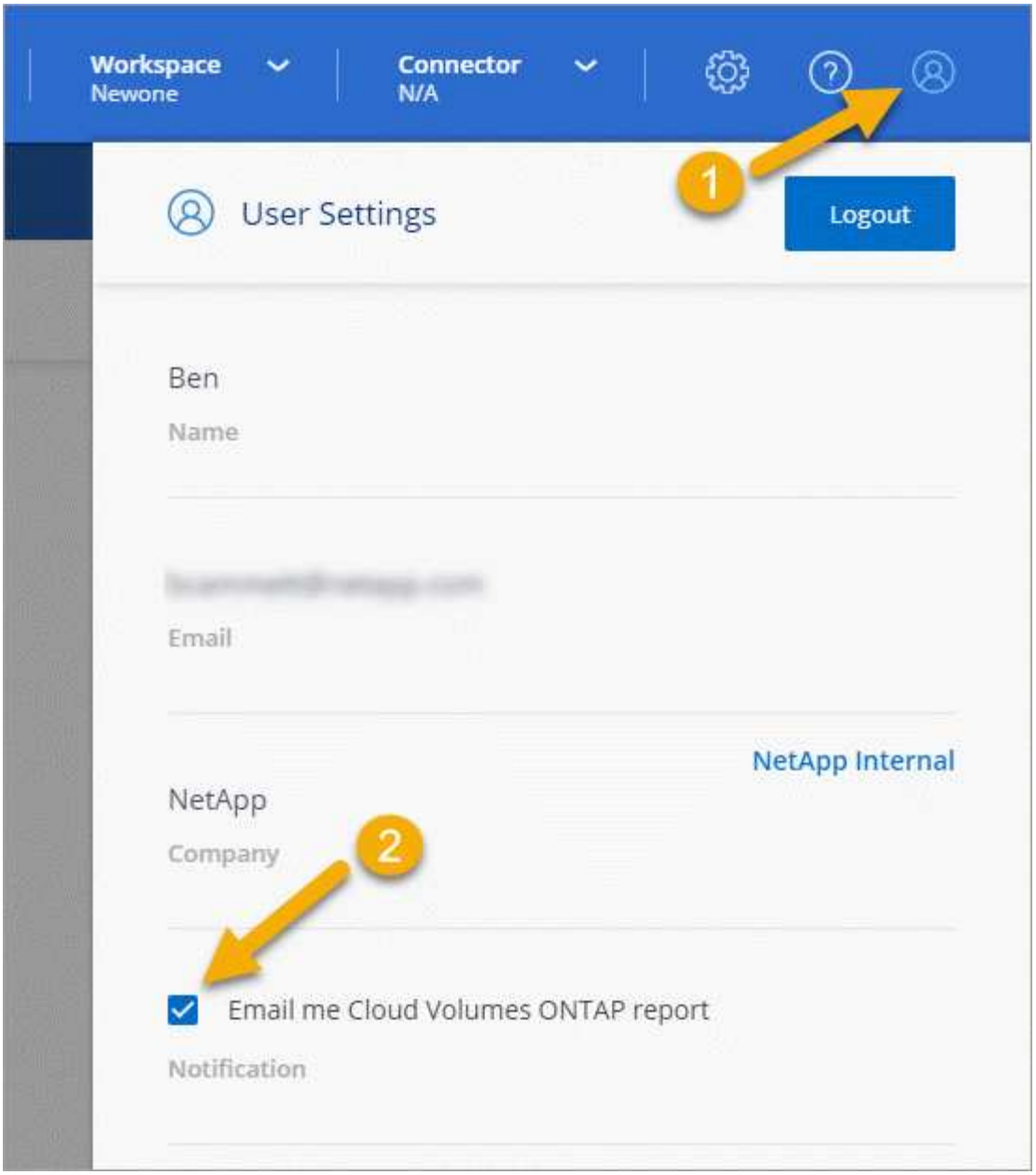
BlueXPが安全なインターネット接続経由でライセンスファイルにアクセスできない場合は、次の操作を実行できます "自分でファイルを取得し、ファイルをBlueXPに手動でアップロードします"。

ライセンスの有効期限

ノードベースのライセンスの有効期限が切れる30日前に警告が表示され、ライセンスの有効期限が切れると再度表示されます。次の図は、ユーザインターフェイスに表示される 30 日間の有効期限に関する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。

アカウント管理者がオプションを有効にしている場合、Cloud Volumes ONTAP レポートにライセンスの有効期限に関する警告が電子メールで送信されます。



E メールで送信されたレポートには、 2 週間ごとにライセンスの有効期限に関する警告が記載され

期限までにライセンスを更新しない場合は、 Cloud Volumes ONTAP システムがシャットダウンされます。再起動すると、自動的にシャットダウンされます。

ライセンスの更新

ネットアップの担当者に連絡してノードベースのBYOLサブスクリプションを更新すると、BlueXP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てCloud Volumes ONTAP システムにインストールします。

BlueXPが安全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、次の操作を実行できます "自分でファイルを取得し、ファイルをBlueXPに手動でアップロードします"。

新しいシステムへのライセンスの移動

既存のシステムを削除してから、同じライセンスを使用して新しいシステムを作成する場合、ノードベースの

BYOL ライセンスを Cloud Volumes ONTAP システム間で移動できます。

たとえば、既存のライセンスが有効なシステムを削除してから、別の VPC / VNet またはクラウドプロバイダ内の新しい BYOL システムでライセンスを使用できます。どのクラウドプロバイダでも使用できるのは、クラウドに依存しないシリアル番号 _ のみです。クラウドに依存しないシリアル番号は、 _908xxxx_prefix で始まります。

BYOL ライセンスは、お客様の会社およびNetApp Support Siteの特定のクレデンシャルセットに関連付けられていることに注意してください。

AutoSupport と Active IQ デジタルアドバイザ

ONTAP の AutoSupport コンポーネントはテレメトリを収集し、分析用に送信します。Active IQ デジタルアドバイザは AutoSupport からデータを分析し、プロアクティブなサポートと最適化を提供します。Active IQ は、人工知能を使用して潜在的な問題を特定し、ビジネスに影響が及ぶ前に解決を支援します。カットオーバーテストのために変更

ローカリゼーションのための変更。docbotとtest loc表示を有効にします。docbotの無効化をテストしています。Rubyのアップグレードを3回目に再テストします。Rubyアップグレードのプッシュをテストしています。

Active IQ では、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、 Active IQ が提供するデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Active IQ でできることは次のとおりです。

- アップグレードを計画する。

  Active IQ では、 ONTAP の新しいバージョンにアップグレードすることで解決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。

- システムの健全性を表示します。

  Active IQ ダッシュボードで、健全性に関する問題が報告されるため、それらの問題の解決に役立ちます。システム容量を監視して、ストレージスペースが不足しないようにします。システムのサポートケースを表示します。

- パフォーマンスを管理

  Active IQ には、 ONTAP System Manager に表示されるよりも長期間にわたるシステムパフォーマンスが表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定します。
  効率性の最大化Storage Efficiency 指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定します。

- インベントリと構成を表示します。

  Active IQ は、インベントリおよびソフトウェアとハードウェアの構成に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認し、サービス契約を更新してサポートを継続するかを確

認します。

関連情報

- "ネットアップのマニュアル： Active IQ Digital Advisor"
- "Active IQ を起動します"
- "SupportEdge サービス"

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。

デフォルトのセットアップ

- BlueXPでは、Cloud Volumes ONTAP を導入するとデータ提供用のStorage VMが1つ作成されます。追加の Storage VM をサポートする構成もあります。 "Storage VM の管理に関する詳細情報"。

  BlueXP 3.9.5リリース以降では、最初のStorage VMで論理スペースのレポートが有効になります。スペースが論理的に報告されると、 ONTAP は、 Storage Efficiency 機能で削減されたすべての物理スペースが使用済みと報告するようにボリュームスペースを報告します。

- BlueXPでは、次のONTAP 機能ライセンスがCloud Volumes ONTAP に自動的にインストールされます。
  - CIFS
  - FlexCache
  - FlexClone
  - iSCSI
  - Cloud Volumes ONTAP 9.12.1 GA以降、マルチテナント暗号化キー管理（MTEKM
  - 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システム上のSVM管理LIF
- Google CloudのHAシステム上のSVM管理LIFです
- AWSのシングルノードシステム上のSVM管理LIF
- ノード管理 LIF

[+]
Google Cloudでは、このLIFがクラスタ間LIFと組み合わされます。

- iSCSI データ LIF
- CIFS および NFS データ LIF

> クラウドプロバイダの要件により、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、HTTPを使用して構成バックアップをコネクタに送信します。

    バックアップには\http://ipaddress/occm/offboxconfig/からアクセスできます。_ipaddress_はコネクタホストのIPアドレスです。

  - BlueXPでは、他の管理ツール（System ManagerやCLIなど）とは異なる方法でいくつかのボリューム属性を設定します。

    次の表に、BlueXPで設定されるボリューム属性とデフォルト値の違いを示します。

属性	**BlueXP**によって設定された値
オートサイズモード	成長
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ボリュームのNTFS UNIX（NFSボリュームの場合）
スペースギャランティスタイル	なし
UNIX 権限（ NFS のみ）	777

+
を参照してください "ONTAP _ volume create _のマニュアルページ" これらの属性については、を参照してください。

システムデータ用の内蔵ディスク

ユーザデータ用のストレージに加えて、BlueXPはシステムデータ用のクラウドストレージも購入します。

AWS

- ノードあたり 3 本のディスクで、ブート、ルート、コアの各データに対応：

- ブートデータ用に 45GiB io1 ディスク
- ルートデータ用に 140GiB GP3 ディスク
- コアデータ用に 540GiB GP2 ディスク

- 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

  スナップショットは、リブート時に自動的に作成されます。

- 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 8GiB です
- 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。

AWS では、 NVRAM はブートディスクにあります。

Azure （シングルノード）

- Premium SSD ディスク × 3 ：
  - ブートデータ用に 10 GiB のディスクを 1 台
  - ルートデータ用に 140GiB のディスクが 1 つ
  - NVRAM 用に 512GiB ディスクが 1 本必要です

    Cloud Volumes ONTAP 用に選択した仮想マシンでウルトラ SSD がサポートされている場合、システムは Premium SSD ではなく 32GiB Ultra SSD を NVRAM に使用します。

- コアを節約するために 1024 GiB の標準 HDD ディスクを 1 台
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot
- Azureのデフォルトでは、すべてのディスクが保存データとして暗号化されます。

Azure （ **HA** ペア）

ページ**BLOB**を使用した**HA**ペア

- ブートボリューム用の 10GiB Premium SSD ディスク × 2 （ノードごとに 1 つ）
- ルート用の 140 GiB 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 1024 GiB の標準 HDD ディスク 2 台 （ノードごとに 1 つ）
- NVRAM 用 512GiB Premium SSD ディスク × 2 （各ノードに 1 つ）
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot

  スナップショットは、リブート時に自動的に作成されます。

- Azureのデフォルトでは、すべてのディスクが保存データとして暗号化されます。

複数のアベイラビリティゾーンに含まれる**HA**ペア

- ブートボリューム用の 10GiB Premium SSD ディスク × 2 （ノードごとに 1 つ）
- 512 GiB Premium Storage 2ページのrootボリューム用blob（ノードごとに1つ）
- コアを節約するために 1024 GiB の標準 HDD ディスク 2 台 （ノードごとに 1 つ）
- NVRAM 用 512GiB Premium SSD ディスク × 2 （各ノードに 1 つ）
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot

  スナップショットは、リブート時に自動的に作成されます。

- Azureのデフォルトでは、すべてのディスクが保存データとして暗号化されます。

Google Cloud （シングルノード）

- ブートデータ用の 10GiB SSD 永続ディスク × 1
- ルートデータ用に 64GiB SSD パーシステントディスクが 1 本
- NVRAM 用に 500GiB SSD 永続ディスクが 1 本
- コアを節約するための 315 GiB 標準永続ディスク 1 台
- ブートデータとルートデータ用の Snapshot

  スナップショットは、リブート時に自動的に作成されます。

- ブートディスクとルートディスクはデフォルトで暗号化されています。

Google Cloud （ **HA** ペア）

- ブートデータ用の 2 本の 10GiB SSD 永続ディスク
- 64 GiB SSD の 4 本の永続的ディスクをルートデータ用に使用
- NVRAM 用に 500GiB の SSD 永続ディスクが 2 本搭載されています
- コアを節約するための 2 つの 315 GiB 標準パーシステントディスク
- メディエーターデータ用の 10GiB 標準永続ディスクが 1 本
- メディエーターのブートデータ用の10GiB標準永続ディスクが1本
- ブートデータとルートデータ用の Snapshot

  スナップショットは、リブート時に自動的に作成されます。

- ブートディスクとルートディスクはデフォルトで暗号化されています。

ディスクが存在する場所

BlueXPでは'次のようにストレージが配置されます

- 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。

知識とサポート

サポートに登録します

BlueXPとそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダのファイルサービスでNetAppのサポートは有効になりません。クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

サポート登録の概要

サポート資格を有効にする登録には、次の2つの形式があります。

- BlueXPアカウントIDサポートサブスクリプションの登録(BlueXPの[サポートリソース]ページにある20桁の960xxxxxxxxシリアル番号)。

  これは、BlueXP内のすべてのサービスのシングルサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポート契約が登録されている必要があります。

- クラウドプロバイダのマーケットプレイスでのサブスクリプションに関連付けられているCloud Volumes ONTAP のシリアル番号を登録している（909201xxxxxxxxのシリアル番号）。

  これらのシリアル番号は、通常PAY_GOシリアル番号と呼ばれ、Cloud Volumes ONTAP の導入時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録することで、サポートチケットのオープンやケースの自動生成などの機能を利用できます。登録を完了するには、以下の手順でNetApp Support Site（NSS）アカウントをBlueXPに追加してください。

NetAppサポートにBlueXPアカウントを登録します

サポートに登録してサポート利用資格をアクティブ化するには、BlueXPアカウントの1人のユーザがNetApp Support SiteアカウントをBlueXPログインに関連付ける必要があります。ネットアップサポートへの登録方法は、NetApp Support Site （NSS）アカウントがあるかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

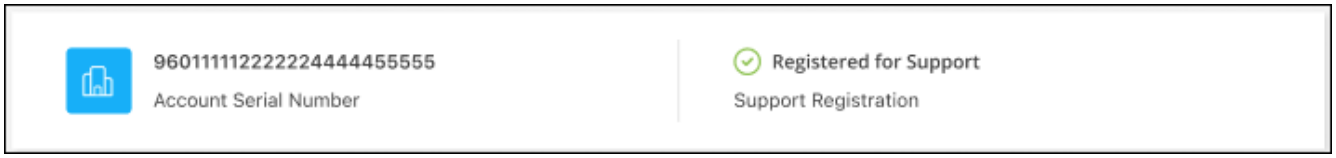
NSSアカウントをお持ちのネットアップのお客様は、BlueXPからサポートに登録するだけで済みます。

手順

1. BlueXPコンソールの右上で、[設定]アイコンを選択し、*[クレデンシャル]*を選択します。

2. [ユーザクレデンシャル]*を選択します。
3. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site（NSS）認証プロンプトに従います。
4. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

   [リソース]ページに、アカウントがサポートに登録されていることが表示されます。



   他のBlueXPユーザにNetApp Support Siteアカウントが関連付けられていない場合、このサポート登録ステータスは表示されません。ただし、BlueXPアカウントがサポートに登録されていないわけではありません。アカウント内の1人のユーザーがこれらの手順を実行している限り、アカウントは登録されています。

NSSアカウントを持たない既存のお客様

NetAppの既存のお客様で、ライセンスとシリアル番号は_NO_NSSアカウントしかお持ちでない場合は、NSSアカウントを作成してBlueXPログインに関連付ける必要があります。

手順

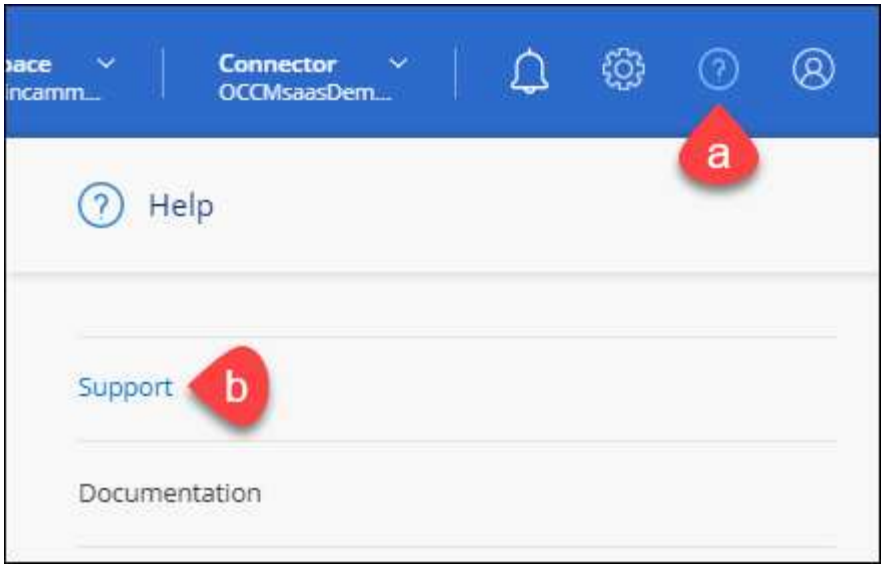
1. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. 必ず、上記のシリアル番号フィールドに使用されているBlueXPアカウントのシリアル番号(960xxxx)をコピーしてください。これにより、アカウント処理が高速化されます。
2. の手順を実行して、新しいNSSアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

ネットアップのソリューションを初めて導入する場合は

ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

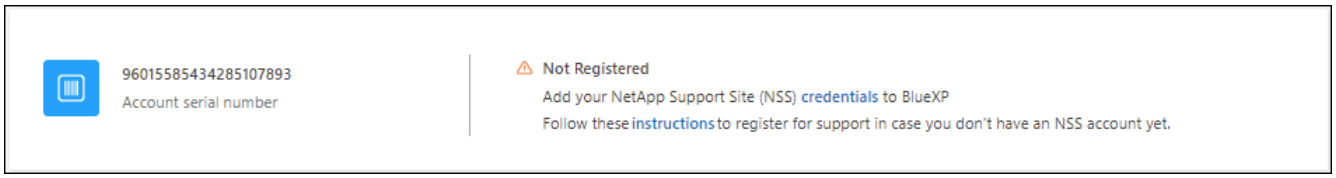
手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

2. サポート登録ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. に移動します "ネットアップサポート登録サイト" 「ネットアップ登録のお客様ではありません」を選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line ）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを選択します。
6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

   この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

   確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. を実行してNetApp Support Site アカウントを作成します "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

完了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetApp Support Siteアカウントを作成したら、の手順を実行してアカウントをBlueXPログインに関連付けます NSSアカウントをお持ちの既存のお客様。

Cloud Volumes ONTAPサポートのためにNSSクレデンシャルを関連付けます

NetApp Support Siteで次の主要なワークフローを有効にするには、BlueXPアカウントにクレデンシャルを関連付ける必要がCloud Volumes ONTAPあります。

- 従量課金制のCloud Volumes ONTAPシステムのサポートを登録しています

  お使いのシステムのサポートを有効にし、ネットアップのテクニカルサポートリソースにアクセスするには、 NSS アカウントを用意する必要があります。

- お客様所有のライセンスを使用（BYOL）する場合のCloud Volumes ONTAP の導入

  ライセンスキーをBlueXPでアップロードし、購入した契約期間のサブスクリプションを有効にするには、NSSアカウントを提供する必要があります。これには、期間の更新の自動更新も含まれます。

- Cloud Volumes ONTAP ソフトウェアを最新リリースにアップグレードしています

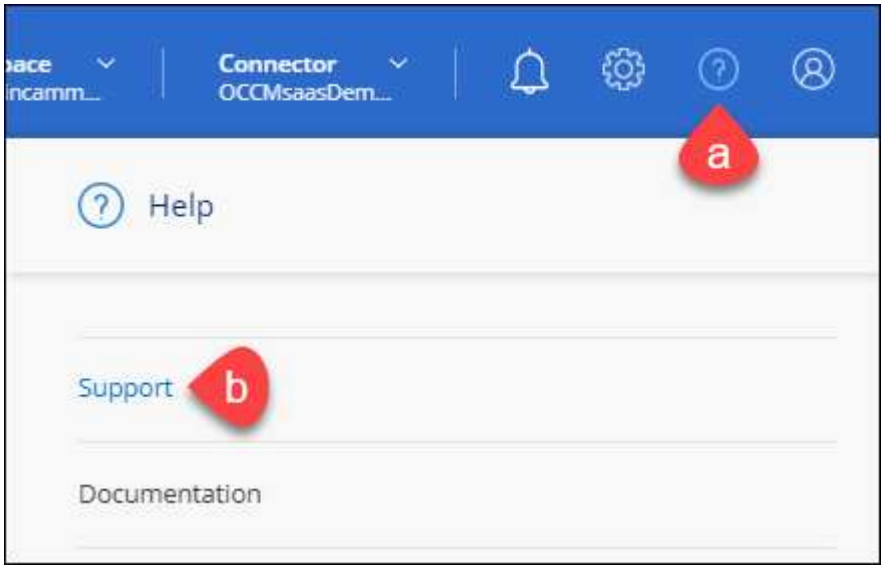
NSSクレデンシャルをBlueXPアカウントに関連付ける方法は、BlueXPユーザログインに関連付けられたNSSアカウントとは異なります。

これらのNSSクレデンシャルは、特定のBlueXPアカウントIDに関連付けられています。BlueXPアカウントに属するユーザは、*[サポート]>[NSS管理]*からこれらのクレデンシャルにアクセスできます。

- お客様レベルのアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することもできます。
- パートナーアカウントまたはリセラーアカウントをお持ちの場合は、1つ以上のNSSアカウントを追加することはできますが、お客様レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上で、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [NSS Management]>[Add NSS Account]*を選択します。
3. プロンプトが表示されたら、*続行*を選択してMicrosoftログインページにリダイレクトします。

   NetAppでは、サポートとライセンスに固有の認証サービスのIDプロバイダとしてMicrosoftエントラIDを使用します。

4. ログインページで、NetApp Support Siteの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

   これらのアクションにより、BlueXPはライセンスのダウンロード、ソフトウェアのアップグレード検証、および将来のサポート登録などの目的でNSSアカウントを使用できます。

   次の点に注意してください。

   - NSSアカウントは、お客様レベルのアカウントである必要があります（ゲストアカウントや一時アカウントではありません）。複数のお客様レベルのNSSアカウントを設定できます。
   - NSSアカウントがパートナーレベルのアカウントの場合、作成できるNSSアカウントは1つだけです。お客様レベルのNSSアカウントを追加しようとすると、パートナーレベルのアカウントが存在する場合は、次のエラーメッセージが表示されます。

     「別のタイプのNSSユーザーがすでに存在するため、このアカウントではNSS顧客タイプは許可されていません。」

   既存のお客様レベルのNSSアカウントがあり、パートナーレベルのアカウントを追加しようとする場合も同様です。

   - ログインに成功すると、ネットアップはNSSのユーザ名を保存します。

     これはシステムによって生成されたIDで、電子メールにマッピングされます。[**NSS Management**]ページで、から電子メールを表示できます ••• メニュー。

   - ログイン認証情報トークンを更新する必要がある場合は、の[認証情報の更新*]オプションも使用できます ••• メニュー。

     このオプションを使用すると、再度ログインするように求められます。これらのアカウントのトークンは90日後に期限切れになります。このことを通知する通知が投稿されます。

ヘルプを表示します

ネットアップでは、BlueXPとその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（ KB ）記事やコミュニティフォーラムなど、 24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、 Web チケット処理によるリモートテクニカルサポートが含まれます。

クラウドプロバイダのファイルサービスのサポート

クラウドプロバイダのファイルサービスとそのインフラ、またはサービスを使用する解決策に関連するテクニカルサポートについては、該当する製品のBlueXPドキュメントの「困ったときは」を参照してください。

- "ONTAP 対応の Amazon FSX"
- "Azure NetApp Files の特長"
- "Cloud Volumes Service for Google Cloud"

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、以下に記載されているサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、 1 日 24 時間、週 7 日間無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPのマニュアル。

- "ナレッジベース"

  BlueXPナレッジベースで問題のトラブルシューティングに役立つ記事を検索します。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりできます。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

- [ケースの作成]*機能を使用するには、最初にNetApp Support SiteクレデンシャルをBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられているクレデンシャルの管理方法について説明します"。
- シリアル番号のあるONTAPシステムのケースをオープンする場合は、そのシステムのシリアル番号にNSSアカウントを関連付ける必要があります。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [**Resources**]ページで、[Technical Support]で次のいずれかのオプションを選択します。

   a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。

   b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。

      - **Service**:問題 が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能を備えたテクニカルサポート問題 に固有のBlueXPなどです。
      - 作業環境：ストレージに該当する場合は、* Cloud Volumes ONTAP *または*オンプレミス*を選択し、関連する作業環境を選択します。

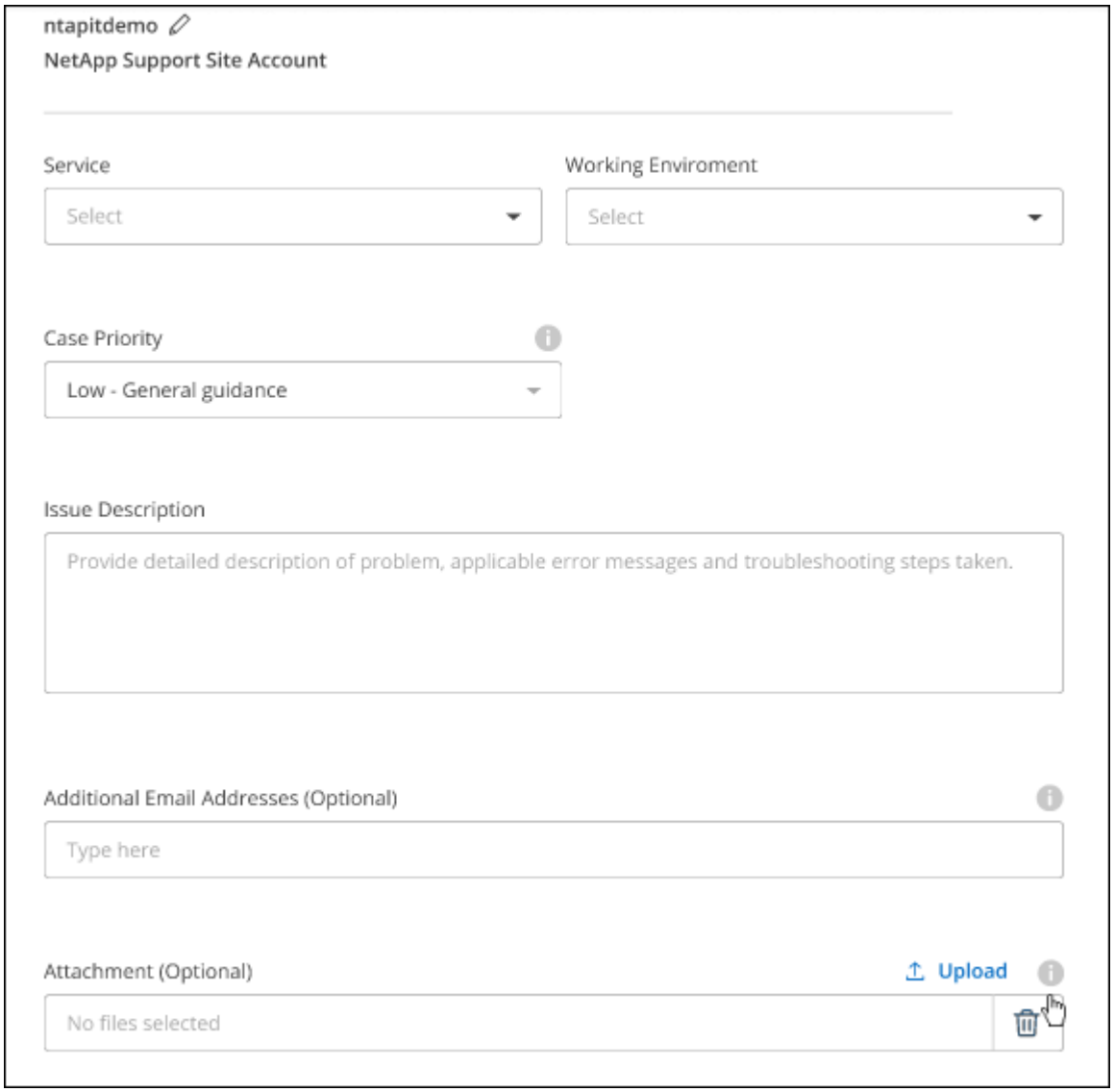
作業環境のリストは、サービスの上部バナーで選択したBlueXPアカウント、ワークスペース、コネクタの範囲内にあります。

- ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

  これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

- *事象の説明 *：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要 を入力します。
- その他のメールアドレス：この問題 を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
- 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

  添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。



完了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。 右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSSアカウントとそれに関連付けられているレコードの会社が、BlueXPアカウントのシリアル番号(例960xxxx）または動作環境のシリアル番号。次のいずれかのオプションを使用して、サポートを受けることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースをに送信します https://mysupport.netapp.com/site/help

サポートケースの管理（プレビュー）

アクティブなサポートケースと解決済みのサポートケースは、BlueXPから直接表示および管理できます。NSSアカウントと会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
  - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
  - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

  テーブルの結果には、選択したビューに関連するケースが反映されます。
- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

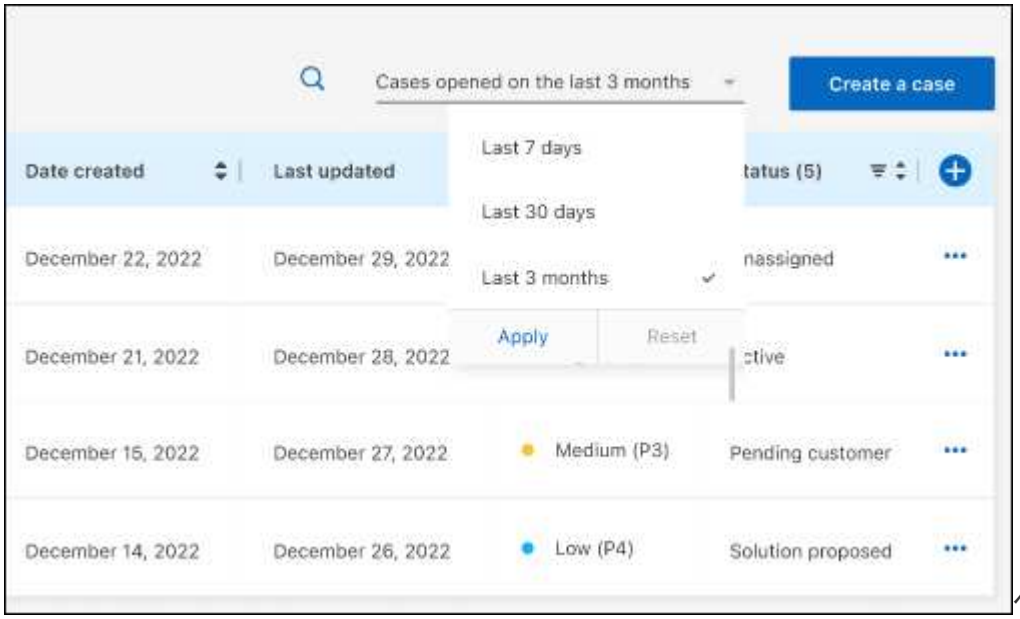
  詳細については、以下の手順を参照してください。
- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

手順

1. BlueXPで、*[ヘルプ]>[サポート]*を選択します。
2. [ケース管理]*を選択し、プロンプトが表示されたらNSSアカウントをBlueXPに追加します。

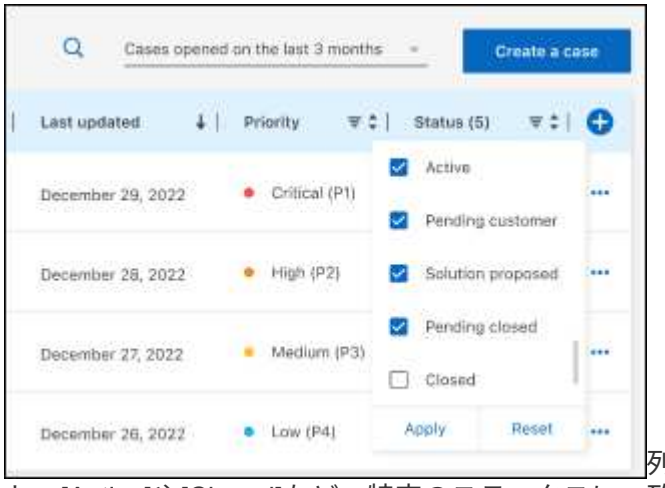
   ケース管理*ページには、BlueXPユーザアカウントに関連付けられたNSSアカウントに関連するオープンケースが表示されます。これは、* NSS管理*ページの上部に表示されるNSSアカウントと同じです。

3. 必要に応じて、テーブルに表示される情報を変更します。
   - [Organization's Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。



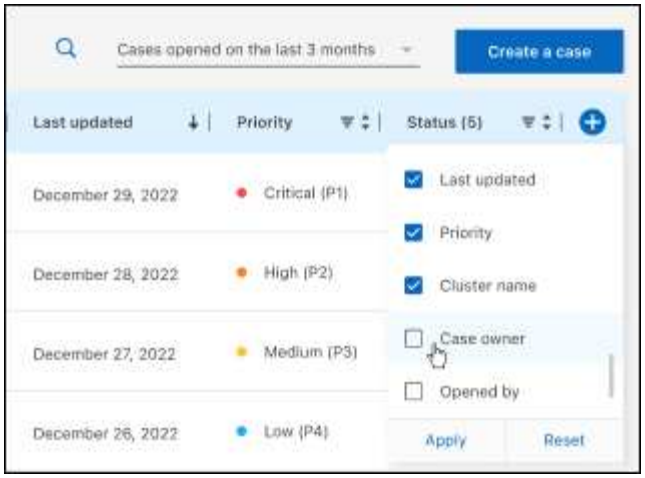
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

   - 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

   - テーブルに表示される列を変更するには、 次に、表示する列を選択します。

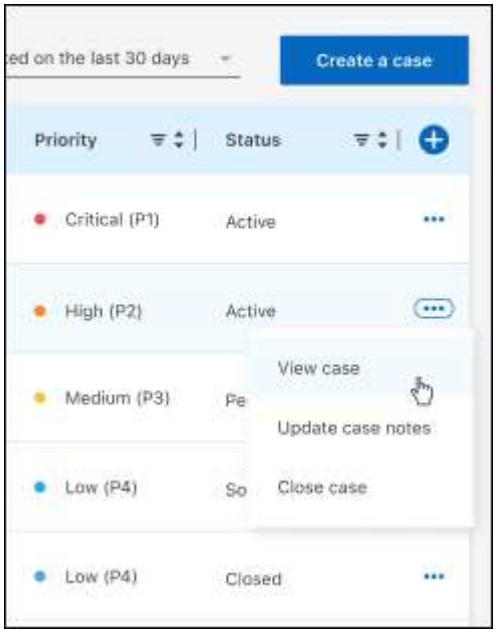


4. 既存のケースを管理するには、 ••• 使用可能なオプションのいずれかを選択します。

   - ケースの表示:特定のケースの詳細を表示します。
   - ケースノートの更新：問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

     添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。

   - ケースをクローズ：ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



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

"https://www.netapp.com/company/legal/copyright/"

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。

"https://www.netapp.com/company/legal/trademarks/"

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/pdf.html?item=/media/11887-patentspage.pdf

プライバシーポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

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。

- "BlueXPに関する注意事項"
- "Cloud Volumes ONTAP メディエーターに関する通知"
- "ONTAP に関する注意"

著作権に関する情報

商標に関する情報