Cloud Volumes ONTAP を使用します

Cloud Volumes ONTAP

NetApp
May 28, 2024

目次

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。

> BlueXPで管理される製品とサービスの実際の使用量と計測値は常にGiBとTiBで計算されますが、GB / GiBとTB / TiBという用語は同じ意味で使用されます。これは、クラウドマーケットプレイスのリスト、価格見積もり、リストの説明、およびその他の関連ドキュメントに反映されます。

"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

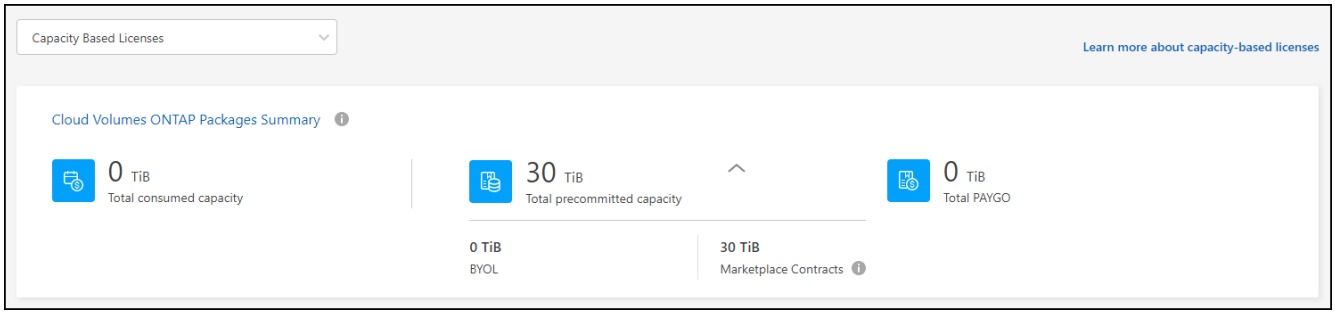
1. BlueXPナビゲーションメニューから、* Governance > Digital Wallet *を選択します。
2. Cloud Volumes ONTAP タブで、 Capacity Based Licenses *を選択したままにします。
3. パッケージの概要を確認します。この概要には、消費容量、事前コミット済み容量の合計、従量課金制の合計容量が表示されます。

    - 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。



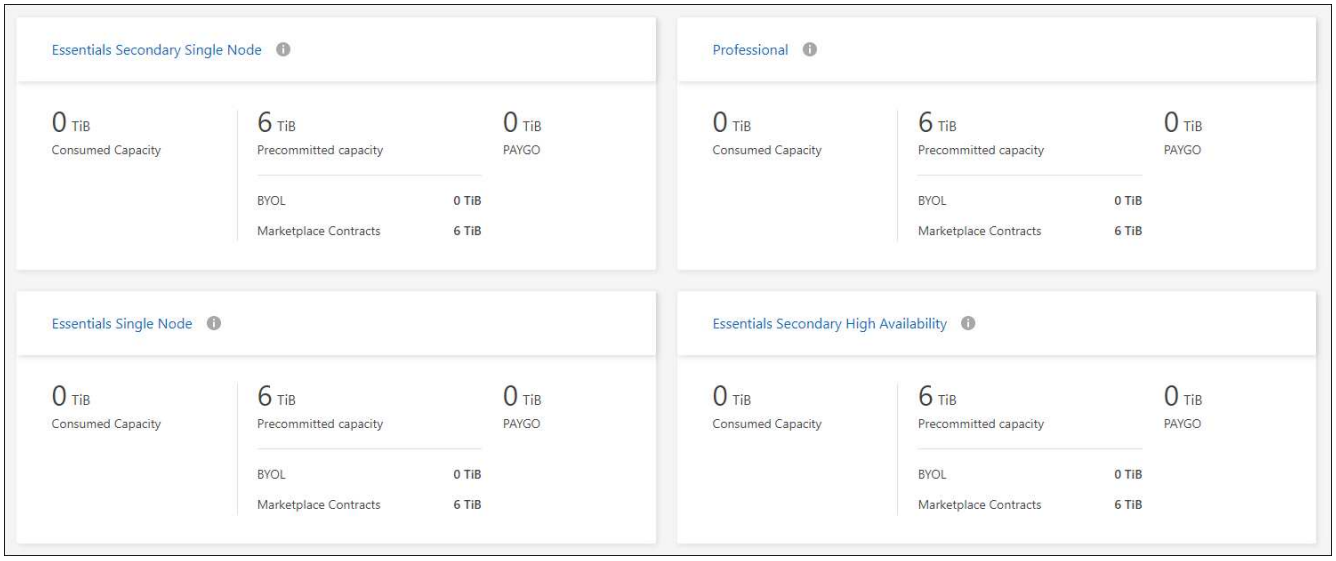
4. ライセンスパッケージごとの使用済み容量を表示します。

- 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"。

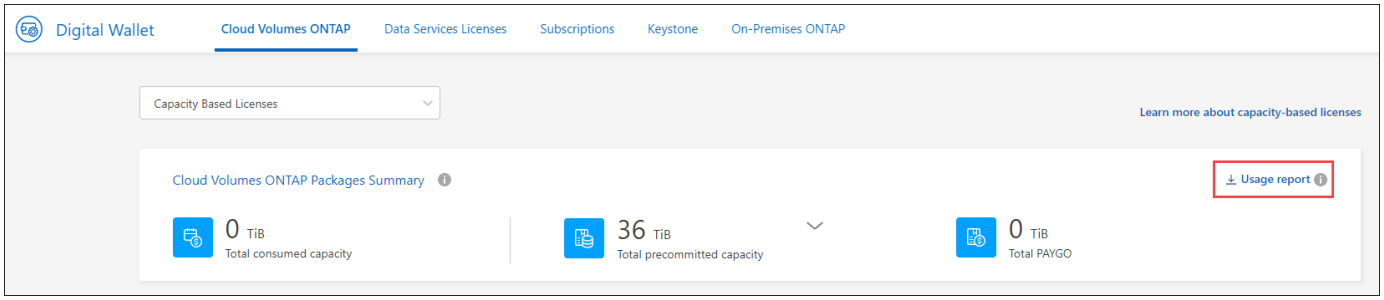
- _推奨容量_は、ネットアップから購入したライセンス容量（BYOLまたはマーケットプレイス契約）です。
  - _BYOL_このパッケージタイプに対してネットアップから購入したライセンス容量を表示します。
  - _Marketplace契約_このパッケージタイプのマーケットプレイス契約で購入したライセンス容量を表示します。
- _PAYGO_ライセンス消費モデル別の消費容量を表示します。

  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ネットアップサポートサイト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* ）。

ライセンスファイルの取得方法の詳細については、を参照してください。 "システムライセンスファイルを取得します"。

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. [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は、 a_packag_ の形式で用意されています。Cloud Volumes ONTAP作業環境を作成するときは、ビジネスニーズに基づいて複数のライセンスパッケージから選択できます。作業環境の作成後にニーズが変わった場合は、パッケージをいつでも変更できます。たとえば、Essentialsパッケージか

らProfessionalパッケージに変更できます。

"容量単位のライセンスパッケージの詳細"。

このタスクについて

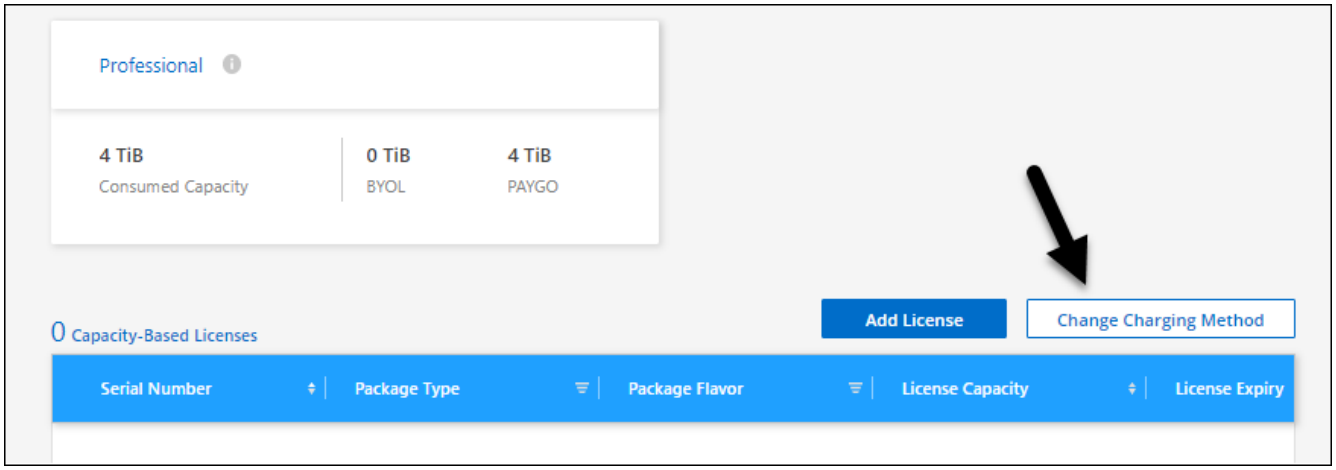
- 課金方法を変更しても、NetApp（BYOL）から購入したライセンスを使用して課金されるか、クラウドプロバイダのマーケットプレイスから購入したライセンスを使用して課金されるか（従量課金制）には影響しません。

  BlueXPは、常に最初にライセンスを請求しようとします。ライセンスが利用できない場合は、マーケットプレイスのサブスクリプションに対して課金されます。BYOLからMarketplaceへのサブスクリプション（またはその逆）では「変換」は必要ありません。

- 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。

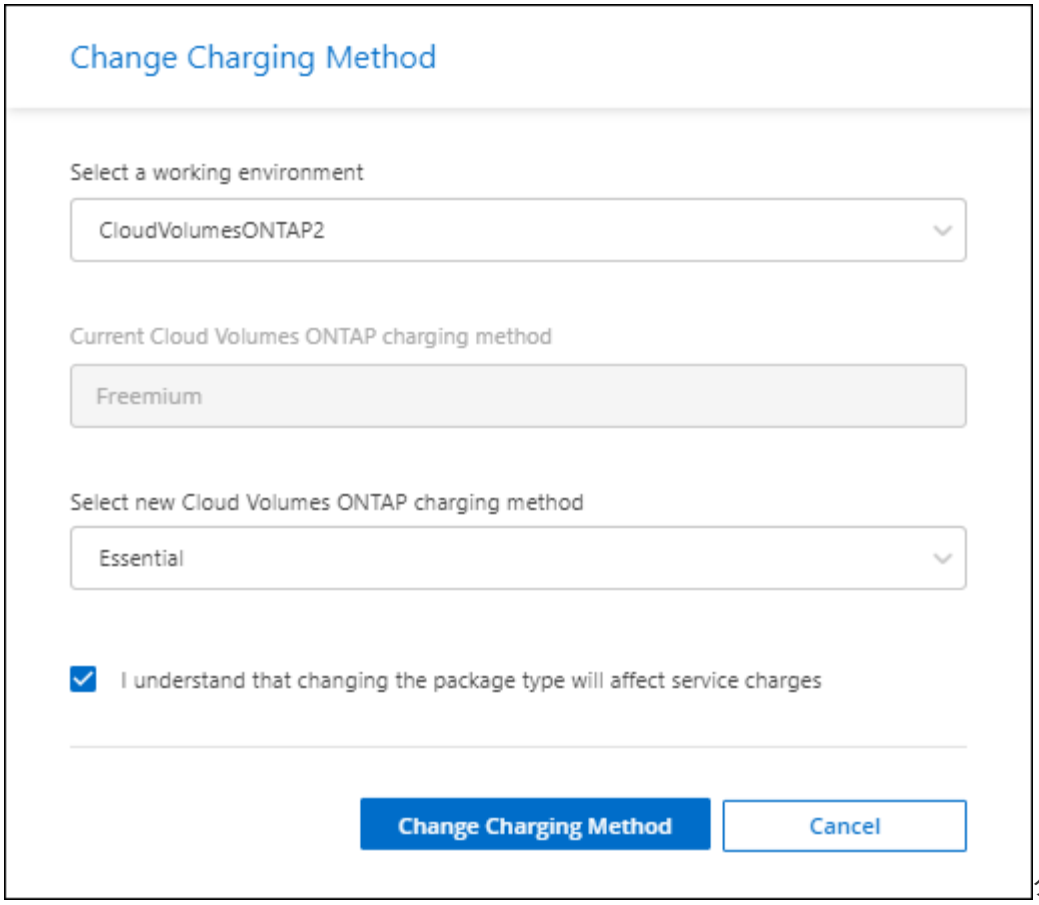
手順

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を管理

KeystoneサブスクリプションをBlueXPデジタルウォレットから管理するには、Cloud Volumes ONTAPで使用するサブスクリプションを有効にし、サブスクリプションのサービスレベルに応じてコミット済み容量の変更を要求します。サービスレベル用に容量の

追加を要求すると、オンプレミスのONTAPクラスタやCloud Volumes ONTAPシステム用に追加のストレージが提供されます。

NetApp Keystoneは、CAPEX（設備投資）やリースよりもOPEX（運用コスト）が望ましいお客様に、ハイブリッドクラウドエクスペリエンスを提供する、柔軟な従量課金制のサブスクリプションベースサービスです。

"Keystoneの詳細はこちら"

アカウントを承認します

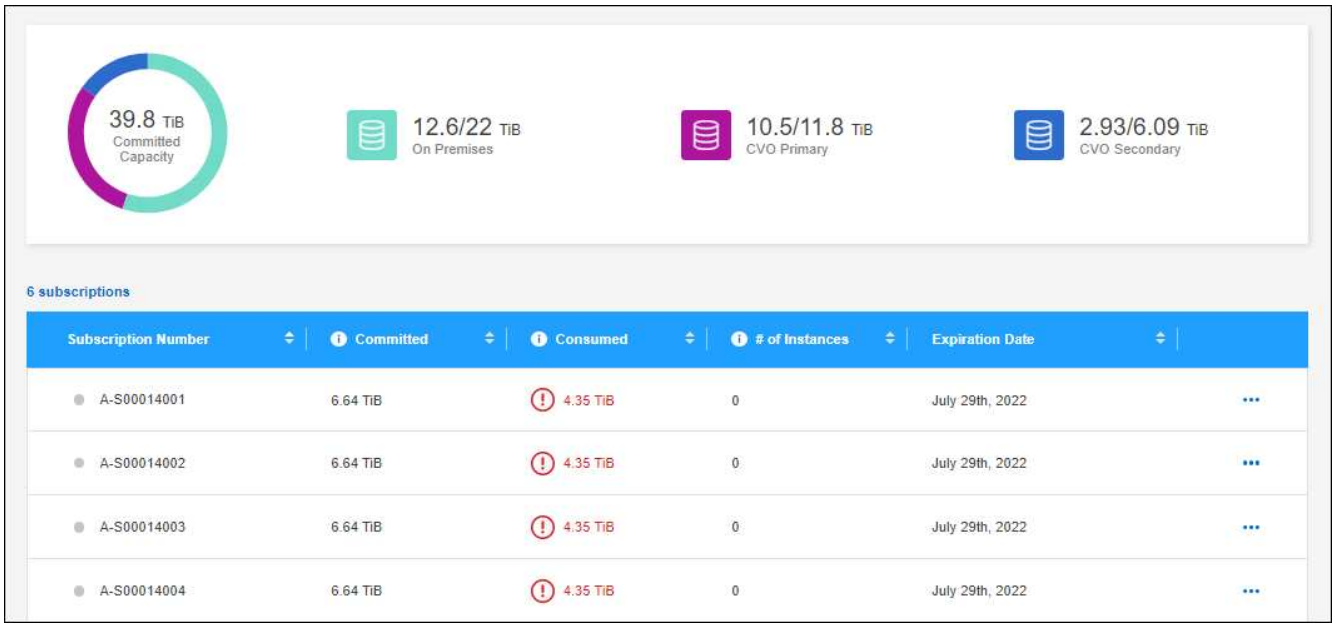
BlueXPでKeystoneサブスクリプションを使用および管理するには、NetAppに連絡して、KeystoneサブスクリプションでBlueXPユーザアカウントを承認する必要があります。

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。

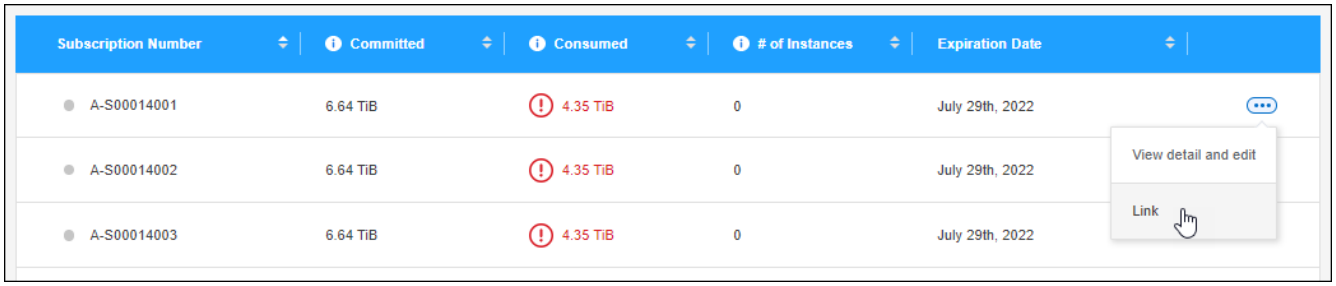


サブスクリプションをリンクします

NetAppがアカウントを承認したら、KeystoneサブスクリプションをCloud Volumes ONTAPで使用できるようにリンクできます。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

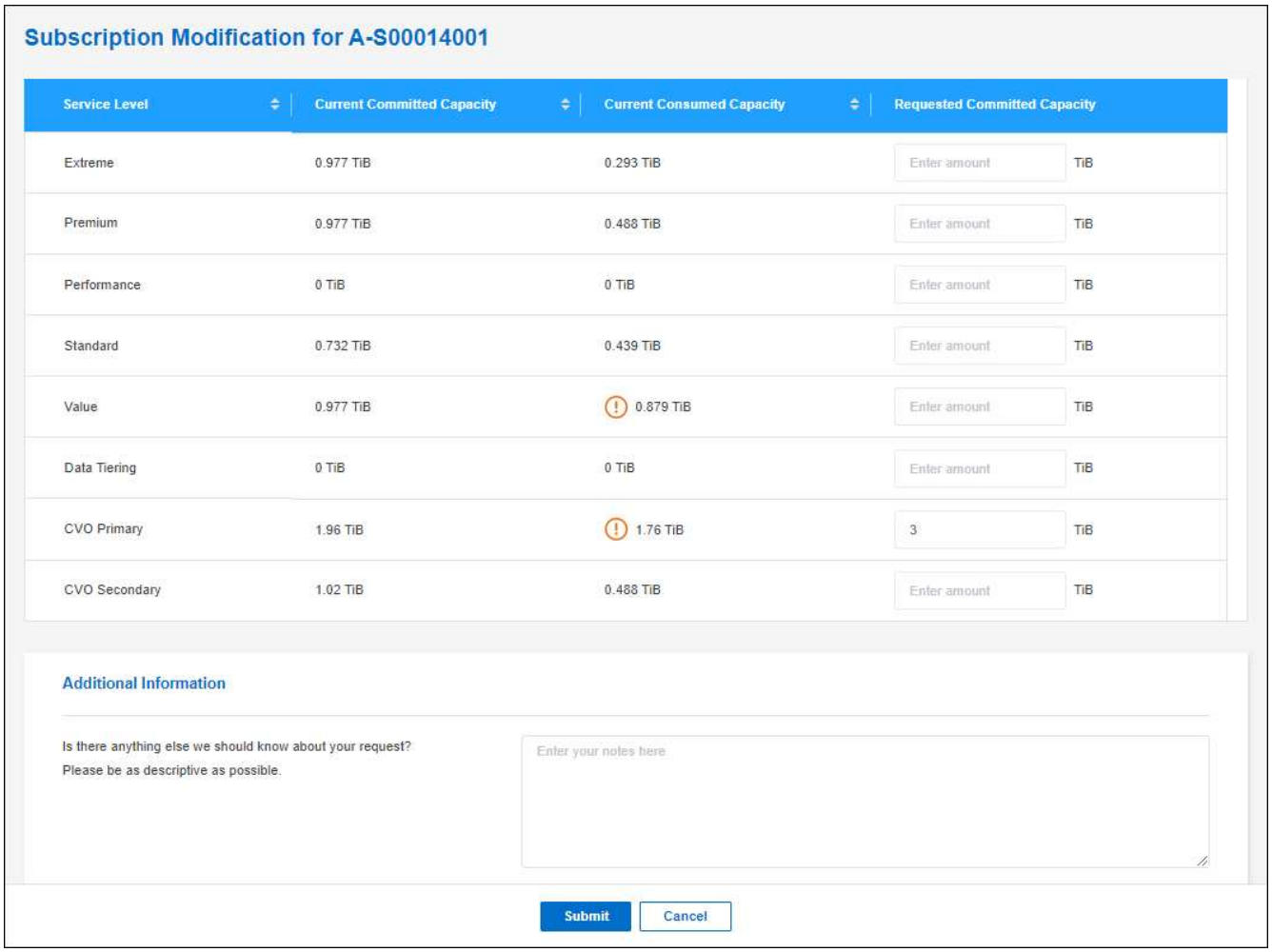
これで、サブスクリプションがBlueXPアカウントにリンクされ、Cloud Volumes ONTAP 作業環境の作成時に選択できるようになりました。

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サービスレベルのコミット済み容量を変更する場合は、BlueXPからNetAppに直接リクエストを送信できます。サービスレベル用に容量の追加を要求すると、オンプレミスクラスタやCloud Volumes ONTAPシステム用に追加のストレージが提供されます。

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. [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。

使用状況の監視

BlueXPデジタルアドバイザダッシュボードを使用すると、Keystoneサブスクリプションの使用状況を監視したり、レポートを生成したりできます。

"サブスクリプションの使用状況の監視の詳細"

サブスクリプションのリンクを解除します

BlueXP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。

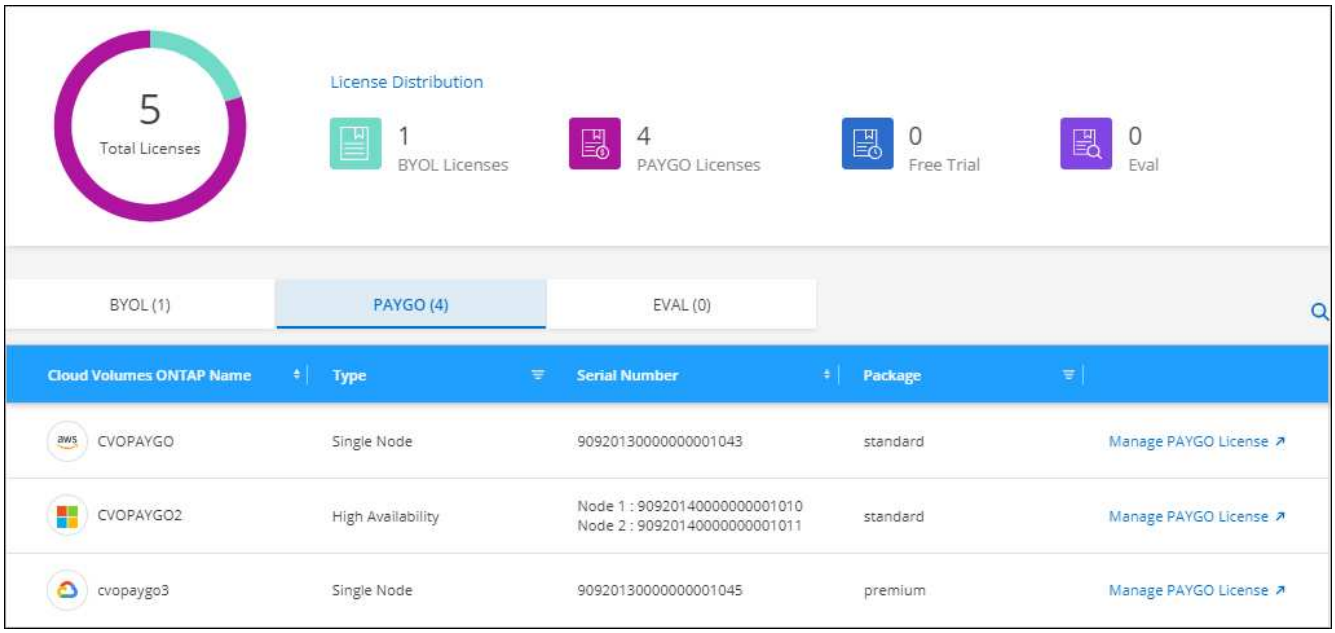
"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

PAYGO ライセンスを管理します

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。

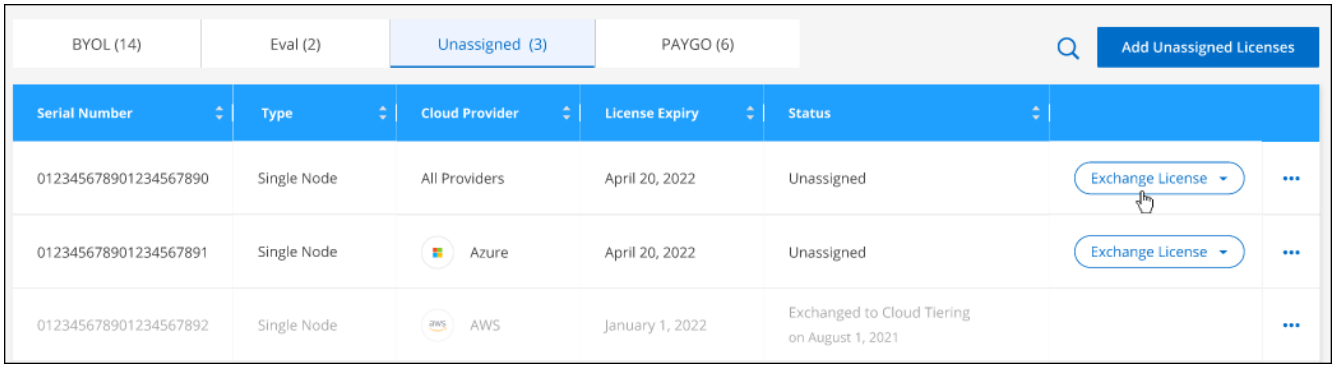
ライセンスを交換すると、 Cloud Volumes ONTAP ライセンスが取り消され、サービスのドル相当ライセンスが作成されます。

- 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

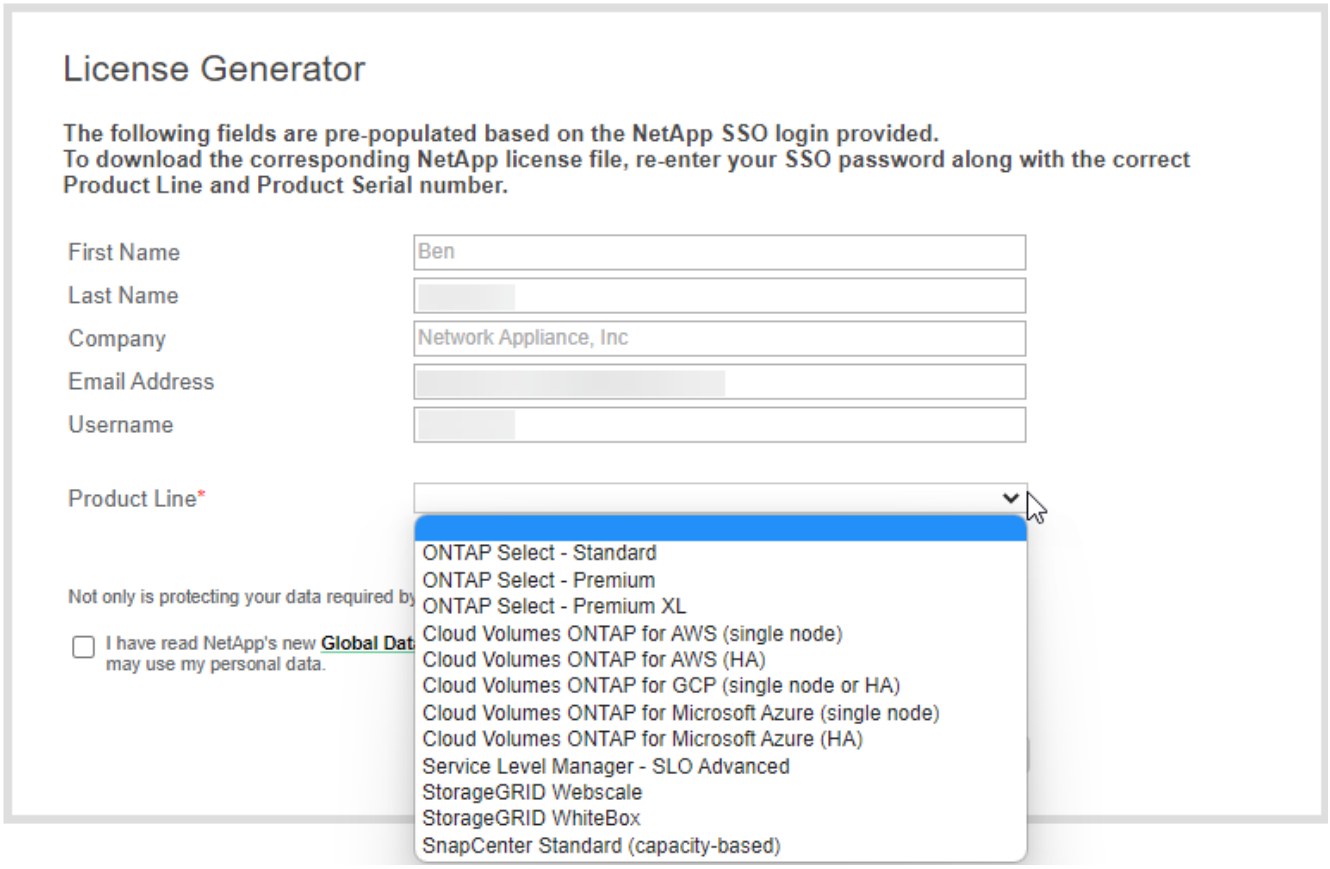
ほとんどの場合、NetApp Support Site アカウントを使用してライセンスファイルを自動的に取得できます。ただし、アップロードできない場合は、ライセンスファイルを手動でアップロードする必要があります。ライセンスファイルがない場合は、 netapp.com から入手できます。

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、ネットアップサポートサイトのクレデンシャルでログインします。

2. パスワードを入力し、製品を選択してシリアル番号を入力し、プライバシーポリシーを読み、同意したことを確認してから、 * Submit * をクリックします。

◦ 例 *



3. 電子メールまたは直接ダウンロードで serialnumber.nlf JSON ファイルを受信するかどうかを選択します。

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。
- 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
   特定のアグリゲート

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. * 詳細、保護、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。
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 169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.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。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
- 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。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-

objects#organizational_units["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

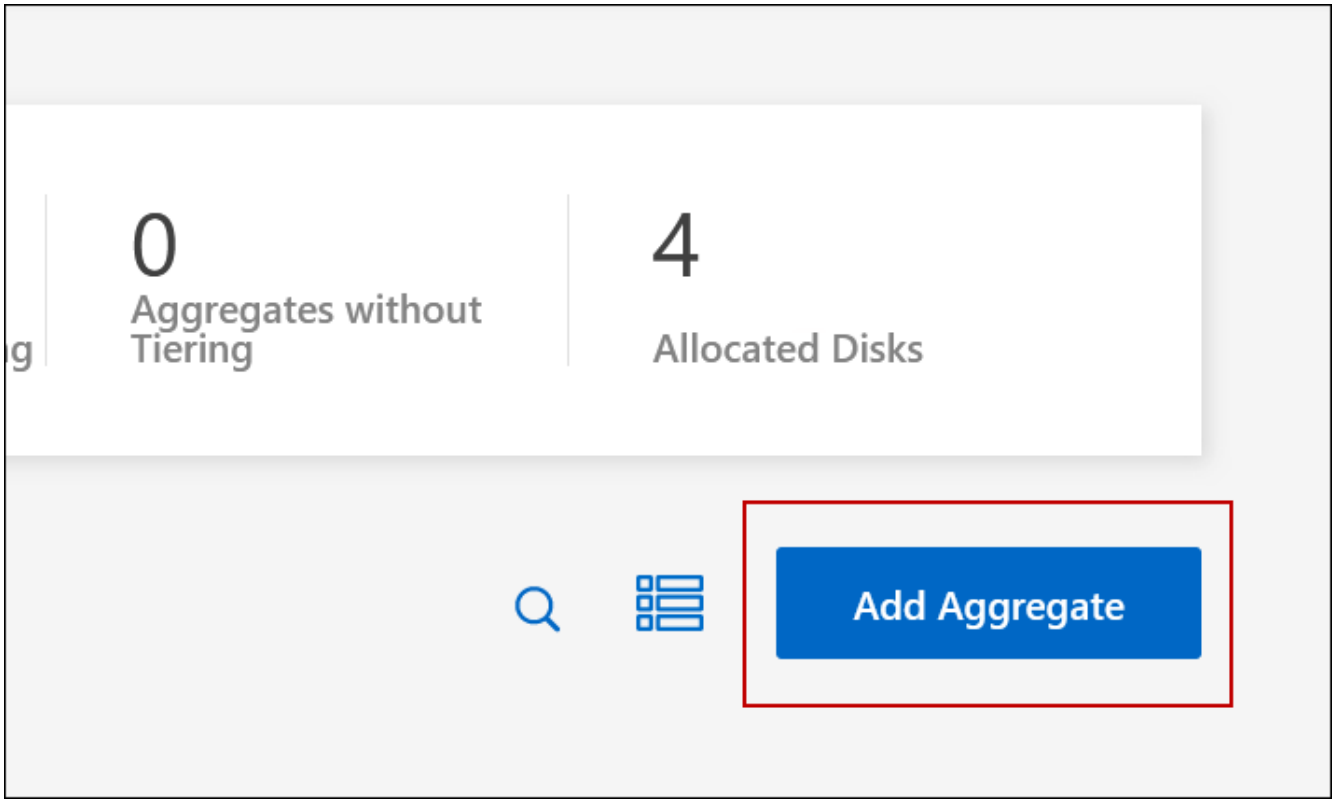
Cloud Volumes ONTAP システムにボリュームが作成されます。

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。

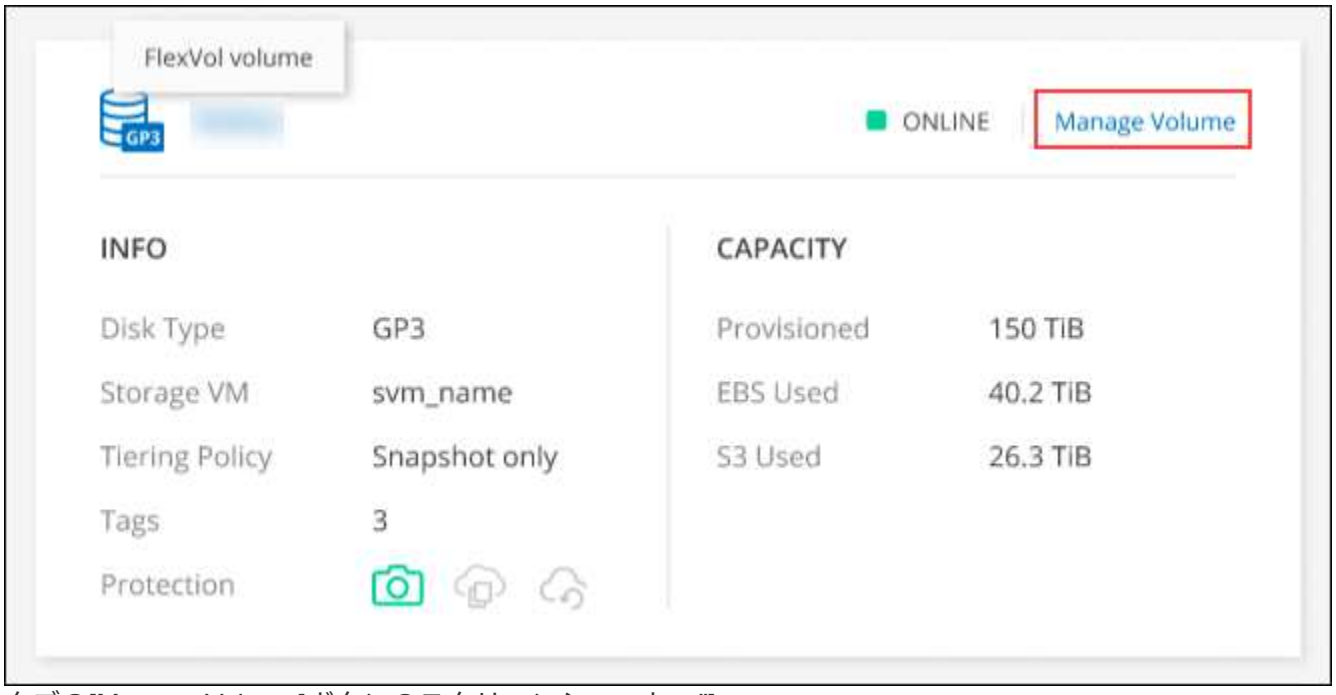
BlueXPの標準ビューまたはアドバンストビューでボリュームを管理できます。標準ビューには、ボリュームを変更するための一部のオプションが用意されています。高度なビューでは、クローニング、サイズ変更、ランサムウェア対策の設定変更、分析、保護、アクティビティの追跡、階層間でのボリュームの移動など、高度な管理が可能です。を参照してください "拡張ビューを使用してCloud Volumes ONTAP を管理します"。

ボリュームを管理します

BlueXPの標準ビューを使用すると、ストレージのニーズ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"。

タスク	アクション
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。
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。

タスク	アクション
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。

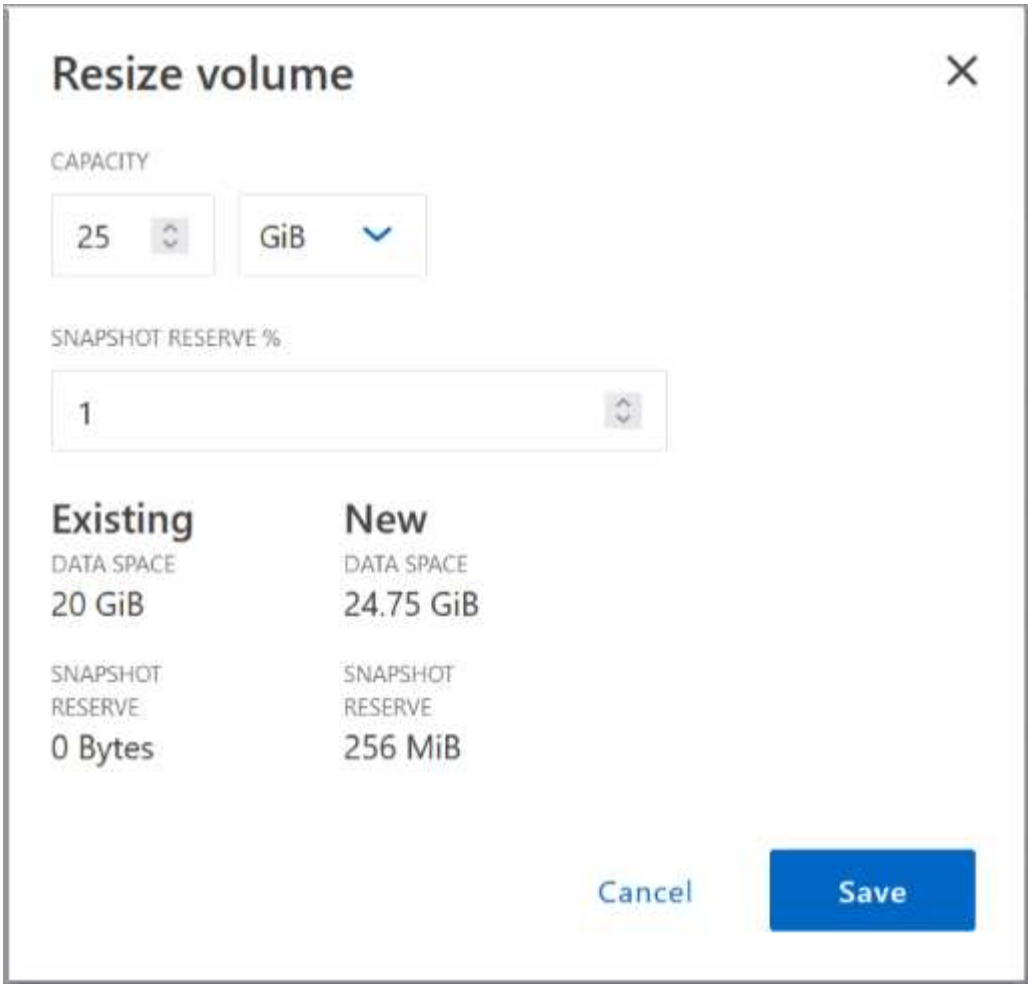
ボリュームのサイズを変更する

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、BlueXPのアドバンストビューで変更できます。

手順

1. System Managerを使用してボリュームのサイズを変更するには、アドバンストビューを開きます。を参照してください "開始方法"。
2. 左側のナビゲーションメニューで、*[ストレージ]>[ボリューム]*を選択します。
3. ボリュームのリストから、サイズを変更する必要があるボリュームを特定します。
4. オプションアイコンをクリックします。 。
5. [サイズ変更]*を選択します。
6. [ボリュームのサイズ変更]*画面で、必要に応じて容量とSnapshotリザーブの割合を編集します。使用可能な既存のスペースを変更後の容量と比較できます。
7. [保存（ Save ）] をクリックします。



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。

タスク	アクション
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、 CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（ SRV ）が含まれている必要があります。ifdef::gCP[] Google Managed Active Directoryを設定している場合、デフォルトで は、169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.169.254.6254のIPアドレスで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。
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。

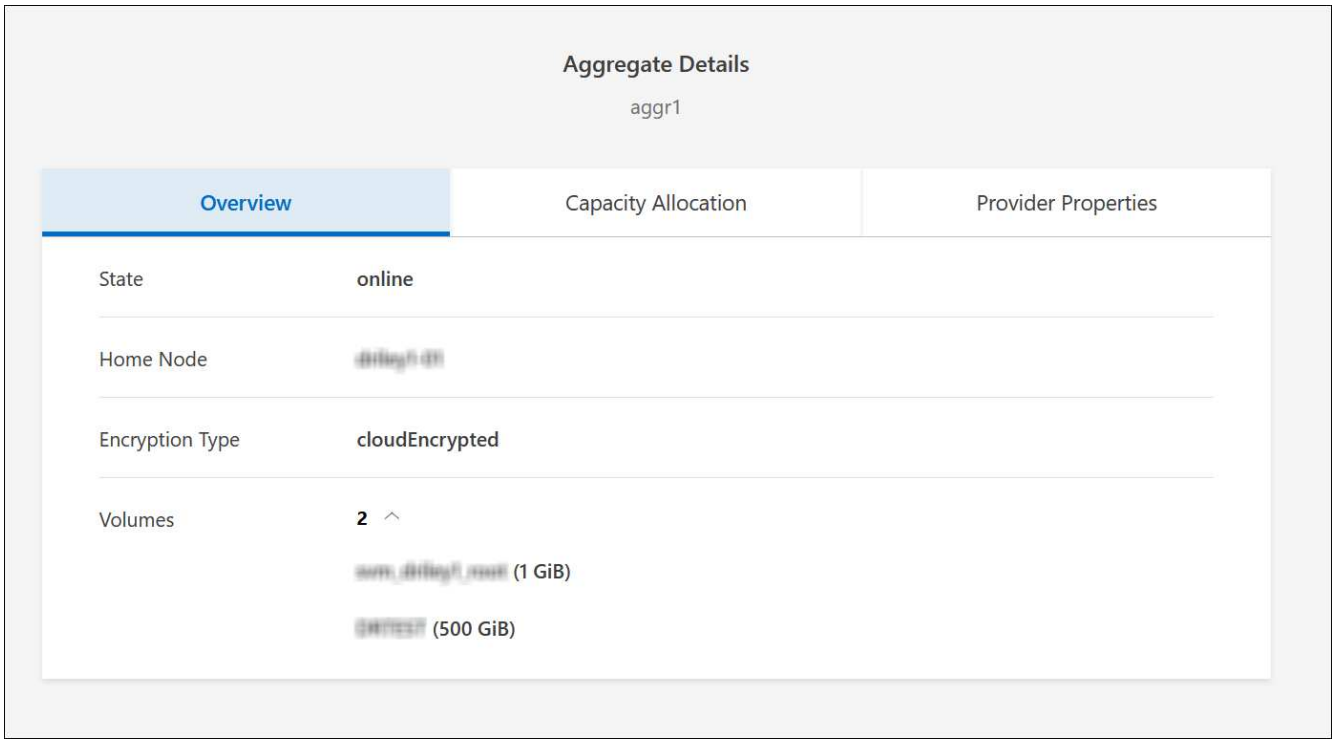
2. アグリゲートから移動する 1 つ以上のボリュームを指定します。

   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、 （省略記号アイコン）>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"。

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

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。

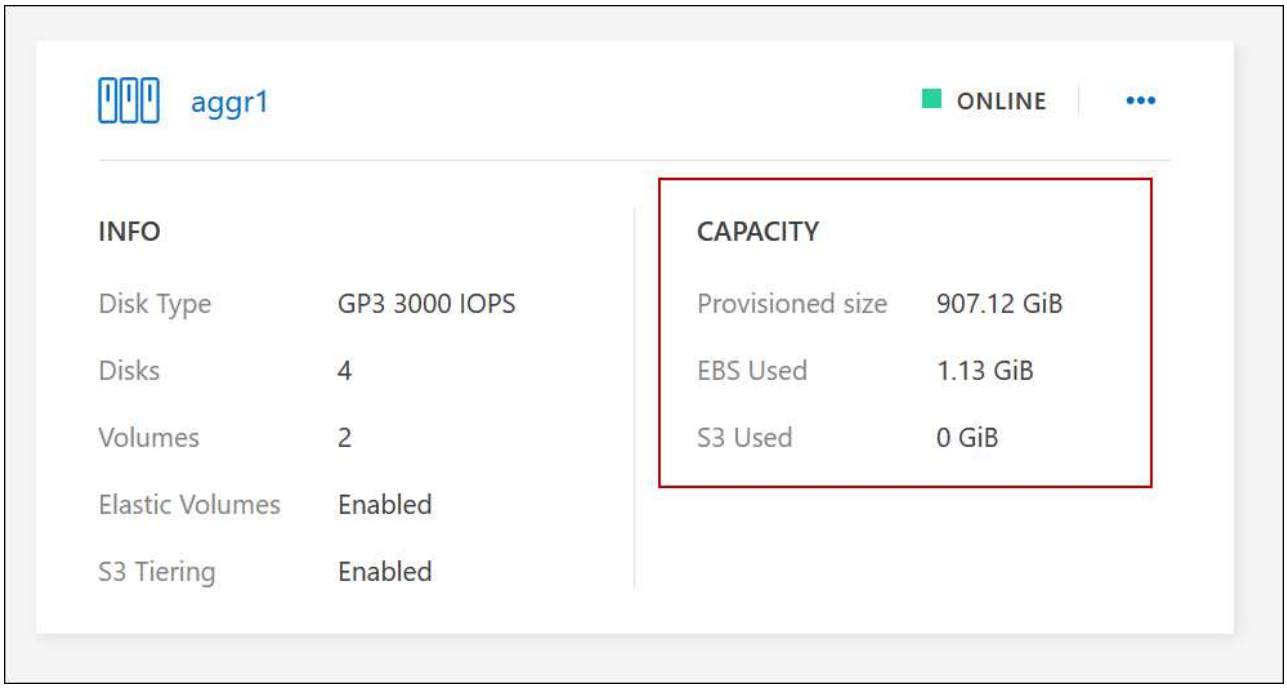
このタスクについて

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、 （省略記号アイコン）>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。 （省略記号アイコン）>[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。

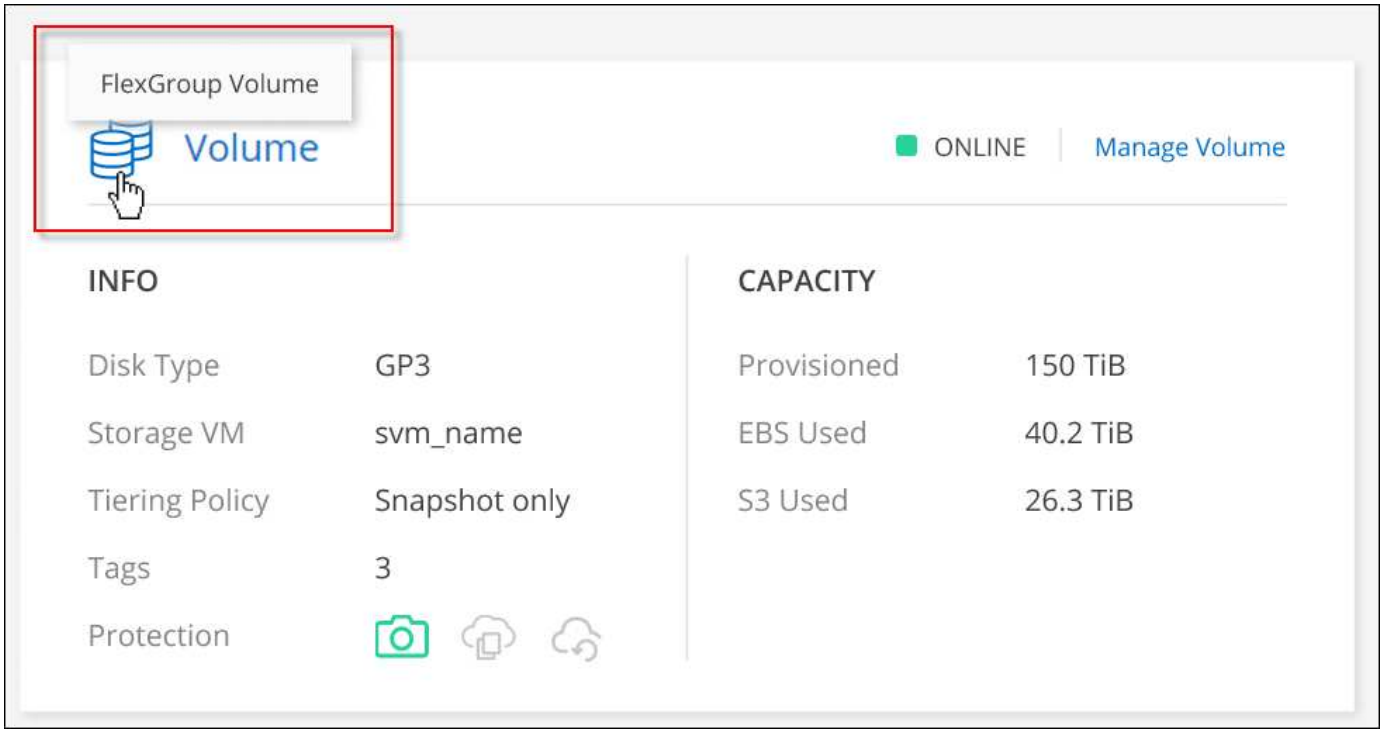
- ボリュームがクローンである。
- ボリュームがクローンの親です。
- ソースアグリゲートまたはデスティネーションアグリゲートには、スループットが最適化された HDD （ st1 ）が 1 本含まれています。
- いずれかのアグリゲートでオブジェクトに古い命名規則が使用されています。両方のアグリゲートで同じ名前形式を使用する必要があります。

  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。

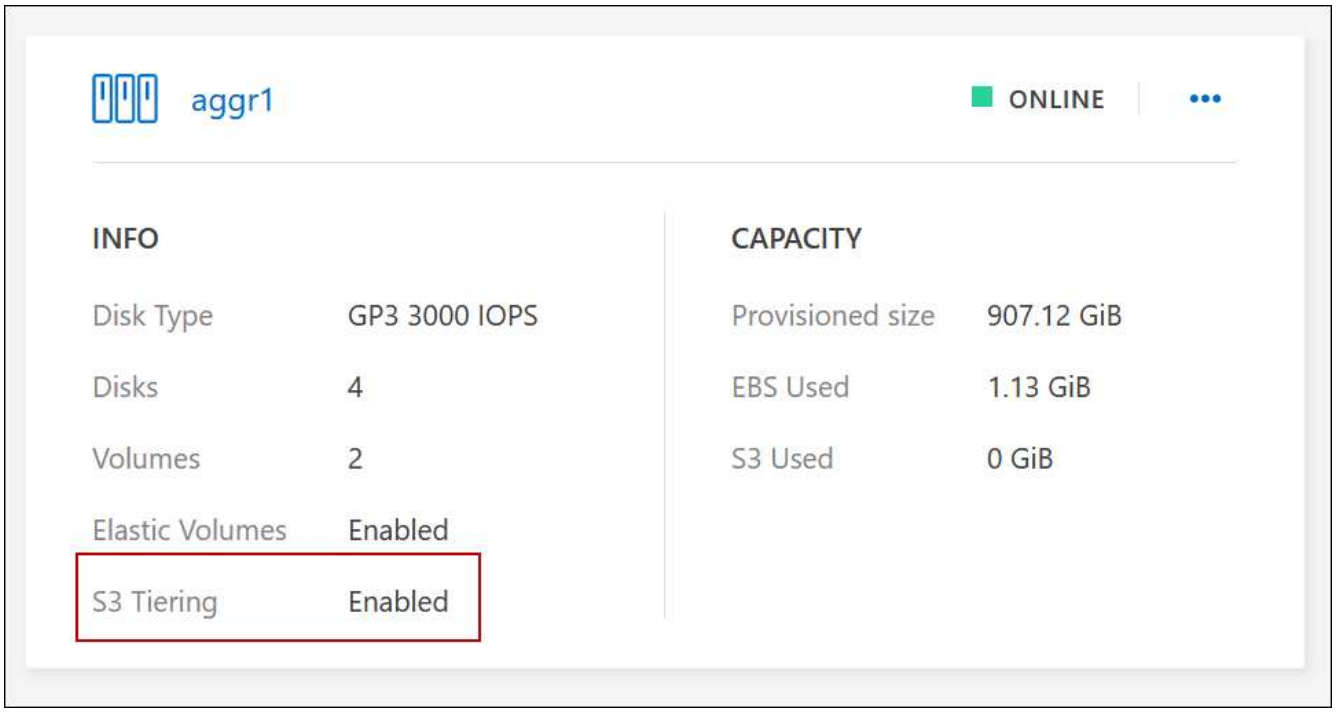
- * 既存のボリューム *

  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。

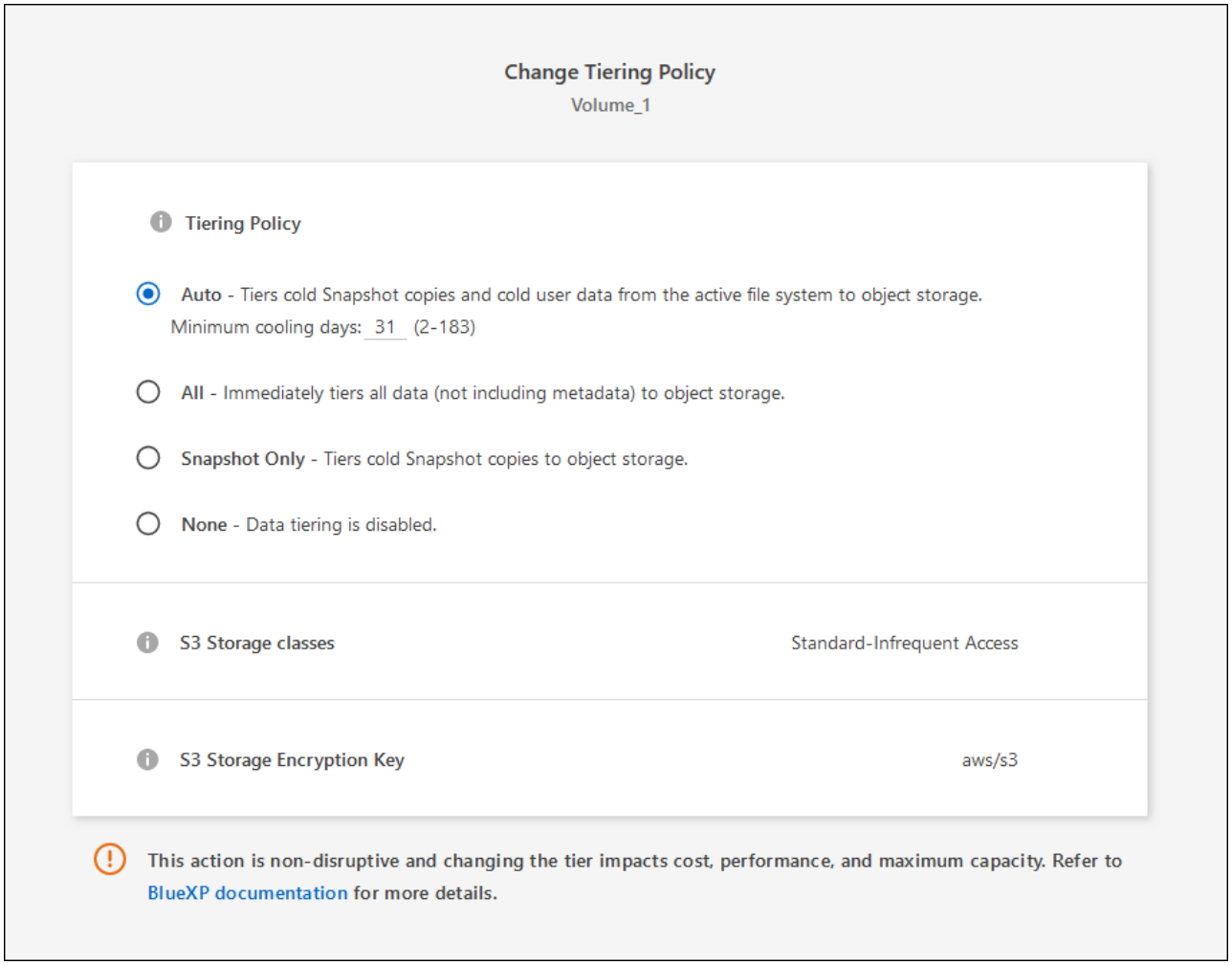
タスク	アクション
新しいボリュームを作成します	[新しいボリュームの追加] をクリックします。

タスク	アクション
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

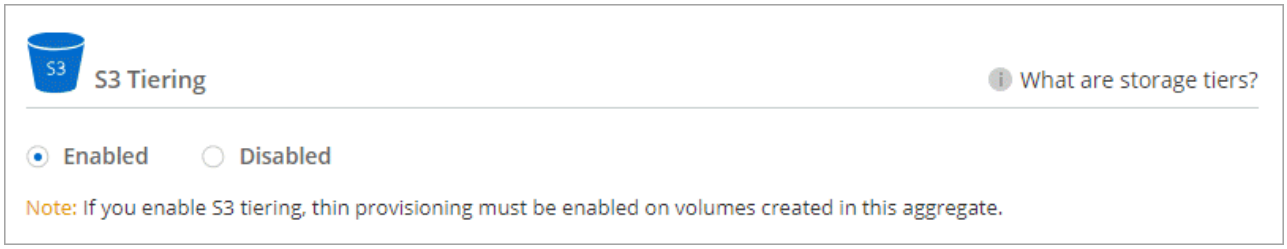
Cloud Volumes ONTAP では、データ保護ボリュームから容量階層にデータを階層化できます。デスティネーションボリュームをアクティブにすると、データは読み取られた時点でパフォーマンス階層に徐々に移動します。

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。

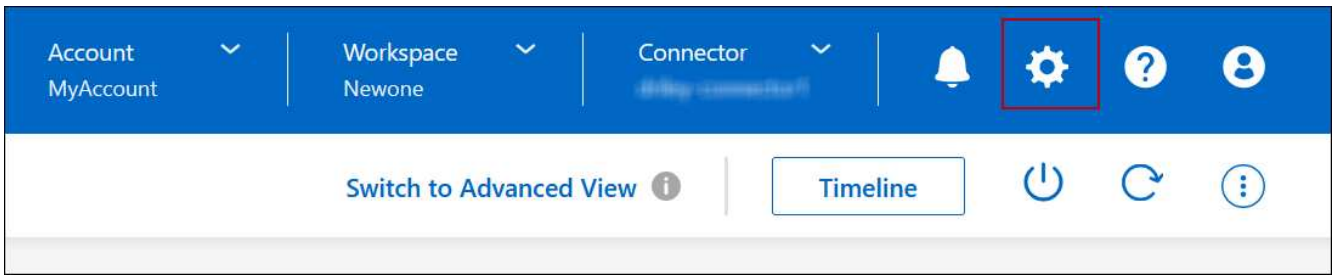
たとえば、購入容量を確実に使用するために、空きスペースを 10% 未満にすることができます。追加の容量が必要になった場合（アグリゲートのディスクの上限に達するまで）、BlueXPで追加のディスクを購入できます。

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*アイコンをクリックし、[Cloud Volumes ONTAP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 』を参照してください"
- "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。

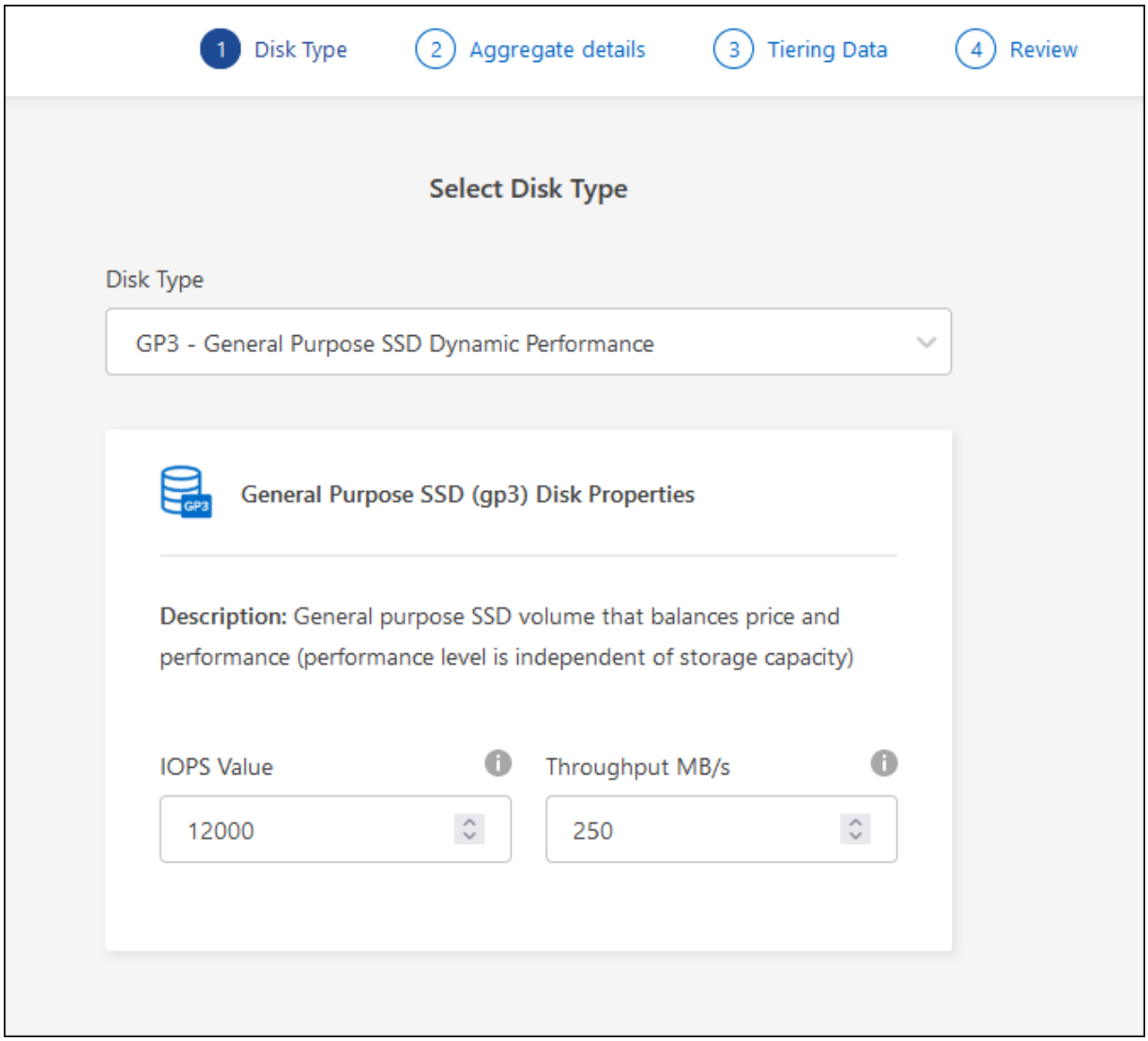
> すべてのディスクとアグリゲートは、BlueXPから直接作成および削除する必要があります。これらのアクションは、別の管理ツールから実行しないでください。これにより、システムの安定性が低下し、将来ディスクを追加できなくなる可能性があります。また、クラウドプロバイダの冗長料金が発生する可能性もあります。

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

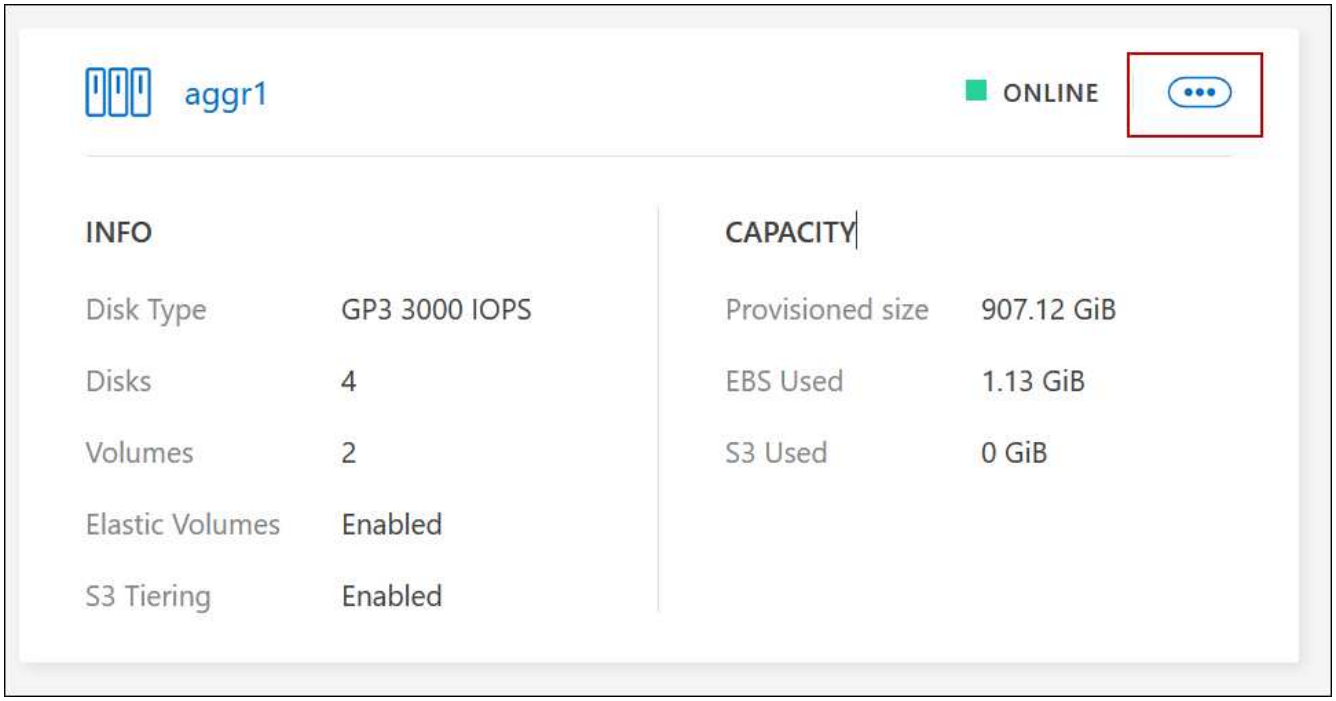
アグリゲートを削除する場合は、まずアグリゲート内のボリュームを削除しておく必要があります。

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、 （省略記号アイコン）*。



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	…（省略アイコン）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	…（省略記号アイコン）メニューの*[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. …（省略記号アイコン）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. …（省略記号アイコン）メニューの*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[**…**（省略記号アイコン）**>**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。

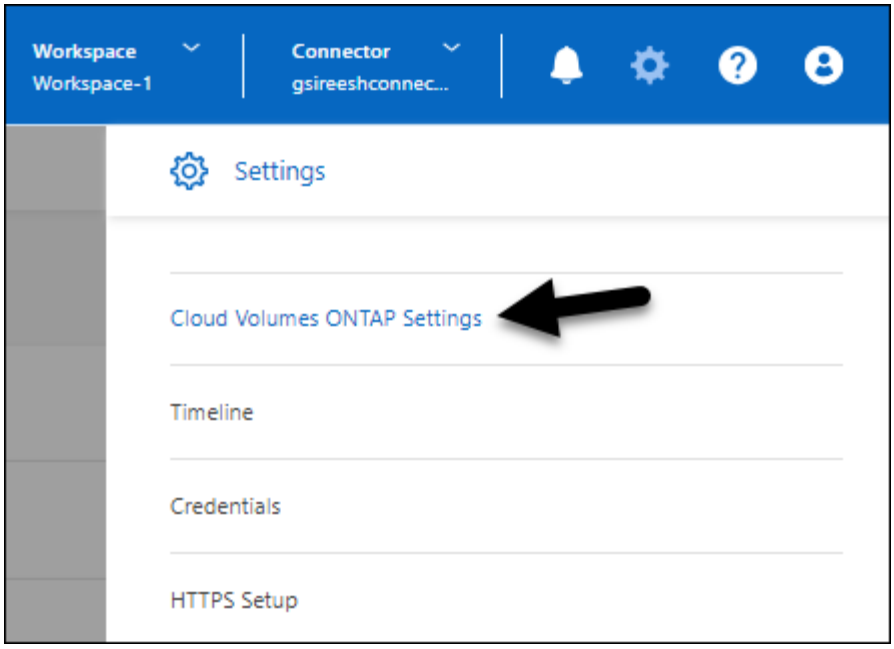
これらの設定は、コネクタによって管理されるすべてのCloud Volumes ONTAP システムに適用されます。別のコネクタがある場合は、別の方法で設定できます。

必要な権限

Cloud Volumes ONTAP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、*[Cloud Volumes ONTAP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

この比率は、容量管理の決定において重要なパラメータであり、容量管理の自動モードと手動モードのどちらを使用しているかに関係なく、その影響を理解することが不可欠です。リソース利用率とコストのバランスを維持するために、特定のストレージニーズと予想される増加率を考慮してこのしきい値を設定することを推奨します。

手動モードでは、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ると、空きスペース率の低下に対処する必要があることを通知する通知がトリガーされます。これらの通知を監視し、アグリゲートの容量を手動で管理して、サービスの停止を回避し、最適なパフォーマンスを確保することが重要です。

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

を参照してください "自動容量管理" Cloud Volumes ONTAPで容量が自動的に管理されるようになりました。

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。

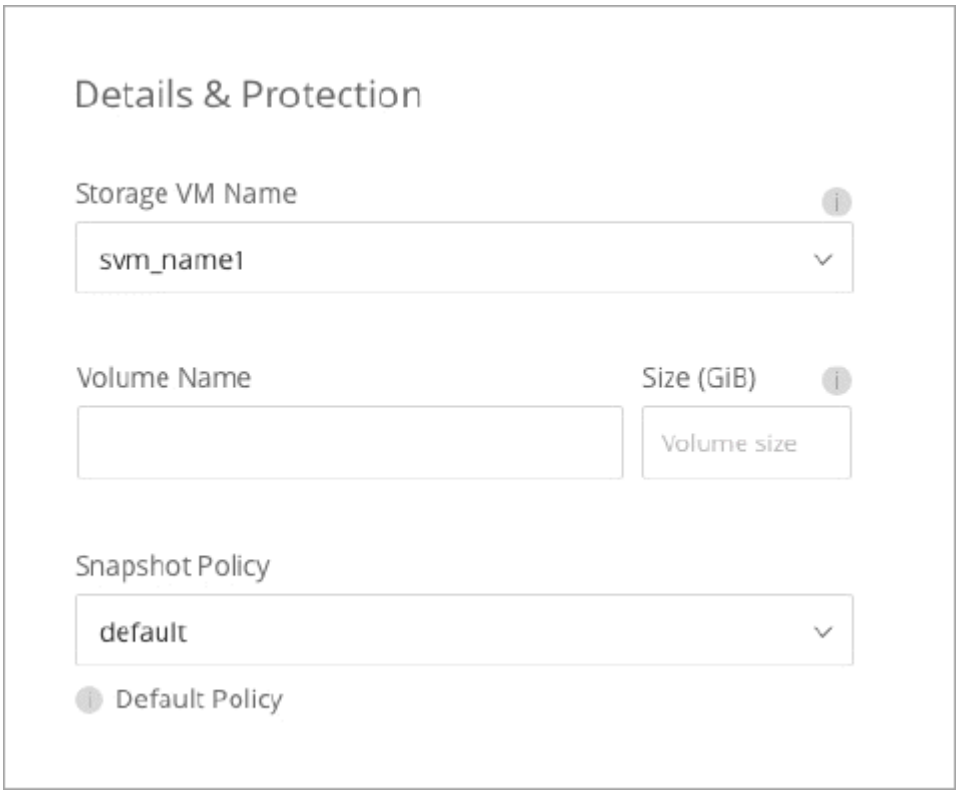
サポートされている Storage VM 数

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。

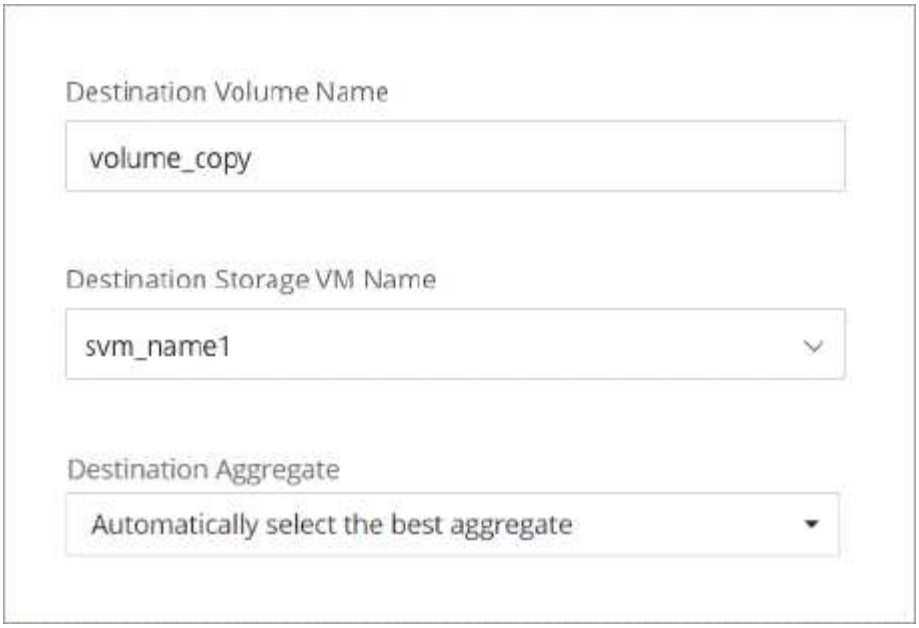
複数の Storage VM を使用できます

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。

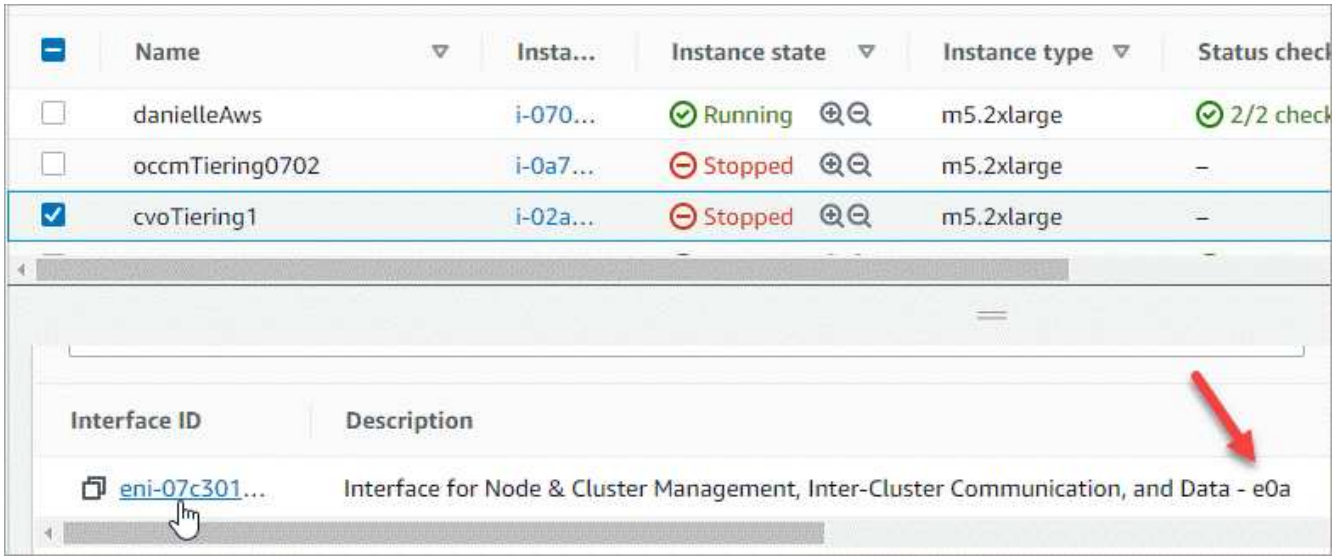
Storage VM 用のオプションの管理 LIF では、単一のノードシステムおよび単一の AZ 内の HA ペア上にプライベート IP アドレスが必要です。この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

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 」は、 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 」は、 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

```
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 」は、 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。

NIC関連の追加タスクを実行するには、Azureで適切な権限を持つネットワーク貢献者ロールまたはカスタムロールを割り当てることができます。これらのNIC関連の権限の詳細については、を参照してください。 "Microsoft Azureのドキュメント"。

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。

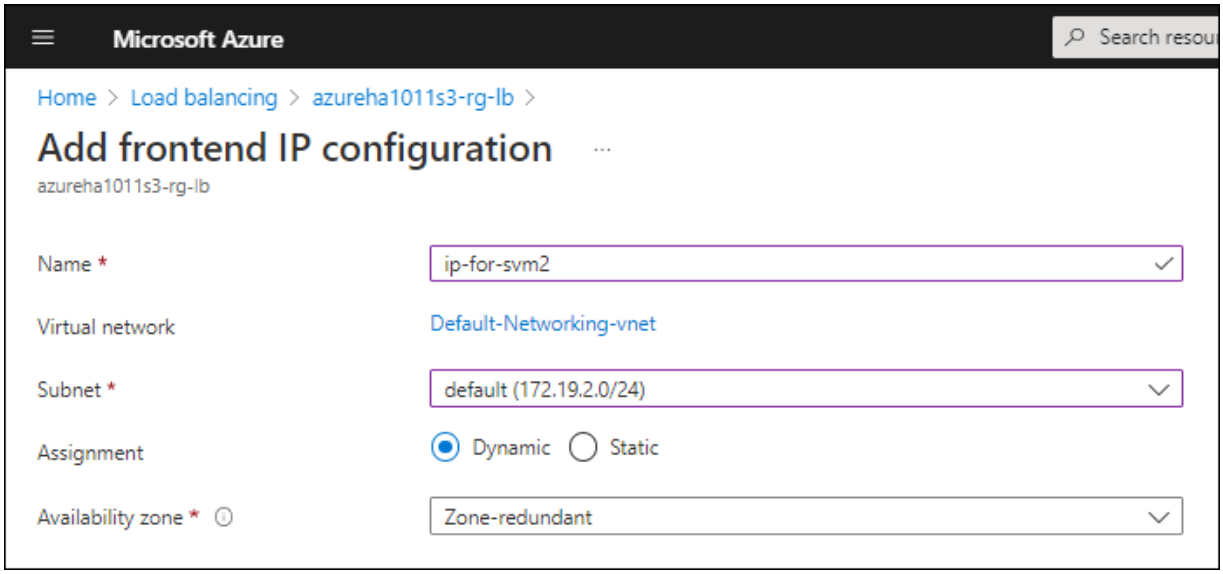
- ノード 1 から NAS データ LIF にアクセスするための IP アドレス × 1
- ノード 2 からの NAS データ LIF アクセス用に 1 つの IP アドレス
- Storage VM （ SVM ）管理 LIF のオプションの IP アドレスです

  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。

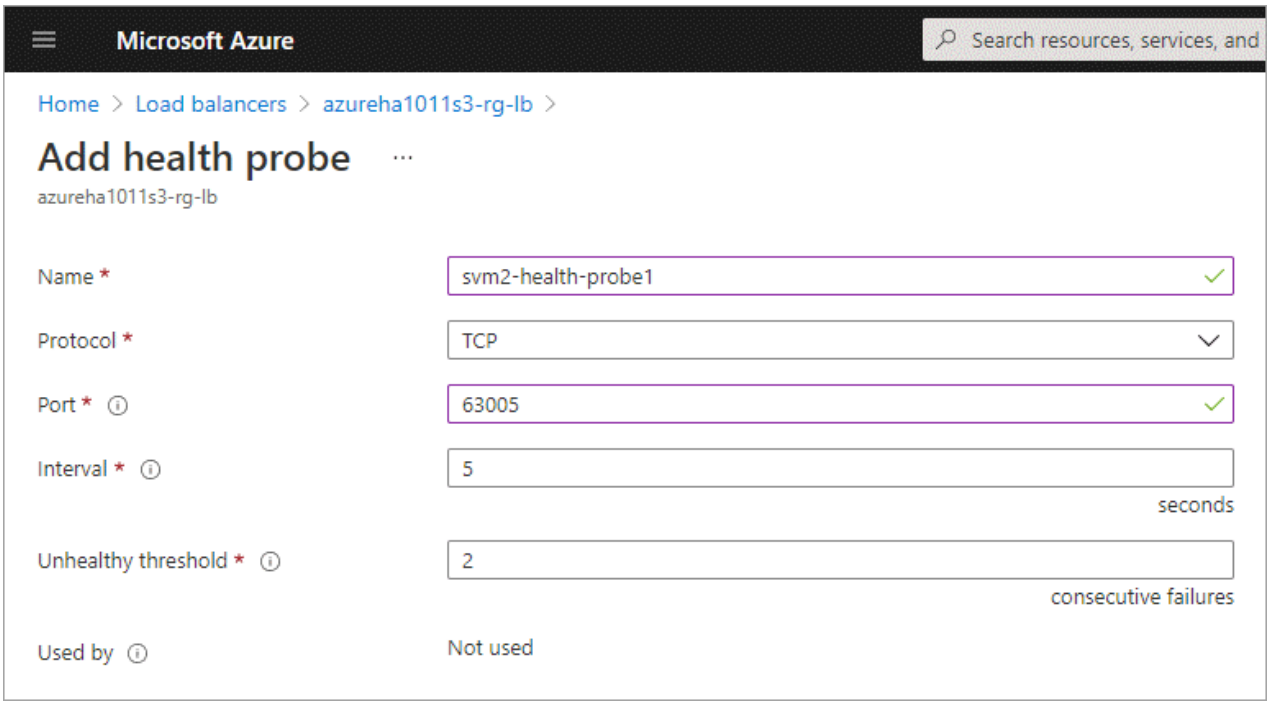


   d. 作成したフロントエンド IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

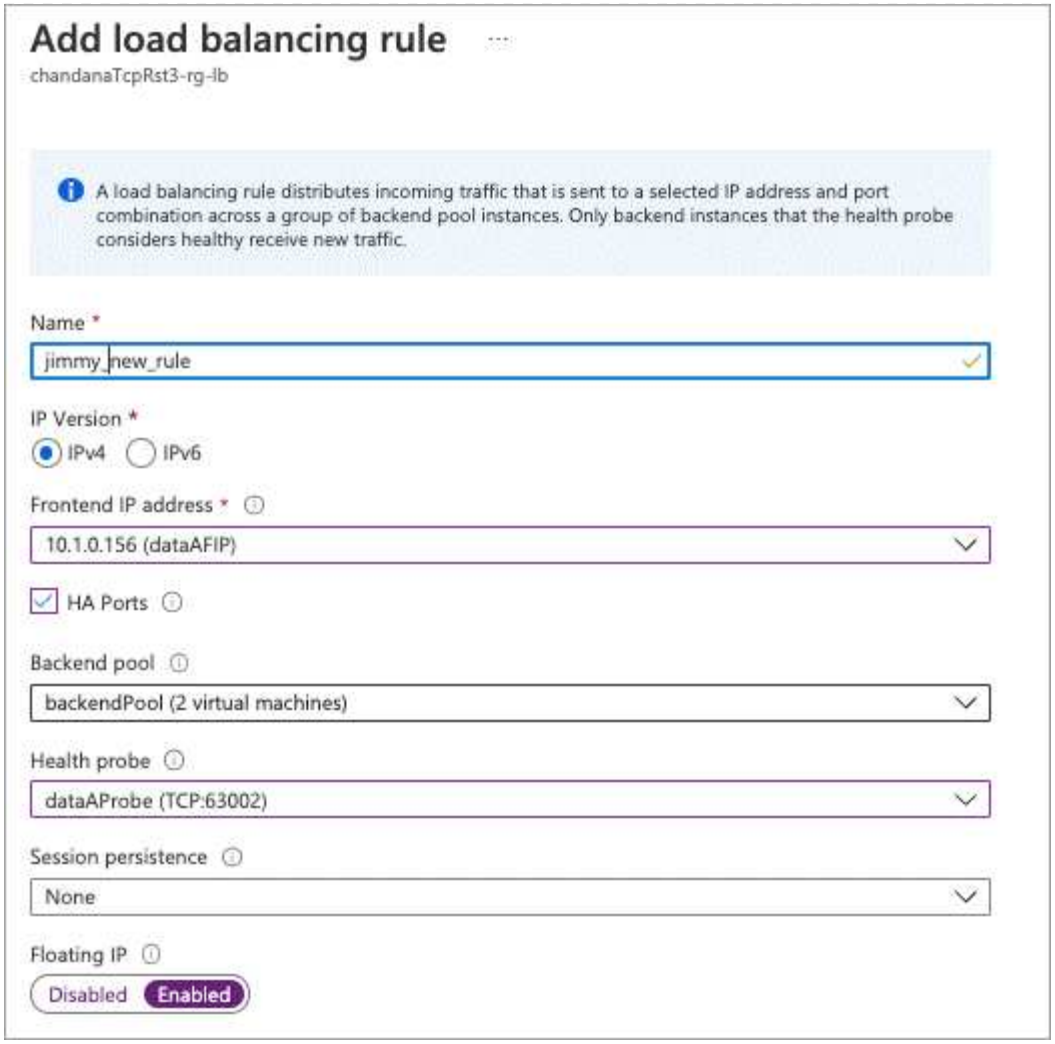
      静的 IP アドレスを使用することをお勧めします。静的 IP で IP アドレスが変更されないようにすることで、アプリケーションの不必要な停止を防止できます。

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

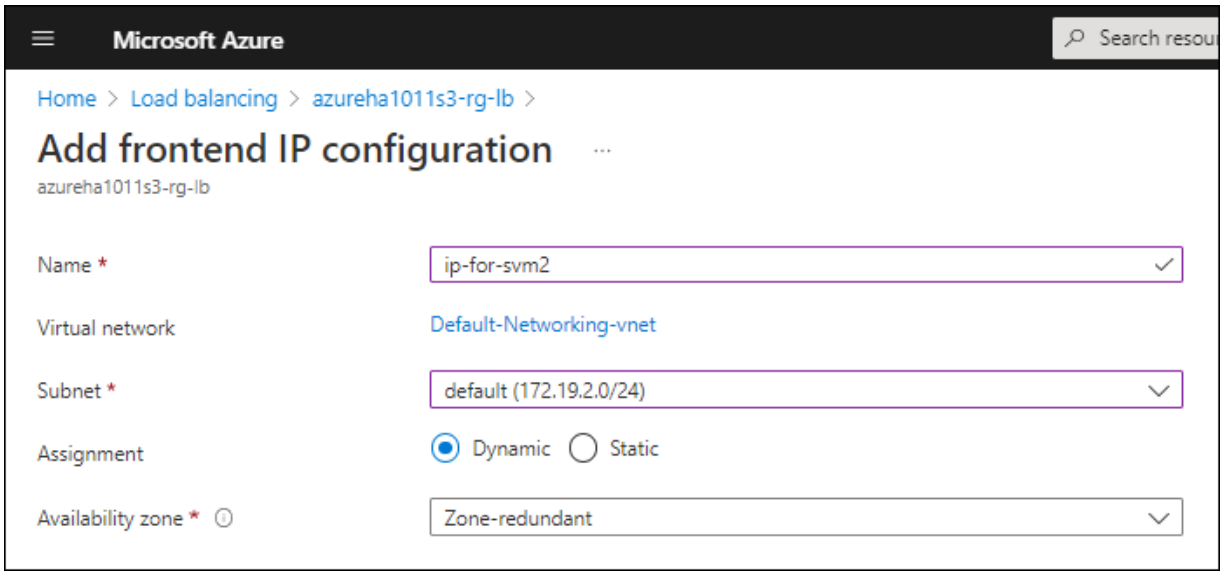
  この管理 LIF は、 SnapCenter などの管理ツールへの接続を提供します。

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。



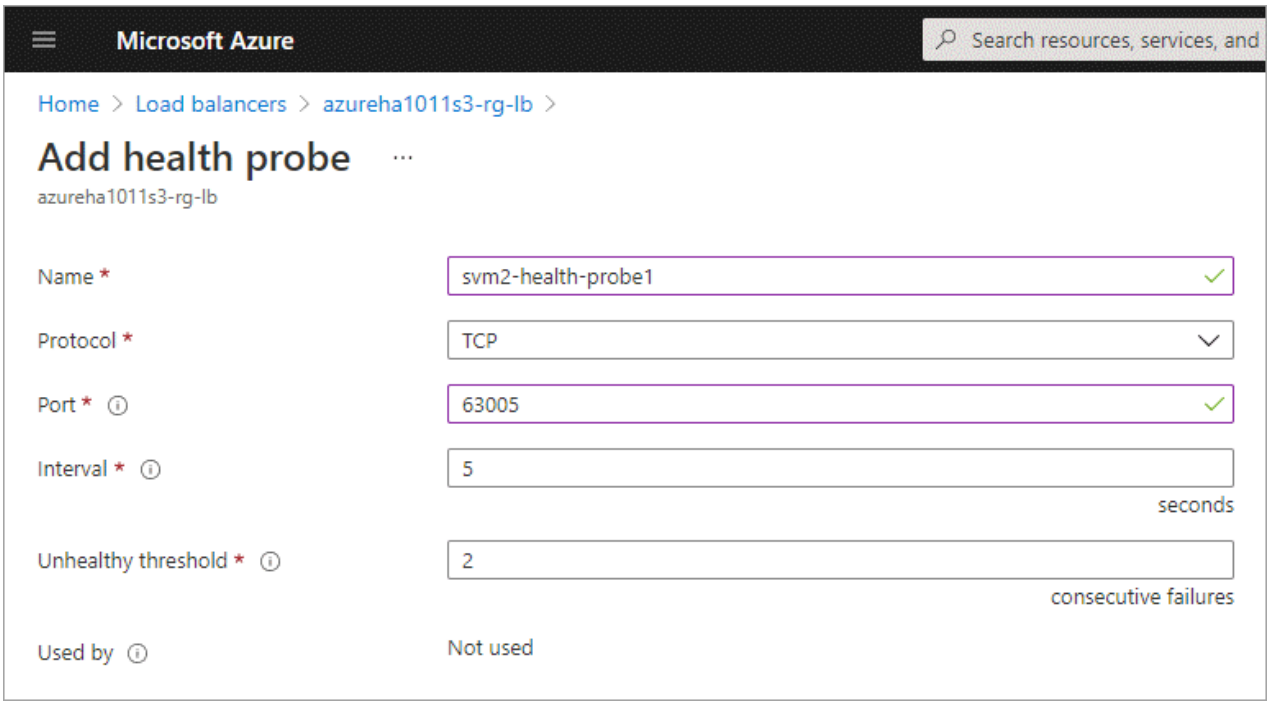
   d. 作成したフロントエンド IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

      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。

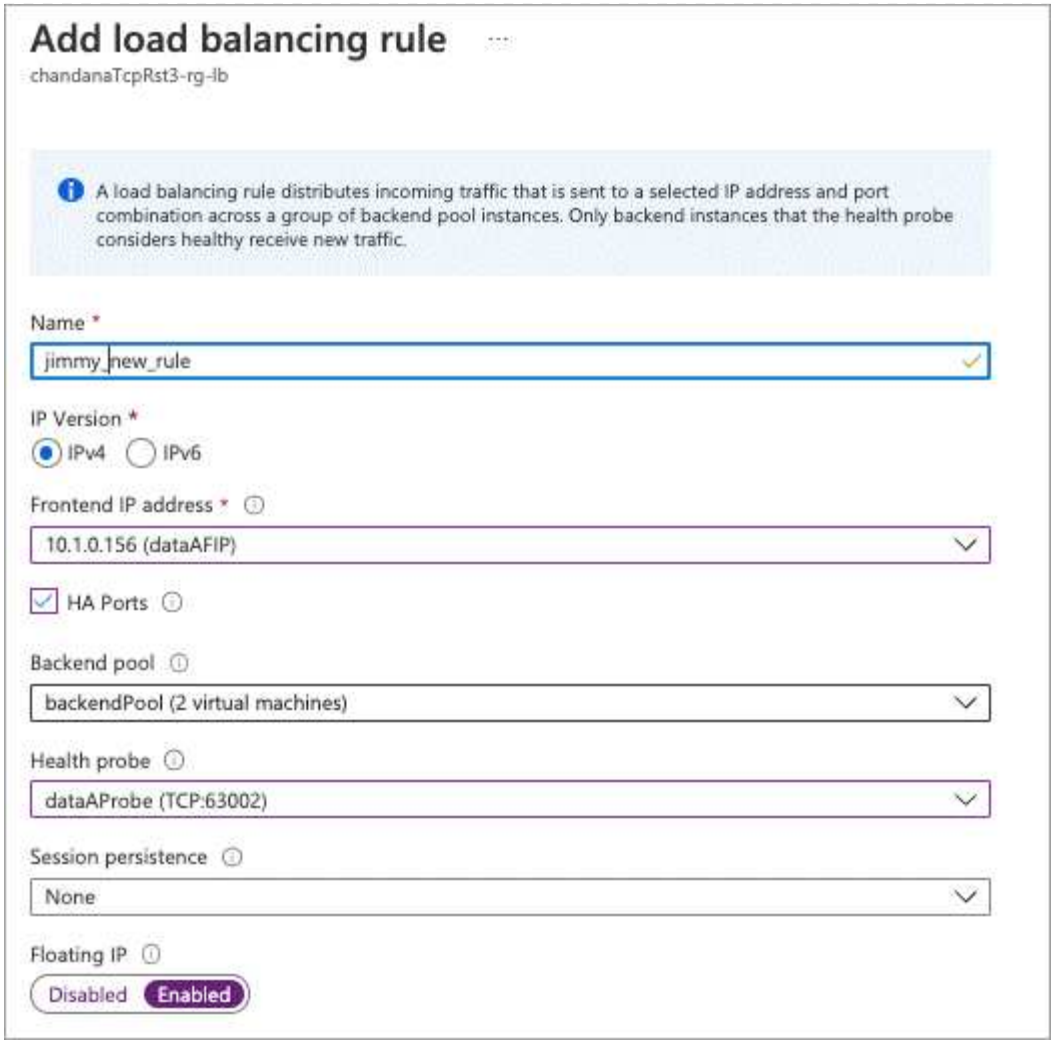
4. 作成した各フロントエンド IP のヘルスプローブを追加します。

   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。

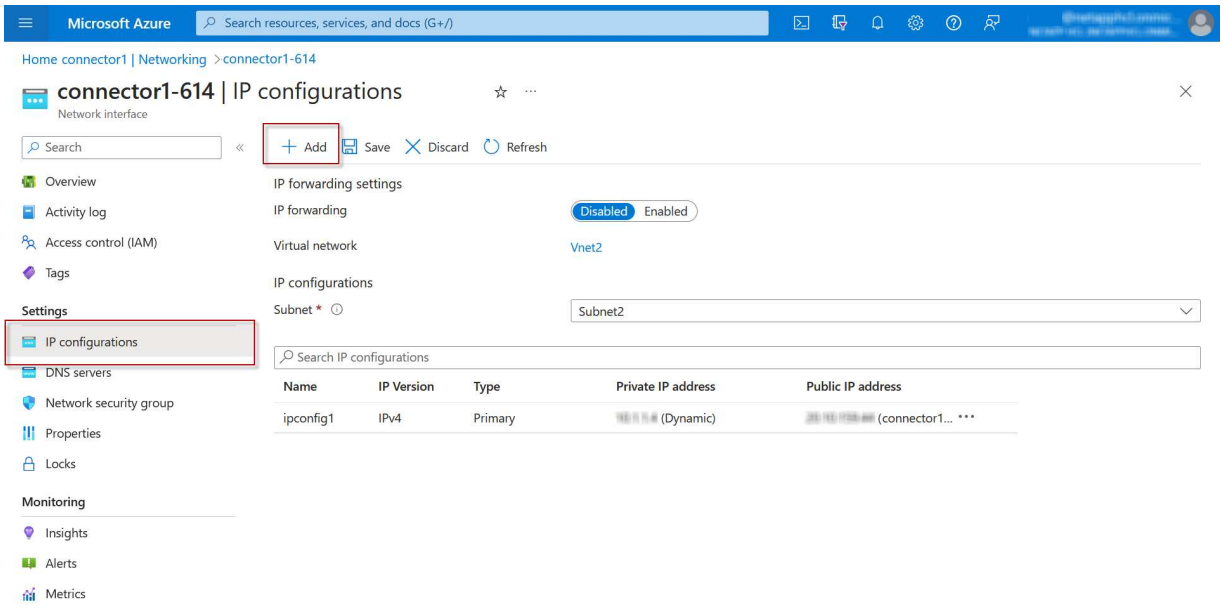
      ポート番号が 63005 ～ 65000. であることが重要です。たとえば、 3 つのヘルスプローブを作成する場合、ポート番号 63005 、 63006 、および 63007 を使用するプローブを入力できます。



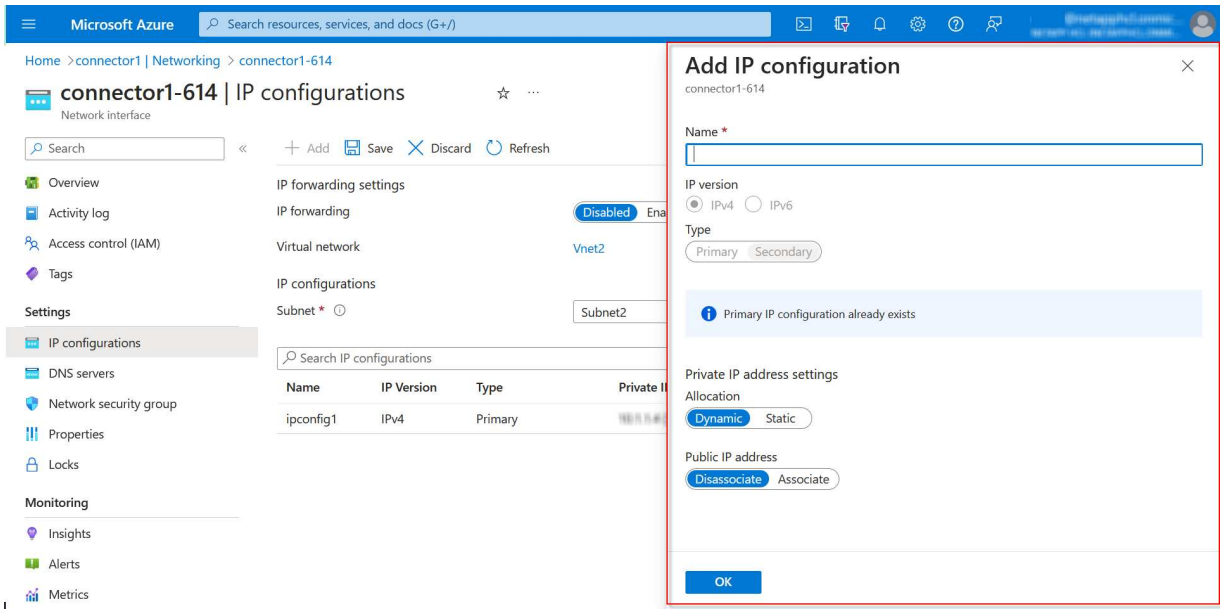
5. フロントエンド IP ごとに新しいロードバランシングルールを作成します。
   a. ロードバランサーの * 設定 * で、 * ロードバランシングルール * をクリックします。
   b. [* 追加（ Add ）] をクリックして、必要な情報を入力する。
      - * 名前 * ：ルールの名前を入力します。
      - * IP バージョン * ：「 * ipv4 * 」を選択します。
      - * フロントエンド IP アドレス *: 作成したフロントエンド IP アドレスのいずれかを選択します。
      - *HA Ports *: このオプションを有効にします。
      - * 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 -vserver <svm-name> -destination 0.0.0.0/0
-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 -vserver <svm-name> -destination 0.0.0.0/0
-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 -vserver <svm-name> -destination 0.0.0.0/0
-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 -vserver <svm-name> -destination 0.0.0.0/0
-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 -vserver <svm-name> -destination 0.0.0.0/0
-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 -vserver <svm-name> -destination 0.0.0.0/0
-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/作業環境/{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/作業環境/{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）" AWSに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。

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
- NAEはAKVでは使用できません。NAEには、外部でサポートされるKMIPサーバが必要です。

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

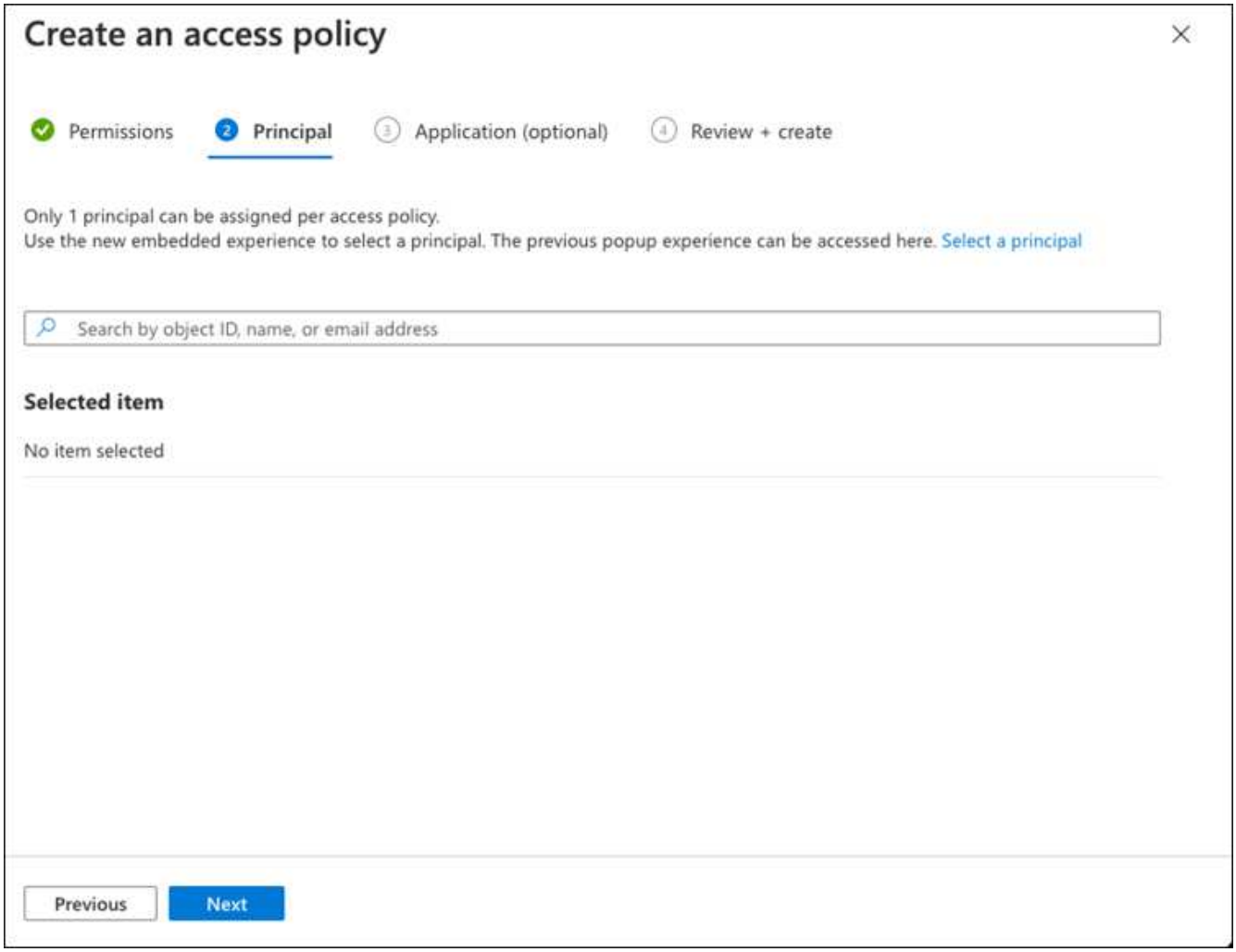
1. 既存のAzure Key Vaultがある場合はCloud Volumes ONTAP 構成に接続できますが、このプロセスの設定にアクセスポリシーを適用する必要があります。
2. Azureポータルで、[** Key Vaults（キーボルト）]セクションに移動します。
3. **[+Create]**をクリックして、リソースグループ、地域、価格階層などの必要な情報を入力します。また、削除したボールトを保持する日数を入力し、キーボールトでパージ保護を有効にする**を選択します。
4. アクセスポリシーを選択するには、 **Next**を選択してください。
5. 次のオプションを選択します。
   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
    - キー権限:20が選択されています
    - 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

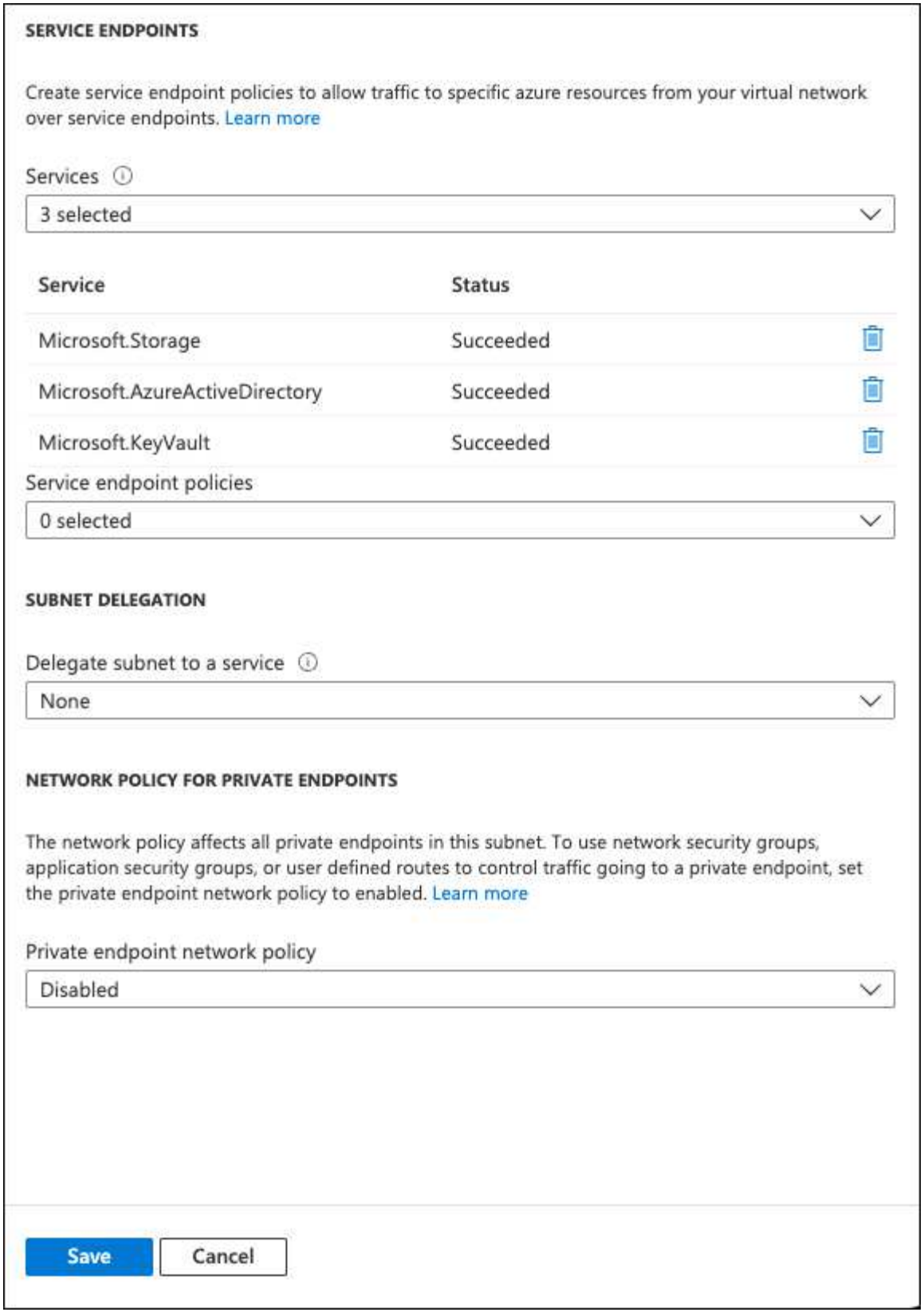
1. Cloud Volumes ONTAP 用に作成したキー・ボールトのメニューで、[**Keys**（キー**）]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。

- 暗号化キー名
- キータイプ：rsa
- RSAキーのサイズ：2048
- Enabled：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。これは、クラスタ管理SVMのエントリと一致している必要があります。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` *`key_vault_URI`* `-key-id` *`full_key_URI`*

   > 。 _full_key_URI 値は、 <https:// <key vault host name>/keys/<key label> の形式で入力し

5. Azure Key Vaultが有効になったら、 `client secret value` プロンプトが表示されたら、

6. 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。

7. 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_name_-aggregate _aggr_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。

8. 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。その場合、「-is-encrypted」パラメータは「true」と表示されます。vol show -vserver_svm_name_-fields is-cencryptedです

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. カスタムロールをCloud KMSキーとCloud Volumes ONTAP サービスアカウントに割り当てます。「gcloud kms keys add -iam-policy binding_key_name_-- keyring_key_ring_name — location_key_location_- member serviceAccount ：_service_account_Name — role project_id_id_roles/custommskmsk`key
4. サービスアカウントのJSONキーをダウンロードします。「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.<プロジェクト>.internal -name -servers_server_address_-vserver _svm_name _
4. CMEKエントリを作成します：'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「vol create _volume_name」をテストするボリュームを作成します。-aggregate -aggregate_aggregate_aggregate—vserver vserver_name _size 10Gです

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」コマンド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

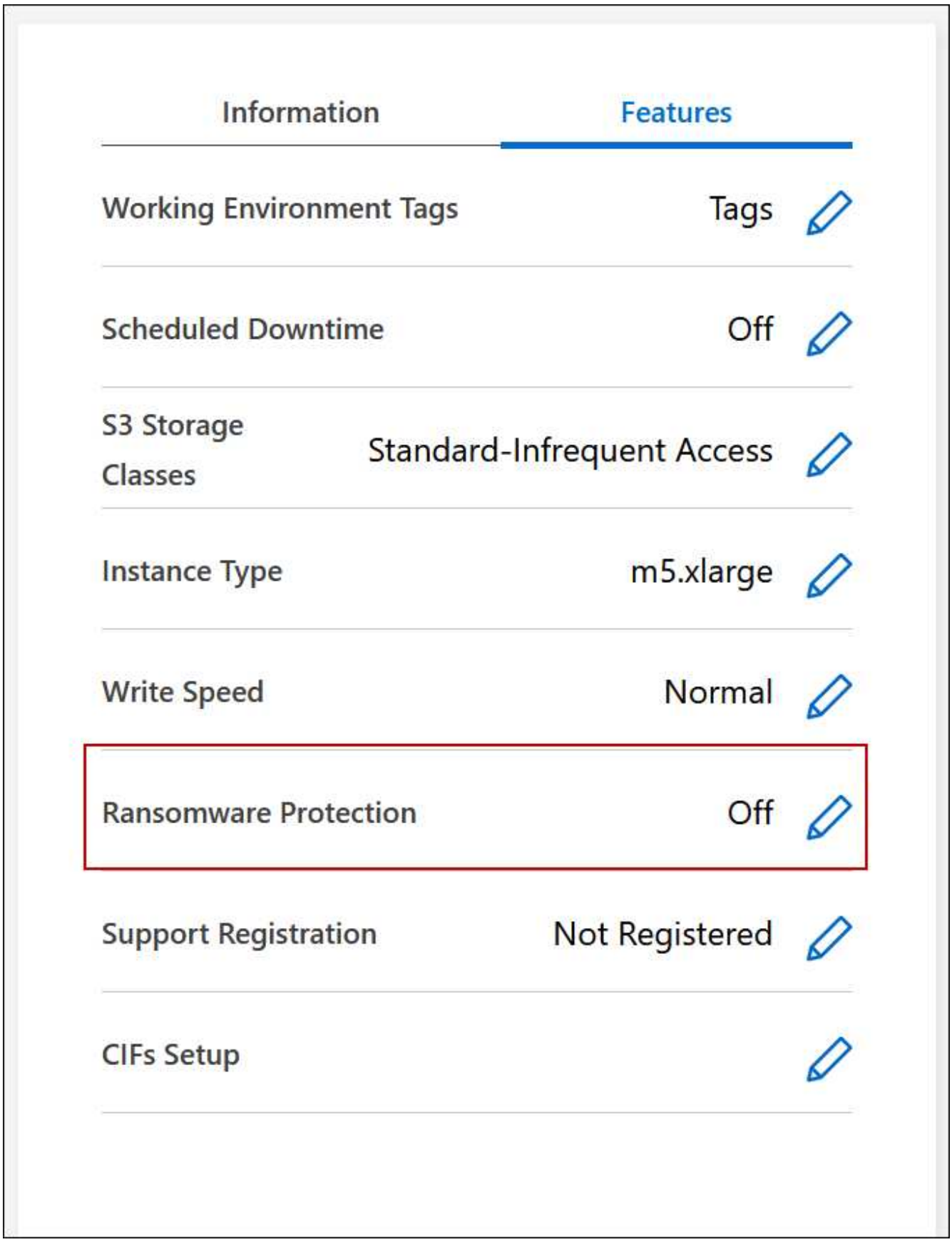
（ARP）です。これらのソリューションは、可視化、検出、修復のための効果的なツールを提供します。

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。

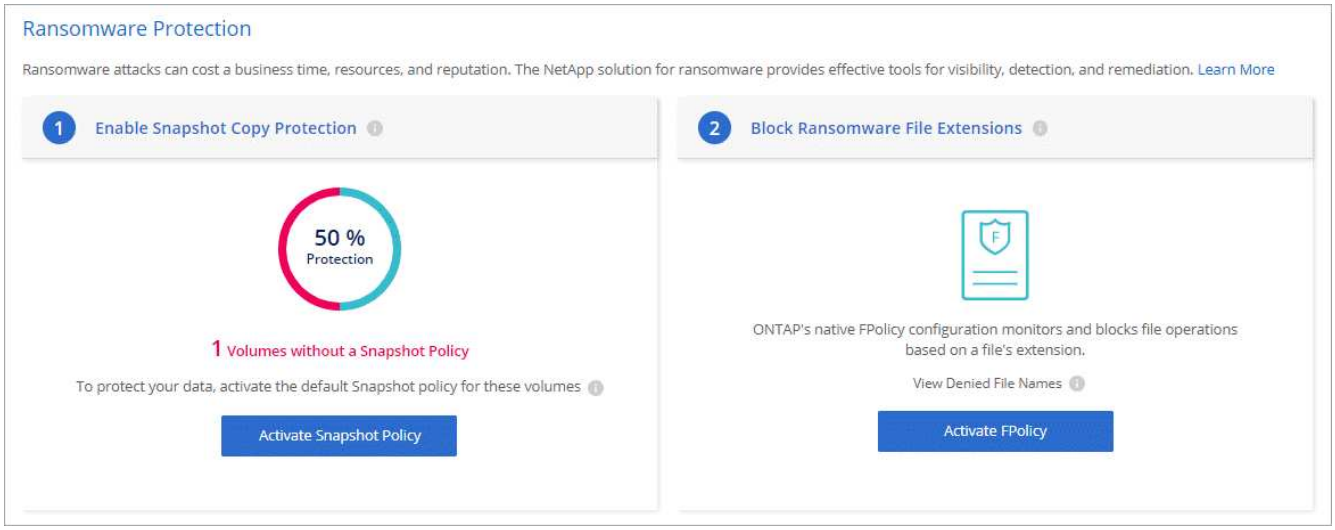
b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これにより、ファイルの拡張子に基づいてファイル操作をブロックできます。

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ライセンスでのみ使用できます

（1~36カ月）。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。

ARPライセンスは「フローティング」ライセンスと見なされます。つまり、単一のCloud Volumes ONTAPインスタンスにバインドされず、複数のCloud Volumes ONTAP環境に適用できます。

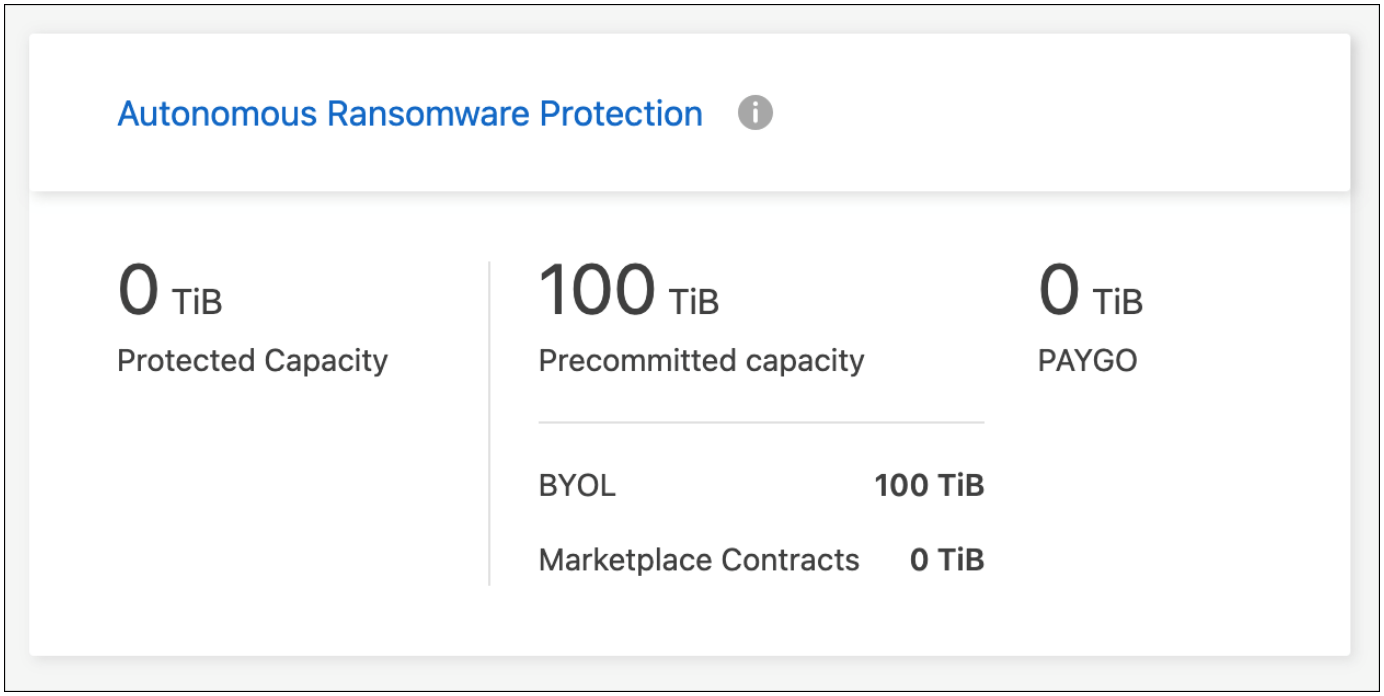
ノードベースのCloud Volumes ONTAPライセンスでのARP機能の使用は、現在Digital Walletには反映されていません。ノードベースのARP使用状況を表示する機能は、今後のリリースでDigital Walletで利用できるようになる予定です。

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。ARPの課金は、ARP機能が有効になっているボリュームのプロビジョニング済み容量の合計に基づいて、ボリュームレベルで計測されます。最小ライセンス容量は1TBです。ただし、ARP機能の最小容量課金はありません。

ARPが有効なボリュームの状態は「ラーニングモード」または「アクティブ」になります。ARP状態が「Disabled」のボリュームは課金対象から除外されます。たとえば、30TiBの容量がプロビジョニングされたCloud Volumes ONTAP環境では、ARPが有効な15TiBのボリュームの一部のみを含めることができます。

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
9.14.0	9.14.1
9.13.1.	9.14.1
	9.14.0
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

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
9.9.1	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。

パッチリリース

2024年1月より、BlueXPでパッチをアップグレードできるのは、3つの最新バージョンのCloud Volumes ONTAPのパッチリリースのみです。BlueXPに表示する3つの最新バージョンは、最新のGAリリースを使用して決定されます。たとえば、現在のGAリリースが9.13.1の場合、BlueXPには9.11.1~9.13.1のパッチが表示されます。バージョン9.11.1以前のパッチリリースにアップグレードする場合は、手順を手動でアップグレードする必要があります。 ONTAPイメエシノタウンロオト。

パッチ（P）リリースの一般的なルールとして、あるバージョンリリースから現在実行しているバージョンまたは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。

C4、M4、R4 EC2インスタンスタイプを使用した**AWS**でのアップグレード

Cloud Volumes ONTAPでは、c4、m4、およびr4 EC2インスタンスタイプがサポートされなくなりました。これらのインスタンスタイプを使用して、既存の環境をCloud Volumes ONTAPバージョン9.8 ~ 9.12.1にアップグレードできます。アップグレードする前に、 インスタンスタイプの変更。インスタンスタイプを変更できない場合は、 ネットワークの強化を有効にする をクリックしてください。インスタンスタイプの変更とネットワークの拡張の有効化の詳細については、次のセクションを参照してください。

バージョン9.13.0以降を実行しているCloud Volumes ONTAPでは、C4、M4、R4 EC2インスタンスタイプでアップグレードすることはできません。この場合は、ディスクの数を減らしてから インスタンスタイプの変更 または、c5、m5、r5 EC2インスタンスタイプの新しいHAペア構成を導入し、データを移行します。

インスタンスタイプの変更

c4、m4、r4のEC2インスタンスタイプでは、c5、m5、r5のEC2インスタンスタイプよりも多くのディスクをノードあたりに配置できます。実行しているc4、m4、またはr4 EC2インスタンスのノードあたりのディスク数が、c5、m5、およびr5インスタンスのノードあたりの最大ディスク許容量を下回っている場合は、EC2インスタンスタイプをc5、m5、またはr5に変更できます。

"EC2インスタンスごとにディスクと階層化の制限を確認する"
"Cloud Volumes ONTAP の EC2 インスタンスタイプを変更します"

インスタンスタイプを変更できない場合は、の手順に従います。 [ネットワークの強化を有効にする]。

ネットワークの強化を有効にする

Cloud Volumes ONTAPバージョン9.8以降にアップグレードするには、c4、m4、またはr4インスタンスタイプを実行しているクラスタでenable_enhanced networking_を有効にする必要があります。ENAを有効にするには、ナレッジベースの記事を参照してください。 "AWS Cloud Volumes ONTAPインスタンスでSR-IOVやENAなどの拡張ネットワークを有効にする方法"。

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]
- すべてのLIFがホームポートにあることを確認する

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

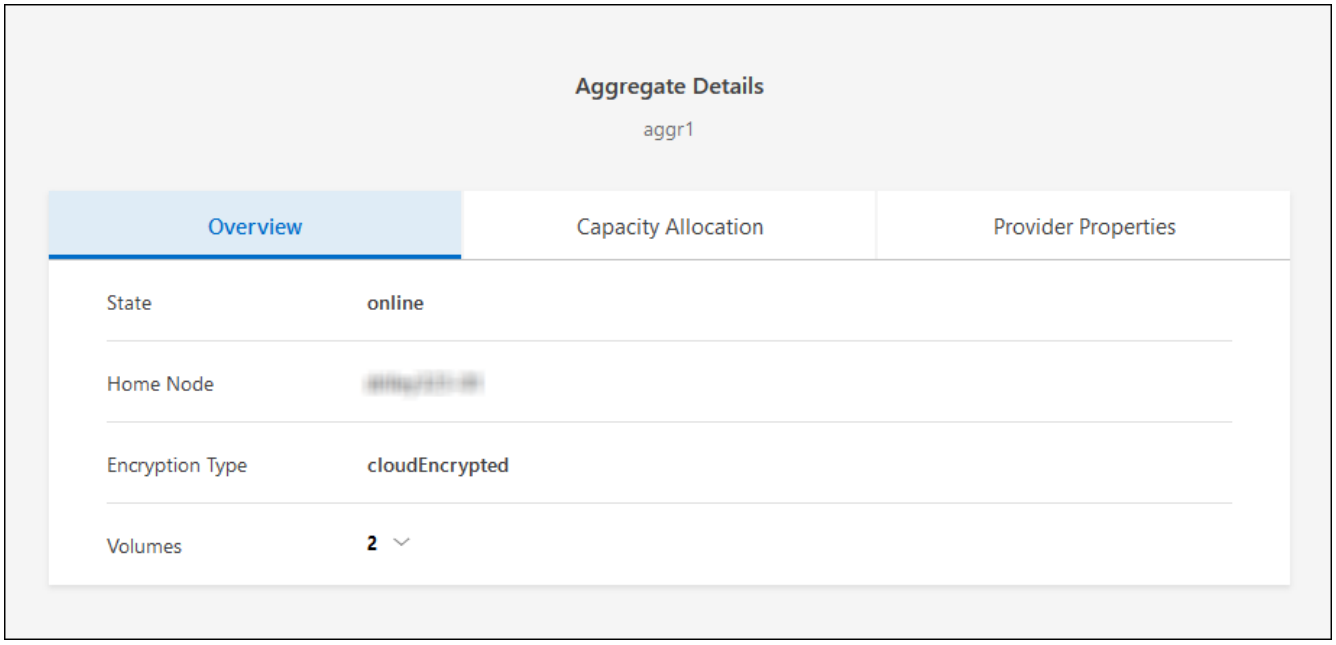
ソフトウェアを更新する前に、 Cloud Volumes ONTAP のアグリゲートがオンラインである必要があります。アグリゲートはほとんどの構成でオンラインになっている必要がありますが、オンラインになっていない場合はオンラインにしてください。

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省略記号ボタンをクリックし、*[アグリゲートの詳細を表示]*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。

すべてのLIFがホームポートにあることを確認する

アップグレード前に、すべてのLIFがホームポートにある必要があります。ONTAPのドキュメントを参照してください。 "すべてのLIFがホームポートにあることを確認する"。

アップグレードエラーが発生した場合は、 "技術情報アーティクル「Cloud Volumes ONTAPのアップグレードが失敗する」"。

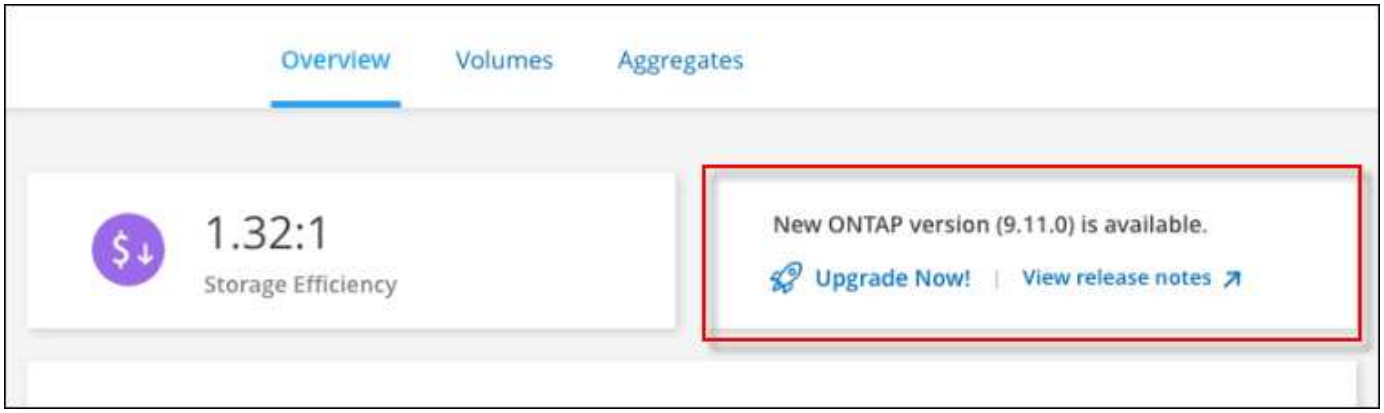
Cloud Volumes ONTAP をアップグレードします

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。

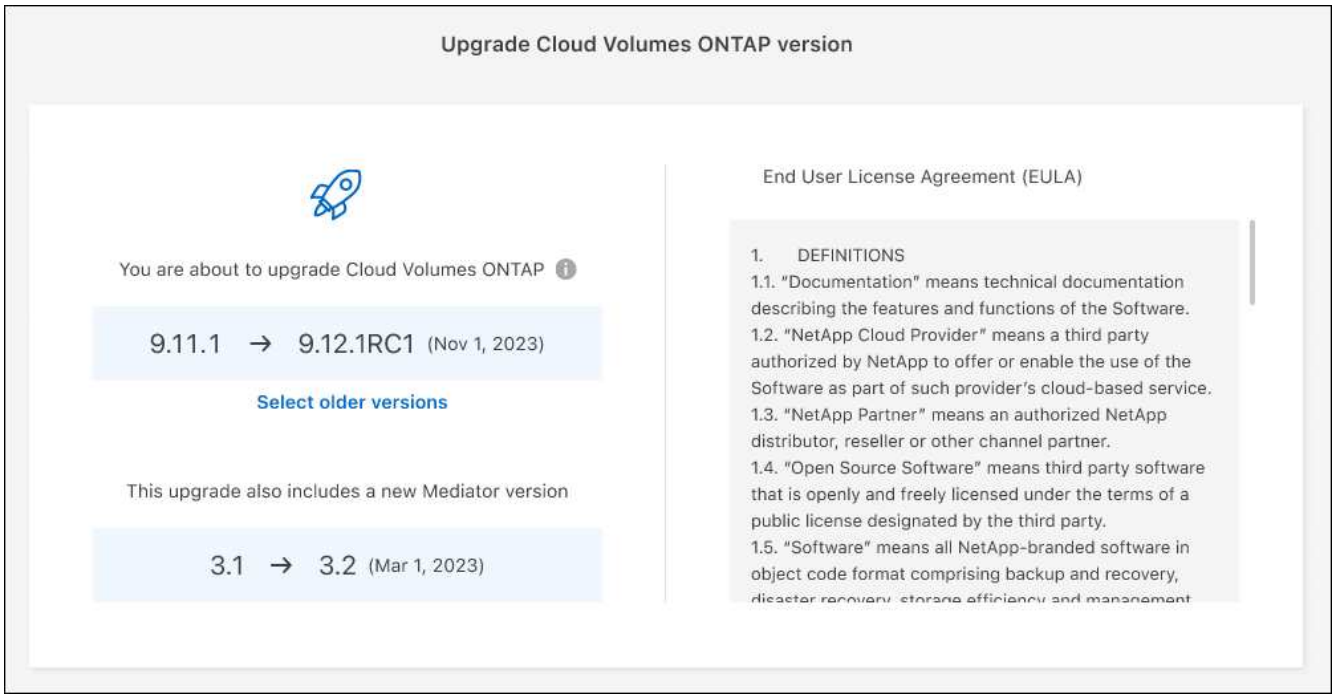
タブの下のリンク。"]

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 "ネットアップサポートサイト"。
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/docx_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。 （省略記号アイコン）*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。

   \ <a href="http://<Connector-private-IP-address>/ontap/images/<image-file-name&gt" class="bare">http://<Connector-private-IP-address>/ontap/images/<image-file-name&gt;

   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"。

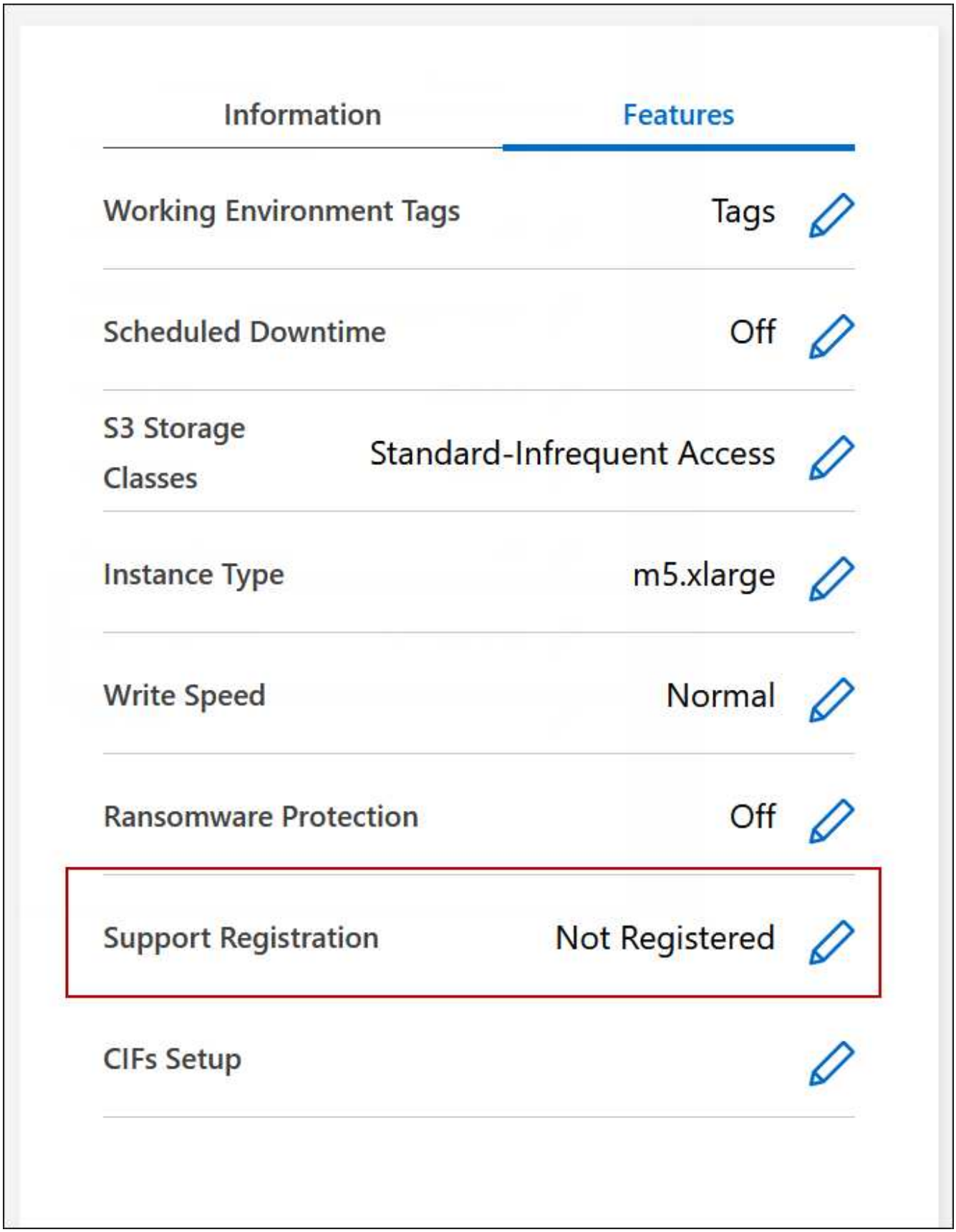
サポートに登録されていないシステムでも、新しいバージョンが利用可能になったときにBlueXPに表示されるソフトウェア更新通知を受け取ります。ただし、ソフトウェアをアップグレードする前に、システムを登録する必要があります。

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。

   "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

2. 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. ネットアップサポートサイトのアカウントを選択し、 * 登録 * をクリックします。

結果

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。

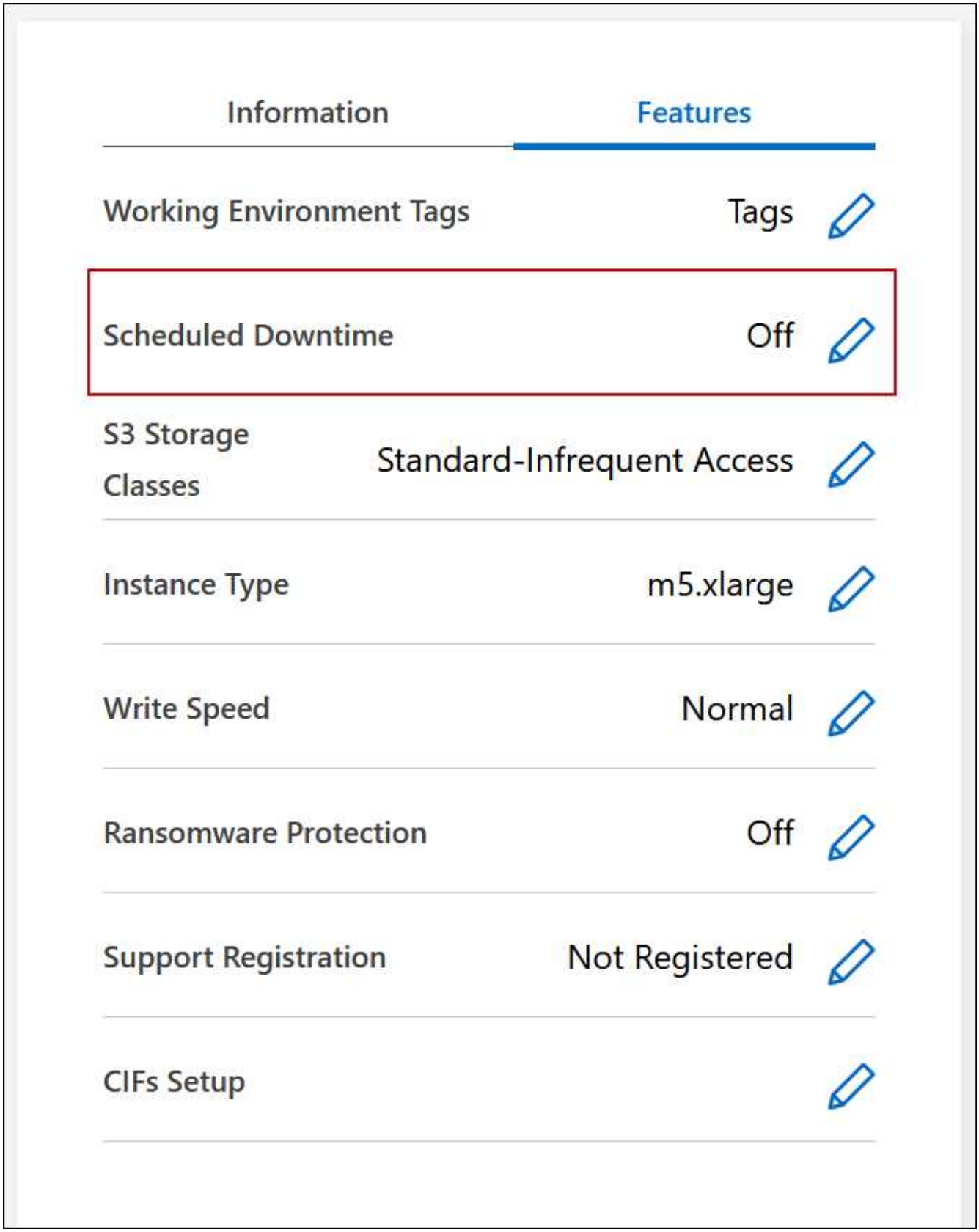
  転送が完了すると、BlueXPによってシステムがシャットダウンされます。

- 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。



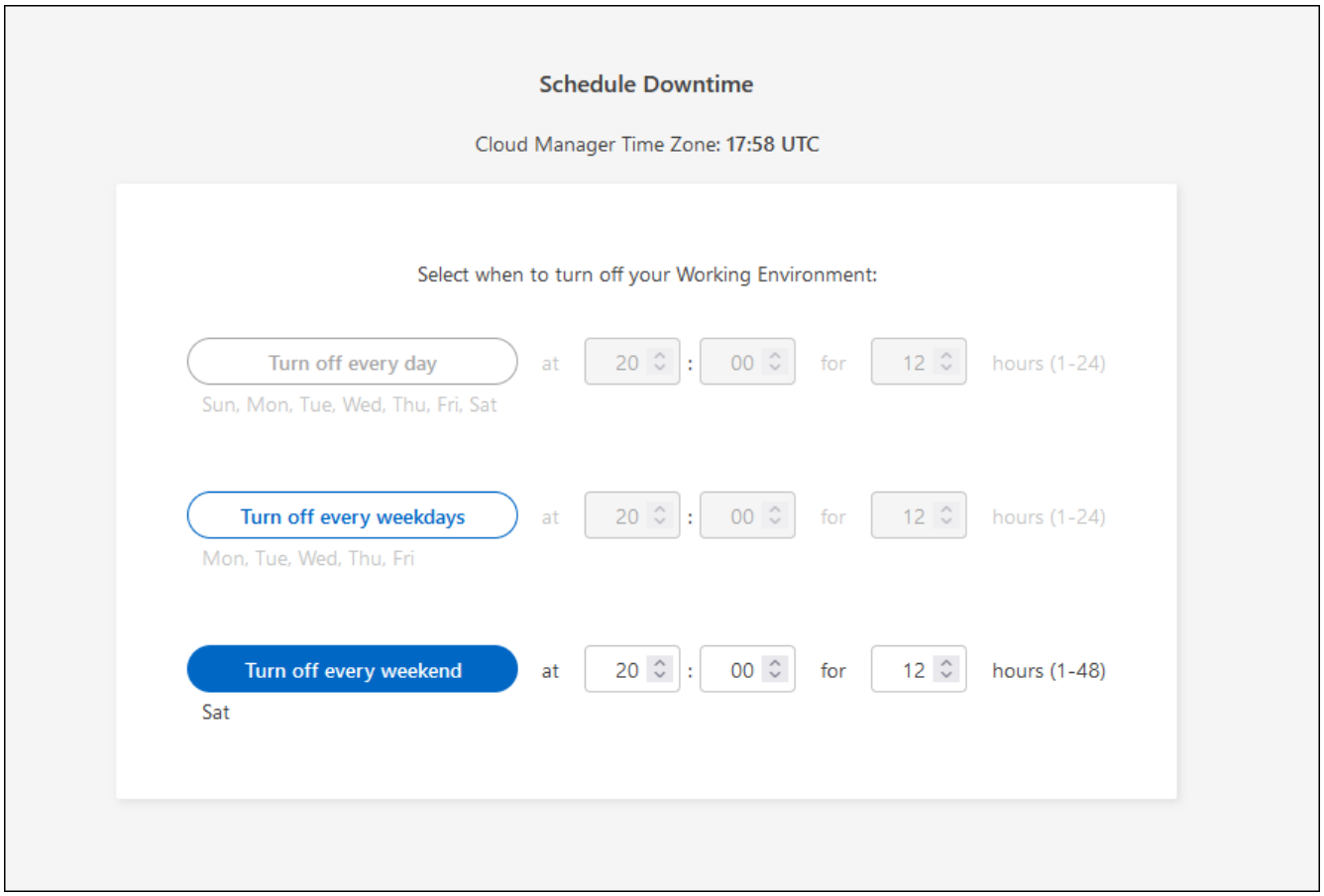
3. シャットダウンスケジュールを指定します。

   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。

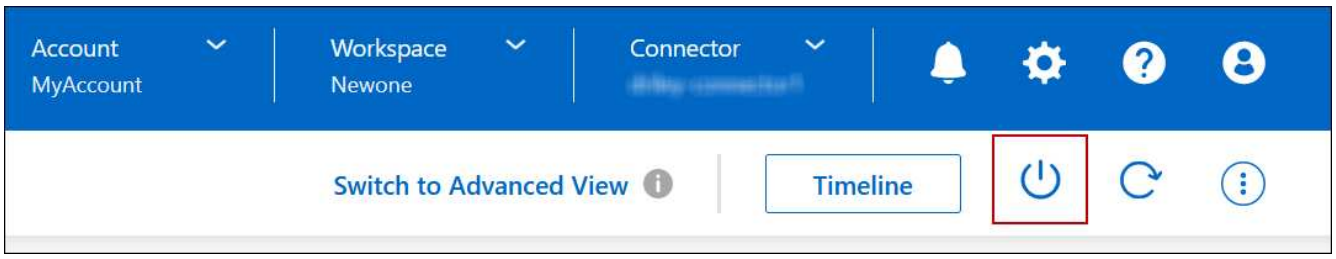
コストを削減するため、BlueXPは定期的にルートディスクと起動ディスクの古いスナップショットを削除します。ルートディスクとブートディスクの両方に対して、最新の 2 つの Snapshot のみが保持されます。

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"

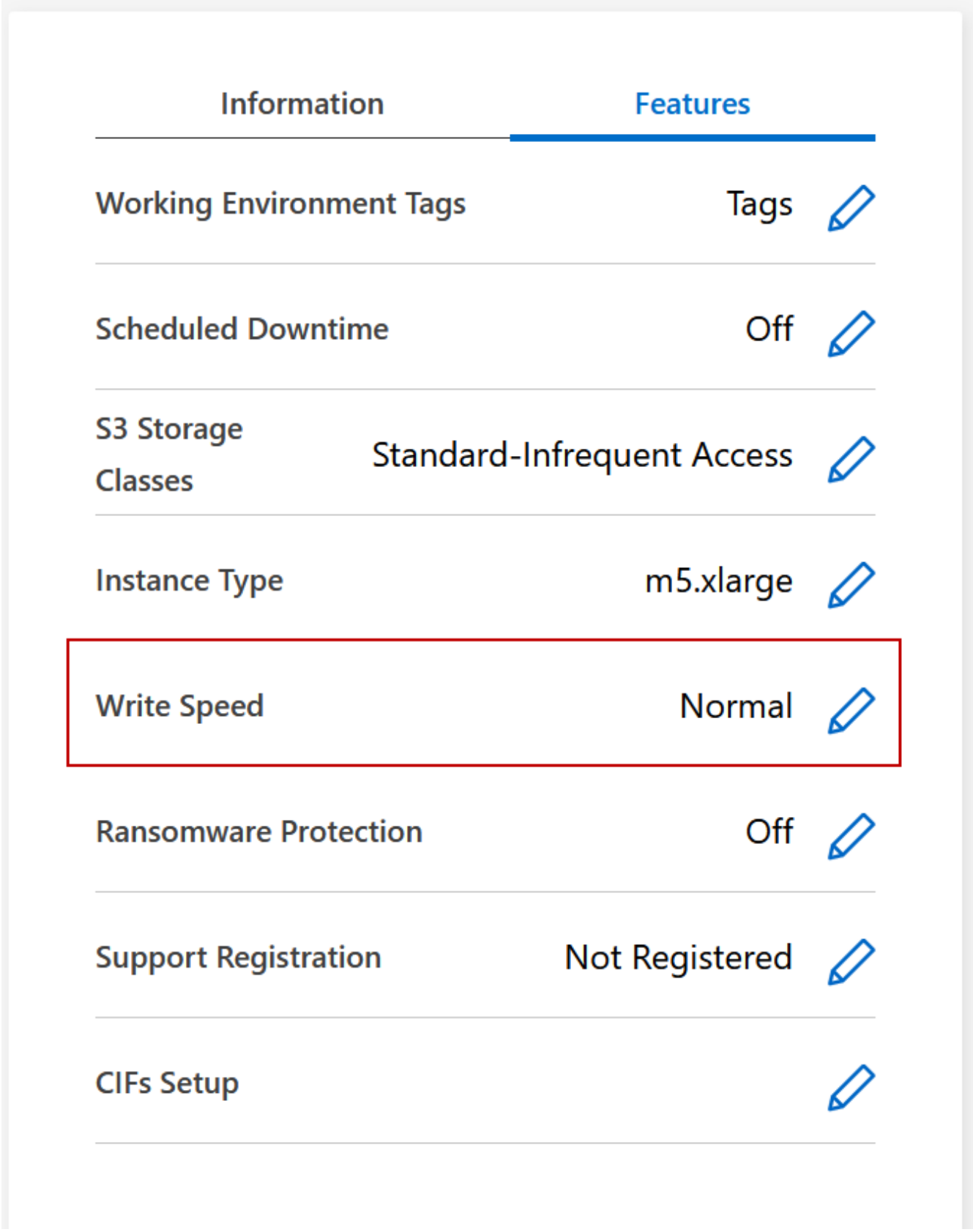
書き込み速度を変更する前に、次のことを確認してください "通常の設定と高い設定の違いを理解する"。

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。

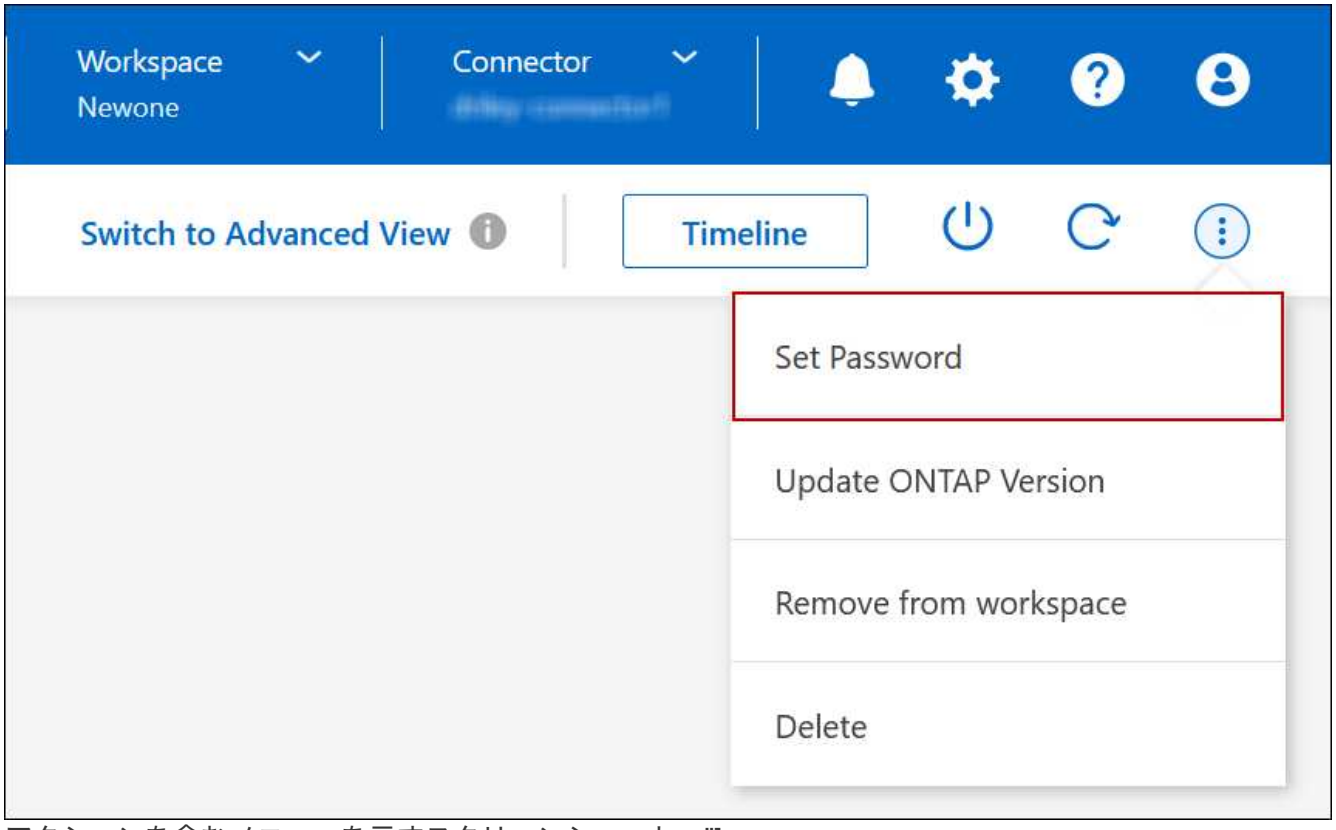
Cloud Volumes ONTAP のパスワードを変更します

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省略記号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。

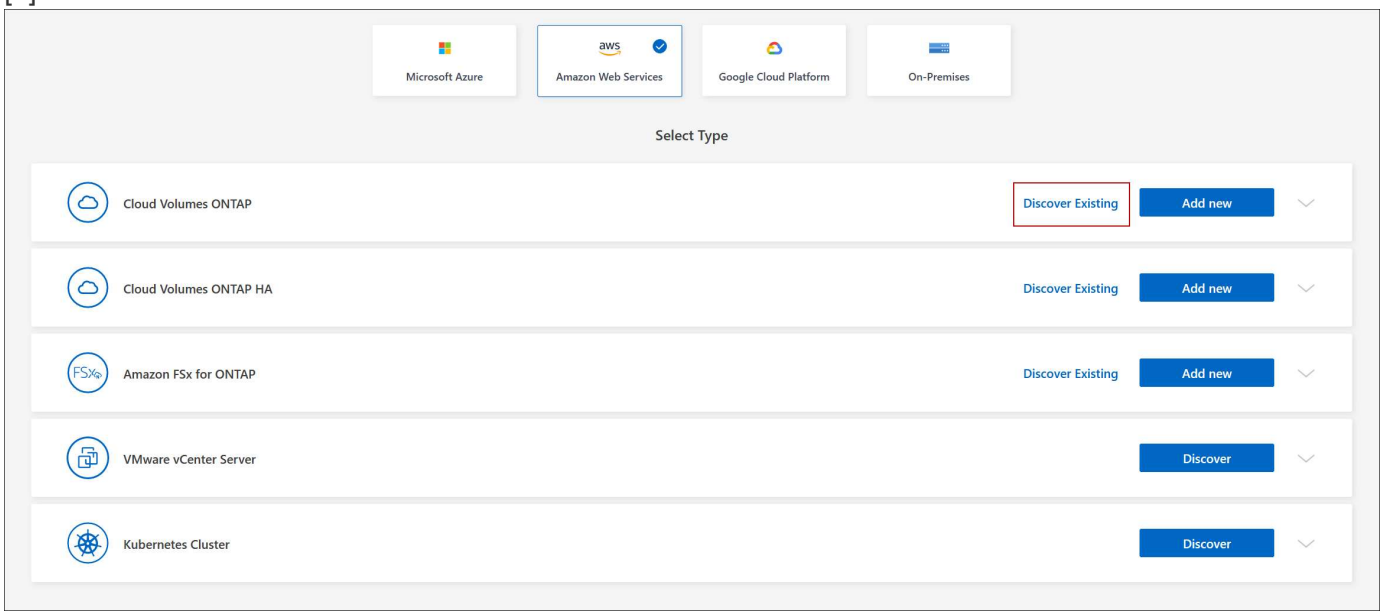
作業を開始する前に

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

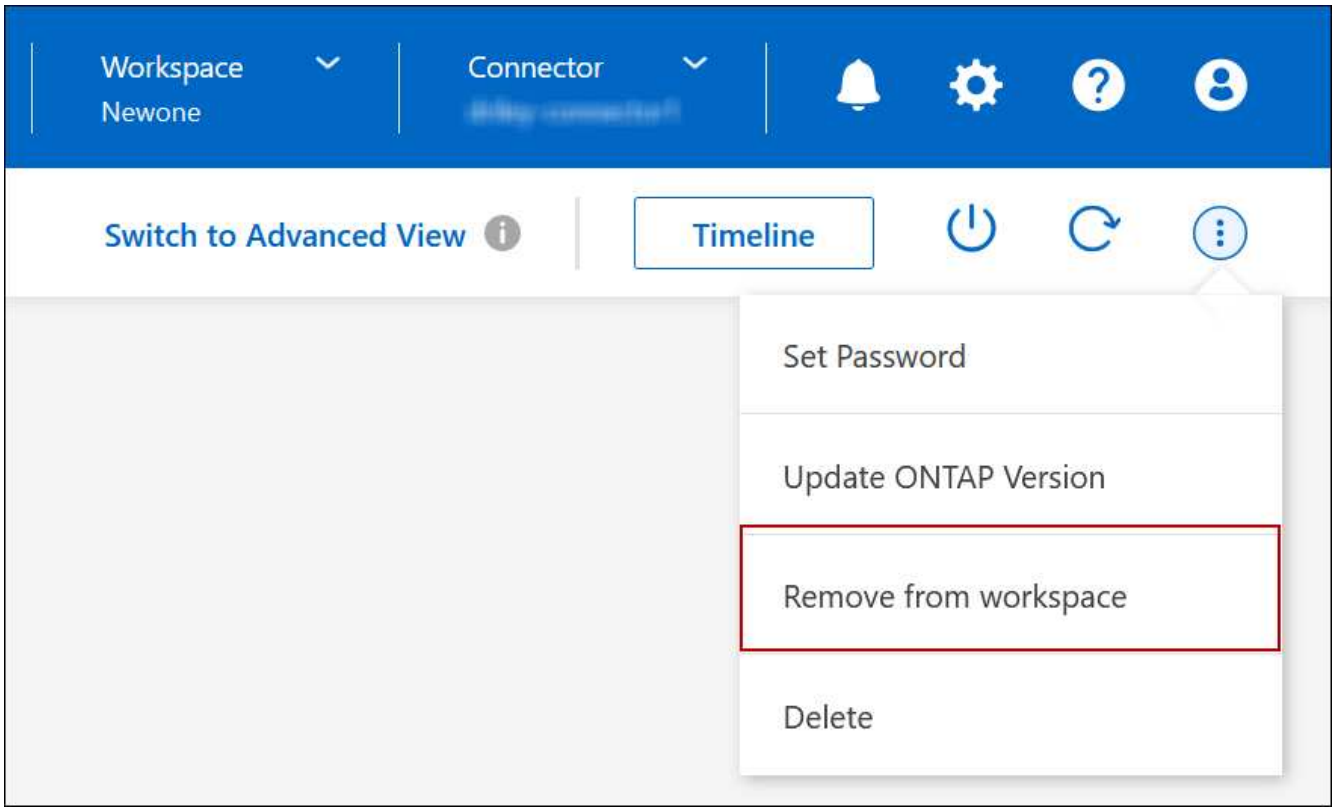
除されません。作業環境は後で再検出できます。

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省略記号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

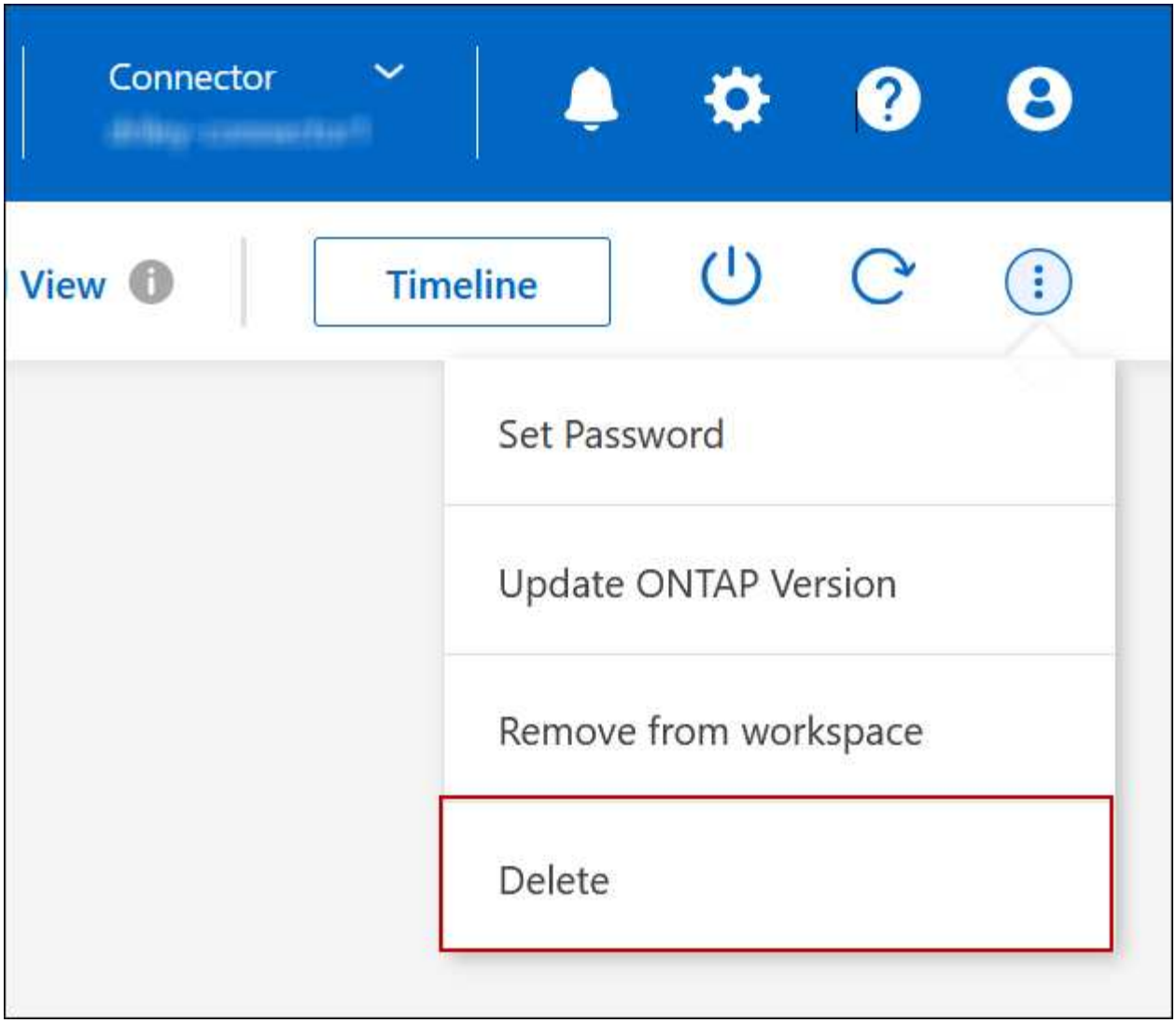
1. 作業環境でBlueXPのバックアップとリカバリを有効にした場合は、バックアップデータが引き続き必要かどうかを確認し、実行します "必要に応じて、バックアップを削除します"。

   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省略記号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。

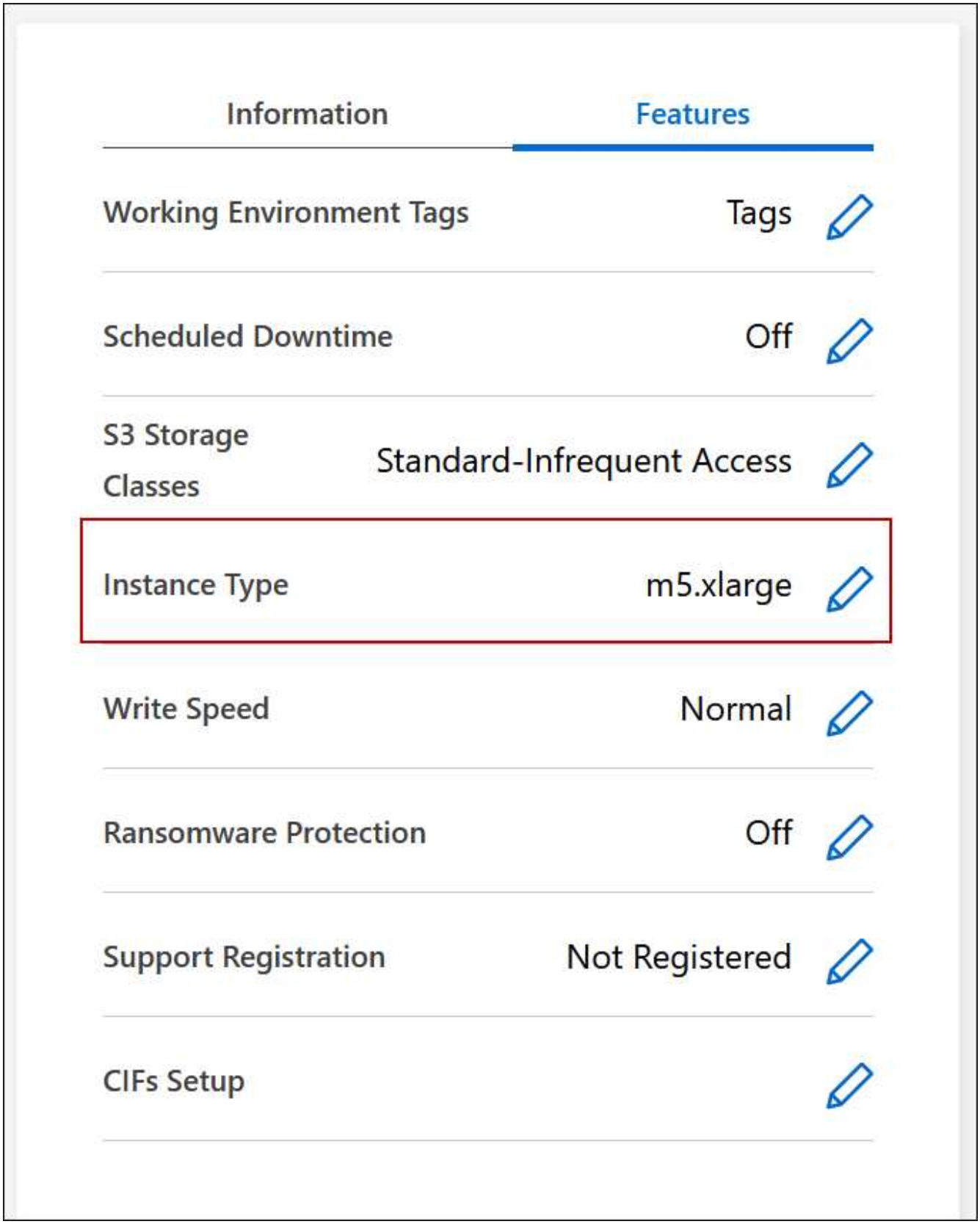
参照

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"。

インスタンスタイプをC4、M4、またはR4インスタンスから変更できない場合は、技術情報アーティクルを参照してください。 "AWS Xen CVOインスタンスからNitro（KVM）への変換"。

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

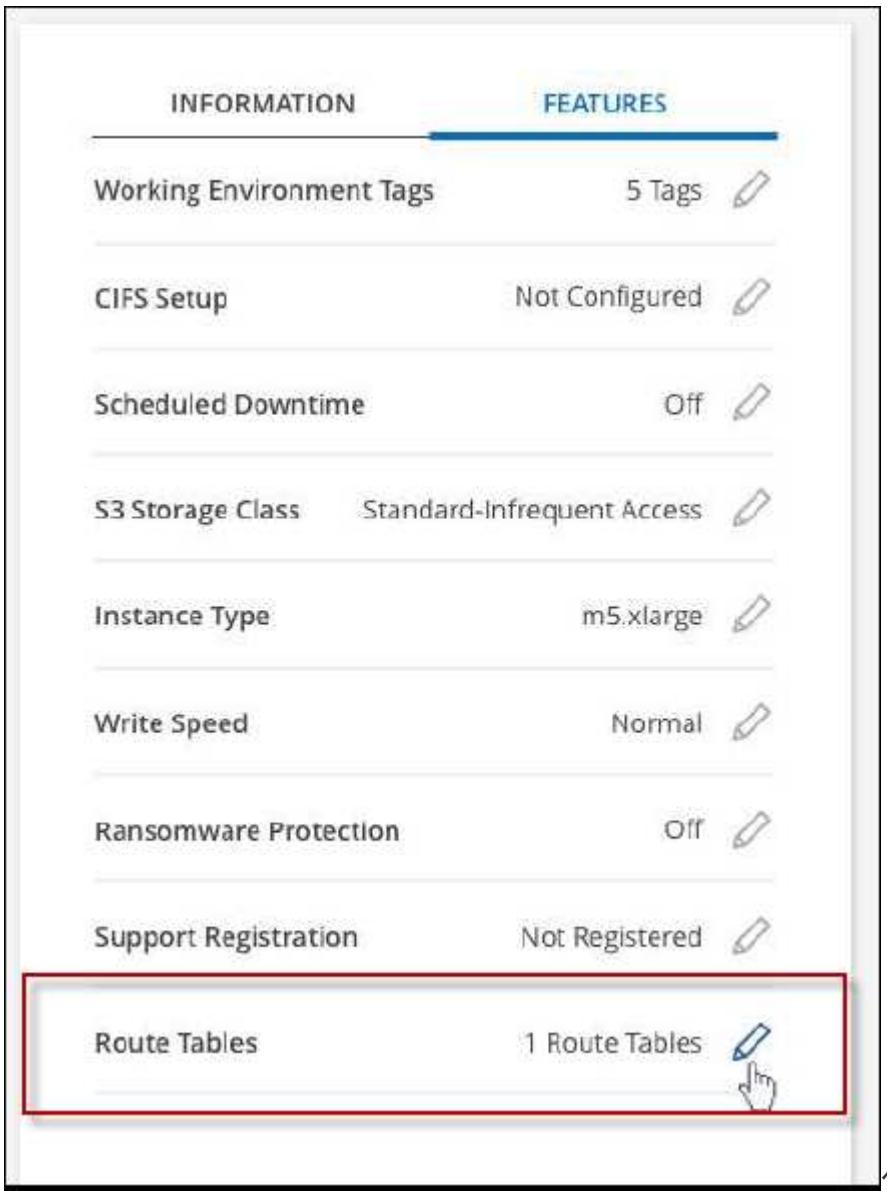
Cloud Volumes ONTAP が新しい設定でリブートします。

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。

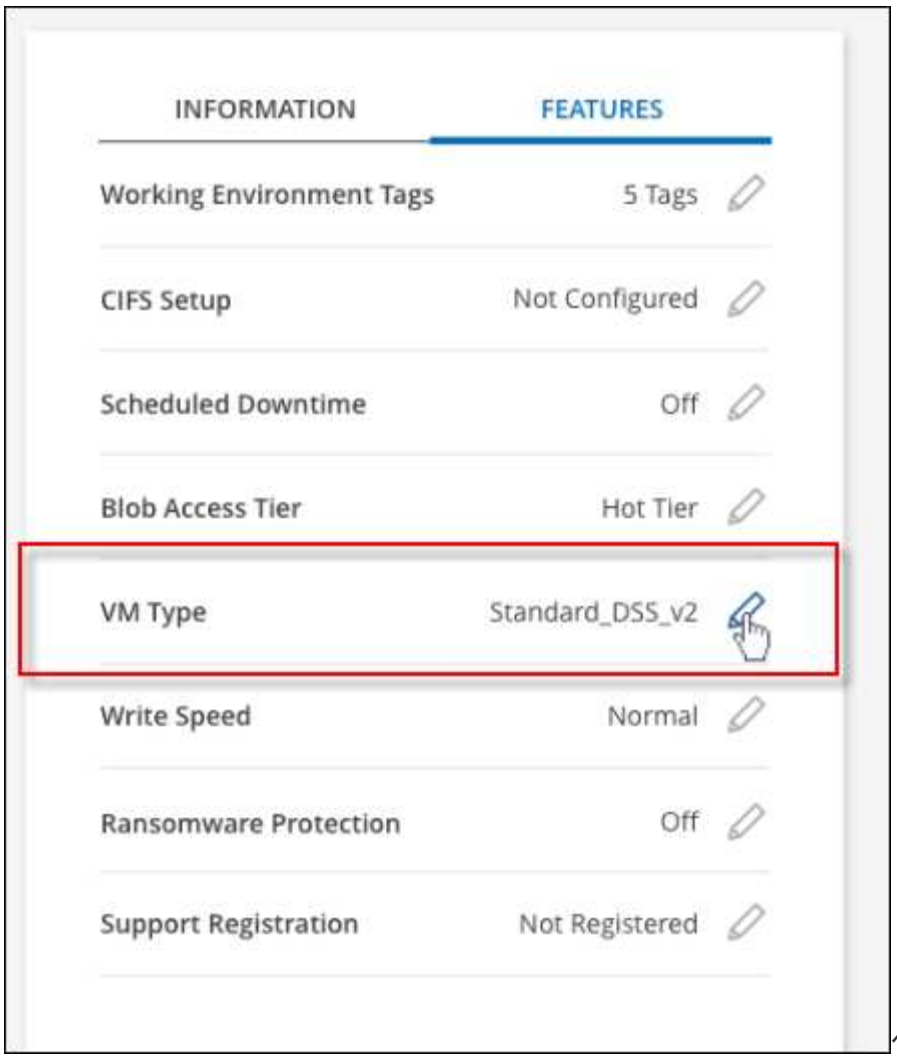
  シングルノードシステムの場合、 I/O は中断されます。

  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。

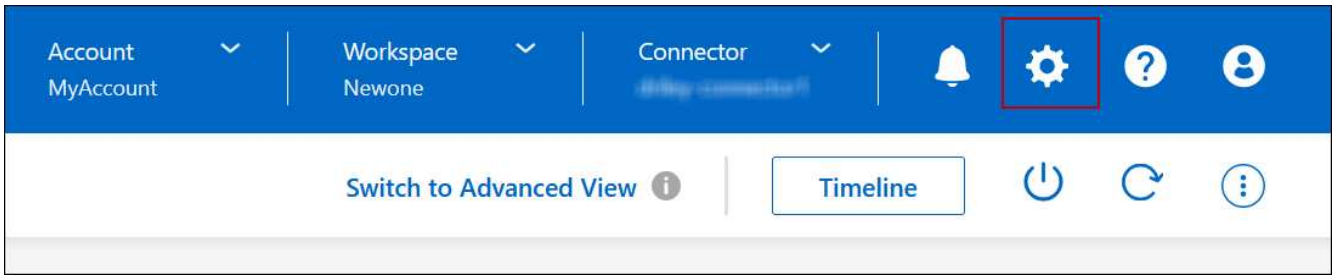
> このプロセスは、 CIFS クライアントの処理を中断する可能性があります。CIFS クライアントからコミットされていないデータは失われる可能性があります。

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、*[Cloud Volumes ONTAP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

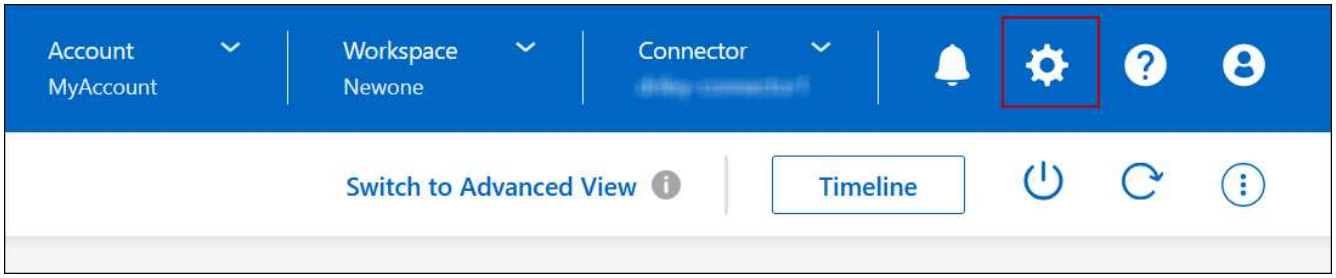
ビジネスで必要な場合は、BlueXPの設定を変更して、Azureプライベートリンクの代わりにサービスエンドポイントを使用するようにCloud Volumes ONTAP を設定できます。この設定を変更すると、新しく作成した環

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、*[Cloud Volumes ONTAP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

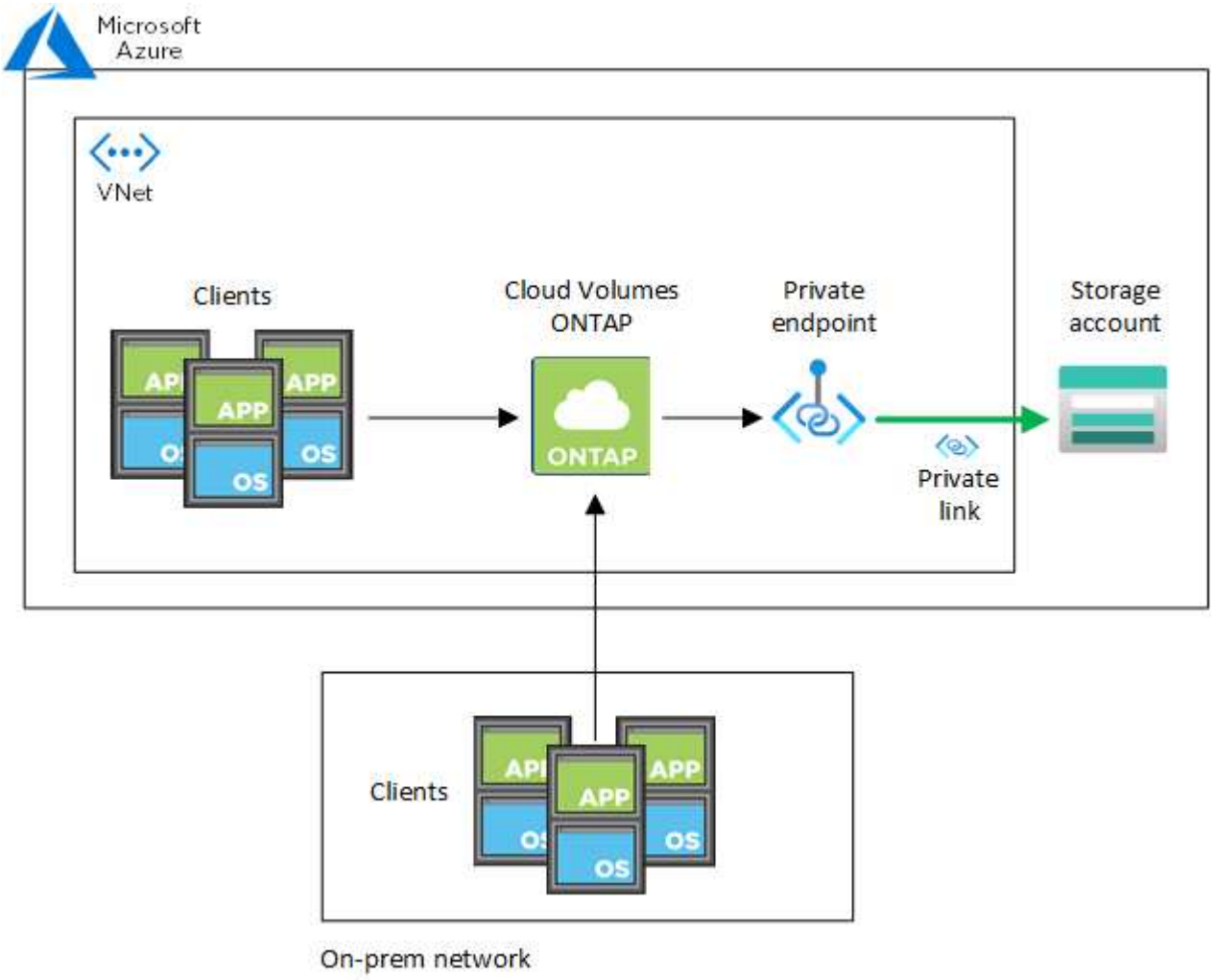
必要に応じて、カスタムDNSを使用する場合は、カスタムDNSサーバからAzureプライベートDNSゾーンに対する条件付きフォワーダを作成する必要があります。詳細については、を参照してください "DNSフォワーダを使用するAzureのドキュメント"。

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. 次の要求本文で 'put/occm/config’API 呼び出しを使用します

```
{ "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。

Azureで**SnapMirror**トラフィックを分離

AzureでCloud Volumes ONTAPを使用すると、SnapMirrorレプリケーションのトラフィックをデータトラフィックや管理トラフィックから分離できます。SnapMirrorレプリケーショントラフィックをデータトラフィックから分離するには、新しいネットワークインターフェイスカード（NIC）、関連付けられたクラスタ間LIF、およびルーティングされないサブネットを追加します。

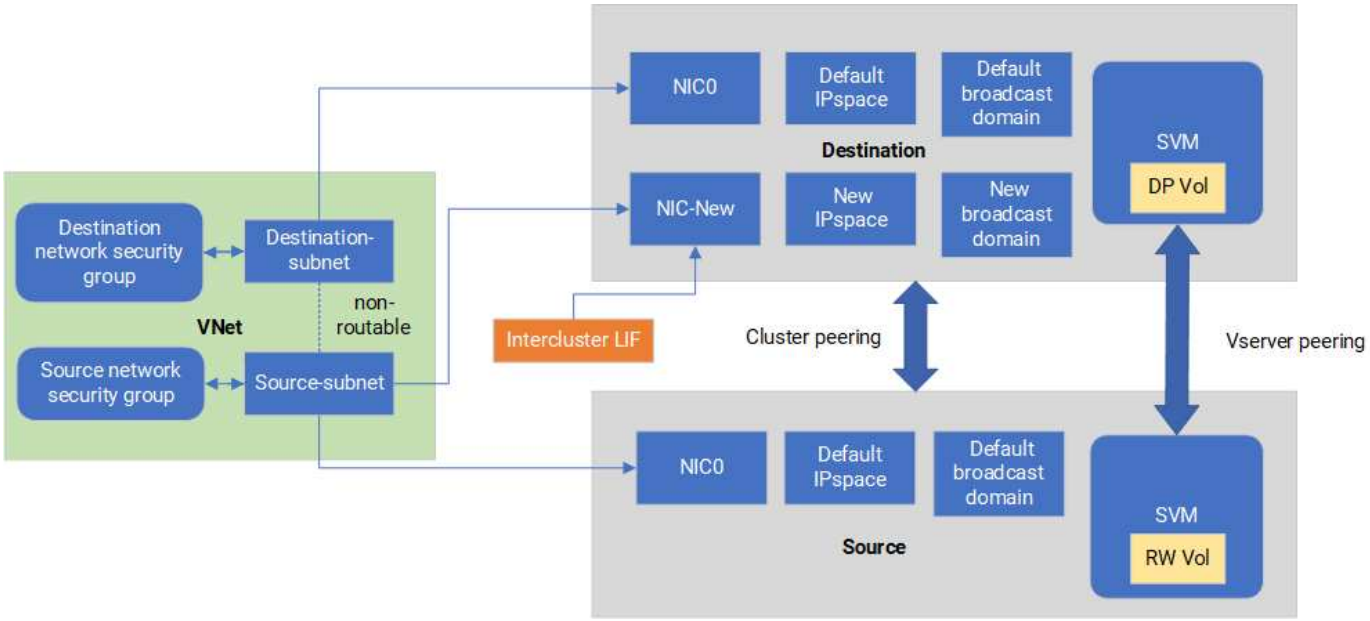
Azureでの**SnapMirror**トラフィックの分離について

デフォルトでは、すべてのNICとLIFが同じサブネット上のCloud Volumes ONTAP環境に設定されます。このような構成では、SnapMirrorレプリケーショントラフィックとデータトラフィックと管理トラフィックが同じ

サブネットを使用します。SnapMirrorトラフィックを分離すると、データトラフィックと管理トラフィックに使用されている既存のサブネットにルーティングできない追加のサブネットが使用されます。

図1

次の図は、1つのノード環境における、追加のNIC、関連付けられたクラスタ間LIF、およびルーティングされないサブネットを使用したSnapMirrorレプリケーショントラフィックの分離を示しています。HAペア構成の場合は若干異なります。



作業を開始する前に

次の考慮事項を確認してください。

- Cloud Volumes ONTAPのシングルノードまたはHAペア構成（VMインスタンス）には、SnapMirrorトラフィックを分離するためにNICを1つだけ追加できます。
- 新しいNICを追加するには、導入するVMインスタンスタイプに未使用のNICが必要です。
- ソースクラスタとデスティネーションクラスタが同じ仮想ネットワーク（VNet）にアクセスできる必要があります。デスティネーションクラスタはAzure内のCloud Volumes ONTAPシステムです。ソースクラスタには、AzureのCloud Volumes ONTAPシステムまたはONTAPシステムを使用できます。

手順1：追加のNICを作成してデスティネーションVMに接続する

このセクションでは、追加のNICを作成してデスティネーションVMに接続する方法について説明します。デスティネーションVMは、AzureのCloud Volumes ONTAP内のシングルノードまたはHAペアシステムで、追加のNICを設定します。

手順

1. ONTAP CLIで、ノードを停止します。

```
dest::> halt -node <dest_node-vm>
```

2. Azureポータルで、VM（ノード）のステータスがstoppedになっていることを確認します。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Azure Cloud ShellのBash環境を使用してノードを停止します。
   a. ノードを停止します。

   ```
   az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
   ```

   b. ノードの割り当てを解除します。

   ```
   az vm deallocate --resource-group <dest_node-rg> --name <dest_node-
   vm>
   ```

4. 2つのサブネット（ソースクラスタサブネットとデスティネーションクラスタサブネット）が相互にルーティングできないように、ネットワークセキュリティグループルールを設定します。
   a. デスティネーションVMに新しいNICを作成します。
   b. ソースクラスタのサブネットIDを検索します。

   ```
   az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet
   -name <vnet> --query id
   ```

   c. ソースクラスタのサブネットのサブネットIDを使用して、デスティネーションVMに新しいNICを作成します。ここでは、新しいNICの名前を入力します。

   ```
   az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new>
   --subnet <id_from_prev_command> --accelerated-networking true
   ```

   d. privateIPAddressを保存します。このIPアドレス（<new_added_nic_primary_addr>）は、クラスタ間LIFの作成に使用されます。 フロオトキヤストトメイン、シンシイNICノクラスタカンLIF。

5. 新しいNICをVMに接続します。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics
<dest_node-vm-nic-new>
```

6. VM（ノード）を起動します。

```
az vm start --resource-group <dest_node-rg>  --name <dest_node-vm>
```

7. Azureポータルで、* Networking *に移動し、新しいNIC（nic-newなど）が存在し、高速ネットワークが有効になっていることを確認します。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

HAペア構成の場合は、パートナーノードでも同じ手順を繰り返します。

手順2：新しいNIC用の新しいIPspace、ブロードキャストドメイン、クラスタ間LIFを作成する

クラスタ間LIF用に別のIPspaceを使用すると、クラスタ間のレプリケーション用にネットワーク機能を論理的に分離できます。

ONTAP CLIを使用して次の手順を実行します。

手順

1. 新しいIPspace（new_ipspace）を作成します。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 新しいIPspace（new_ipspace）にブロードキャストドメインを作成し、nic-newポートを追加します。

```
dest::> network port show
```

3. シングルノードシステムの場合、新しく追加されたポートは_e0b_です。管理対象ディスクを使用するHAペア環境の場合、新しく追加されるポートは_e0d_です。ページblobを使用するHAペア環境の場合、新しく追加されたポートは_e0e_です。VM名ではなくノード名を使用してください。次のコマンドでノード名を検索します。 `node show`。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 新しいブロードキャストドメイン（new_bd）と新しいNIC（nic-new）にクラスタ間LIFを作成します。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 新しいクラスタ間LIFが作成されたことを確認します。

```
dest::> net int show
```

HAペア構成の場合は、パートナーノードでも同じ手順を繰り返します。

手順3：ソースシステムとデスティネーションシステム間のクラスタピアリングを確認する

ここでは、ソースシステムとデスティネーションシステム間のピアリングを検証する手順について説明します。

ONTAP CLIを使用して次の手順を実行します。

手順

1. デスティネーションクラスタのクラスタ間LIFからソースクラスタのクラスタ間LIFにpingを送信できることを確認します。このコマンドはデスティネーションクラスタで実行されるため、デスティネーションIPアドレスはソースのクラスタ間LIFのIPアドレスになります。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
-destination <10.161.189.6>
```

2. ソースクラスタのクラスタ間LIFからデスティネーションクラスタのクラスタ間LIFにpingを送信できることを確認します。destinationは、destinationに作成された新しいNICのIPアドレスです。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
<10.161.189.18>
```

HAペア構成の場合は、パートナーノードでも同じ手順を繰り返します。

手順4：ソースシステムとデスティネーションシステム間にSVMピアリングを作成する

このセクションでは、ソースシステムとデスティネーションシステム間にSVMピア関係を作成する手順を説明します。

ONTAP CLIを使用して次の手順を実行します。

手順

1. ソースのクラスタ間LIFのIPアドレスを `-peer-addrs`。HAペアの場合は、両方のノードのソースクラスタ間LIFのIPアドレスを `-peer-addrs`。

```
dest::> cluster peer create -peer-addrs <10.161.189.6> -ipspace
<new_ipspace>
```

2. パスフレーズを入力して確認します。
3. デスティネーションクラスタLIFのIPアドレスを `peer-addrs`。HAペアの場合は、両方のノードのデスティネーションクラスタ間LIFのIPアドレスを `-peer-addrs`。

```
src::> cluster peer create -peer-addrs <10.161.189.18>
```

4. パスフレーズを入力して確認します。
5. クラスタがピアリングされていることを確認します。

```
src::> cluster peer show
```

ピアリングに成功すると、[availability]フィールドに*[available]

6. デスティネーションでSVMピア関係を作成します。ソースとデスティネーションの両方のSVMがデータSVMである必要があります。

```
dest::> vserver peer create -vserver <dest_svm> -peer-vserver <src_svm>
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVMピアリングを承認

```
src::> vserver peer accept -vserver <src_svm> -peer-vserver <dest_svm>
```

8. SVMがピアリングされていることを確認します。

```
dest::> vserver peer show
```

ピアの状態が表示される **peered***ピアリングアプリケーションは ***snapmirror**

手順**5**：ソースシステムとデスティネーションシステム間に**SnapMirror**レプリケーション関係を作成する

このセクションでは、ソースシステムとデスティネーションシステム間にSnapMirrorレプリケーション関係を作成する手順について説明します。

既存のSnapMirrorレプリケーション関係を移動するには、新しいSnapMirrorレプリケーション関係を作成する前に、既存のSnapMirrorレプリケーション関係を解除する必要があります。

ONTAP CLIを使用して次の手順を実行します。

手順

1. デスティネーションSVMにデータ保護ボリュームを作成します。

```
dest::> vol create -volume <new_dest_vol> -vserver <dest_svm> -type DP
-size <10GB> -aggregate <aggr1>
```

2. SnapMirrorポリシーとレプリケーションスケジュールを指定して、デスティネーションでSnapMirrorレプリケーション関係を作成します。

```
dest::> snapmirror create -source-path src_svm:src_vol  -destination
-path  dest_svm:new_dest_vol -vserver dest_svm -policy
MirrorAllSnapshots -schedule 5min
```

3. デスティネーションでSnapMirrorレプリケーション関係を初期化します。

```
dest::> snapmirror initialize -destination-path  <dest_svm:new_dest_vol>
```

4. ONTAP CLIで次のコマンドを実行して、SnapMirror関係のステータスを検証します。

```
dest::> snapmirror show
```

関係のステータスはです。 `Snapmirrored` 関係の健全性は `true`。

5. オプション：ONTAP CLIで次のコマンドを実行して、SnapMirror関係の操作履歴を表示します。

```
dest::> snapmirror show-history
```

必要に応じて、ソースボリュームとデスティネーションボリュームをマウントし、ソースにファイルを書き込み、ボリュームがデスティネーションにレプリケートされていることを確認できます。

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。

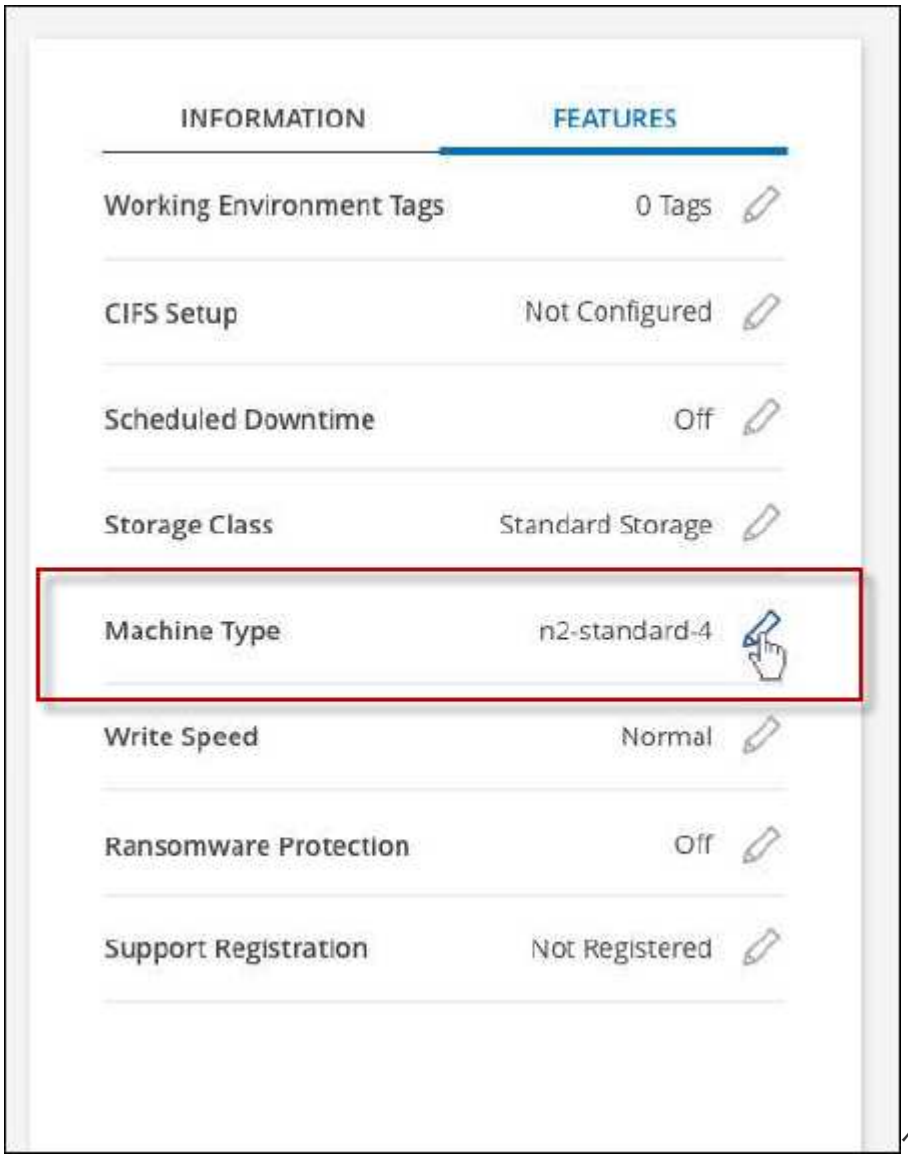
  シングルノードシステムの場合、 I/O は中断されます。

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。

の機能

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。

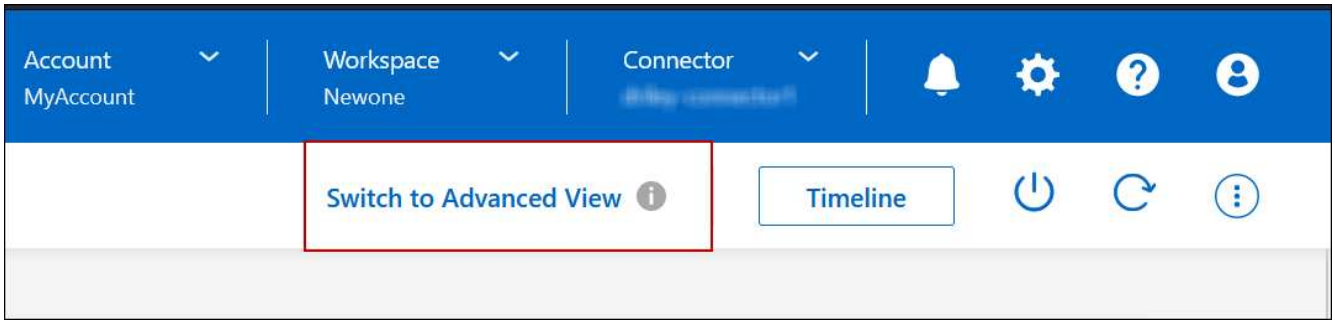
また、System Managerからのロールベースアクセス制御はサポートされていません。

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。

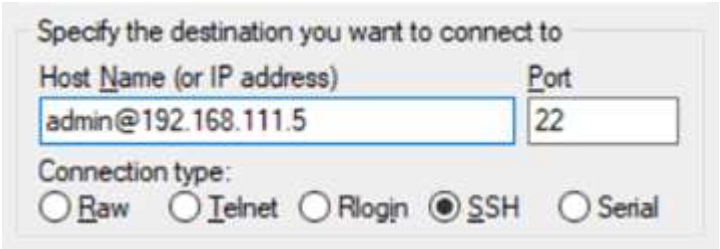
> 複数の AZS に導入されている場合、 Cloud Volumes ONTAP HA 構成では、クラスタ管理インターフェイスにフローティング IP アドレスが使用されます。これは、外部ルーティングが使用できないことを意味します。同じルーティングドメインの一部であるホストから接続する必要があります。

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-sdetails」

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」の略

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-sdetails」

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. 「/opt/application/netapp/cloudmanager/docker _occm/data/`」に移動します
9. プロキシ構成ファイルsquid.confを開きます

   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 cvsonet src <CIDR>`」と入力します

    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 cvsonet」というメッセージが表示されます

    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-sdetails」

EMS を設定します

Event Management System （ EMS ；イベント管理システム）は、 ONTAP システムで発生したイベントについて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"。

著作権に関する情報

商標に関する情報