



システム管理

Cloud Volumes ONTAP

NetApp
May 28, 2024

目次

| | |
|---|----|
| システム管理 | 1 |
| Cloud Volumes ONTAP ソフトウェアをアップグレードします | 1 |
| 従量課金制システムの登録 | 9 |
| Cloud Volumes ONTAP の状態の管理 | 12 |
| NTP を使用してシステム時刻を同期します | 15 |
| システムの書き込み速度を変更する | 15 |
| Cloud Volumes ONTAP のパスワードを変更します | 17 |
| システムを追加、削除、または削除します | 18 |
| AWSの管理 | 21 |
| Azureの管理 | 25 |
| Google Cloudの管理 | 37 |
| 拡張ビューを使用してCloud Volumes ONTAP を管理します | 39 |
| CLIからCloud Volumes ONTAP を管理します | 41 |

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 |

| 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 |
|----------|--------------------|
| 9.10.1 | 9.11.1 |
| | 9.11.0 |
| 9.10.0 | 9.10.1 |
| 9.9.1 | 9.10.1 |
| | 9.10.0 |
| 9.9.0 | 9.9.1 |
| 9.8 | 9.9.1 |
| 9.7 | 9.8 |
| 9.6 | 9.7 |
| 9.5 | 9.6 |
| 9.4 | 9.5 |
| 9.3 | 9.4 |
| 9.2 | 9.3 |
| 9.1 | 9.2 |
| 9.0 | 9.1 |
| 8.3 | 9.0 |

次の点に注意してください。

- Cloud Volumes ONTAP でサポートされるアップグレードパスは、オンプレミスの ONTAP クラスタの場合とは異なります。
- 作業環境に表示されるアップグレード通知に従ってアップグレードすると、これらのサポートされているアップグレードパスに続くリリースにアップグレードするように求められます。
- HTTPS の場所にアップグレードイメージを配置してアップグレードする場合は、サポートされているアップグレードパスに従ってください。
- 場合によっては、ターゲットリリースに到達するために数回アップグレードが必要になることがあります。

たとえば、バージョン 9.8 を実行していて、9.10.1 にアップグレードする場合は、まずバージョン 9.9.1 にアップグレードしてから 9.10.1 にアップグレードする必要があります。

パッチリリース

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イメージシナリオ](#)。

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。

| Aggregate Details | |
|---------------------|---------------------|
| aggr1 | |
| Overview | Capacity Allocation |
| Provider Properties | |
| State | online |
| Home Node | [redacted] |
| Encryption Type | cloudEncrypted |
| Volumes | 2 ▾ |

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」"。

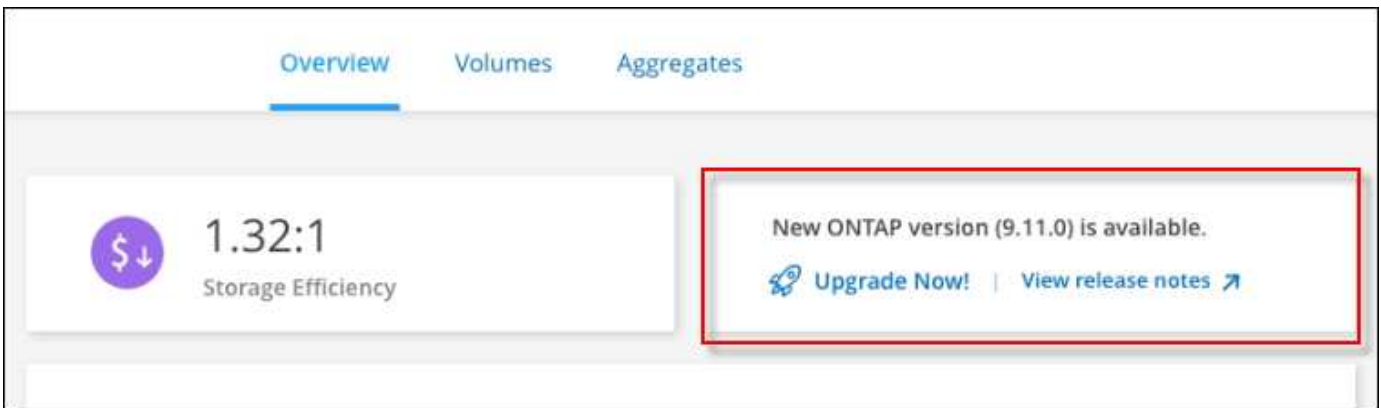
Cloud Volumes ONTAP をアップグレードします

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。

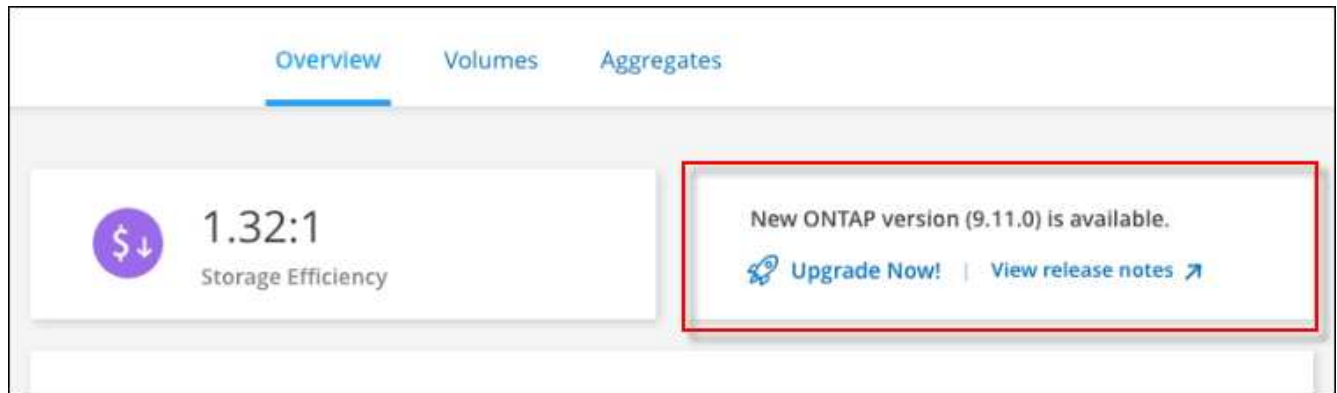
作業を開始する前に

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

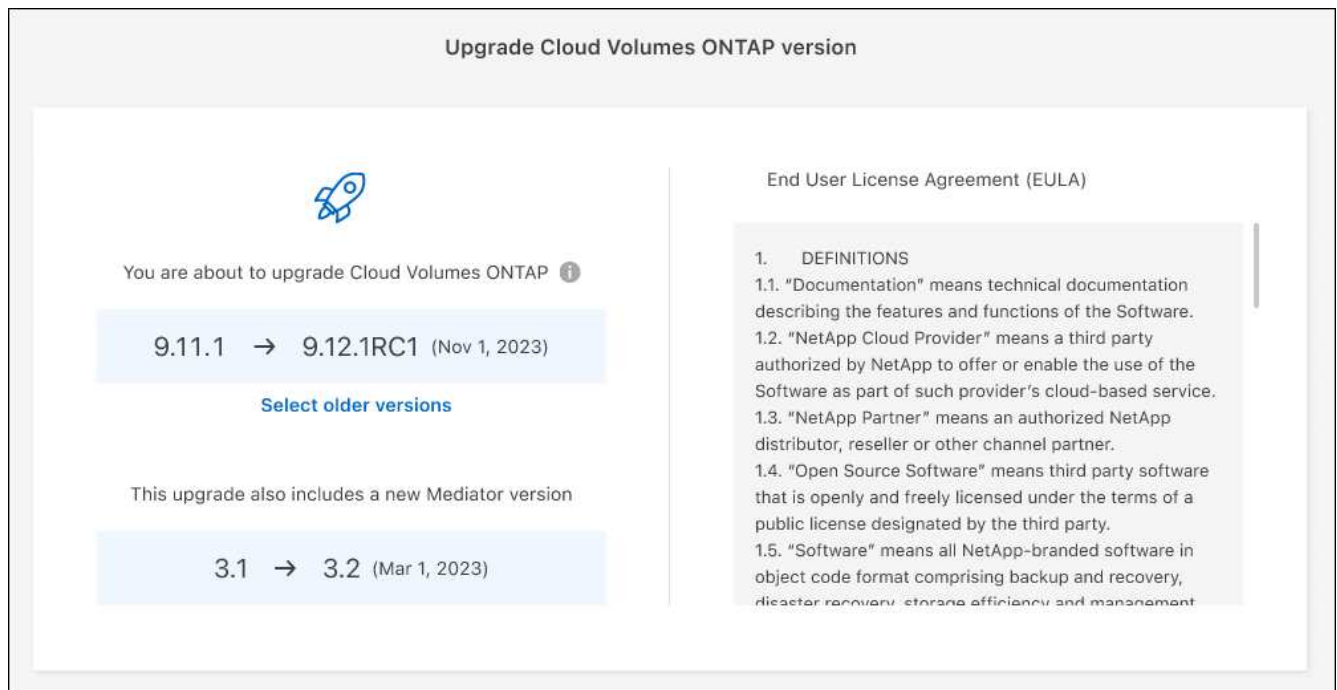


BlueXPの通知を通じてCloud Volumes ONTAPをアップグレードするには、NetApp Support Siteアカウントが必要です。

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。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/

- 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。
- [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://&lt;Connector-private-IP-address&gt;/ontap/images/&lt;image-file-name&gt;" class="bare">http://&lt;Connector-private-IP-address&gt;/ontap/images/&lt;image-file-name&gt;</a>;
```



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。

- [* 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

- 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。

| Information | Features |
|--------------------------|--|
| Working Environment Tags | Tags  |
| Scheduled Downtime | Off  |
| S3 Storage Classes | Standard-Infrequent Access  |
| Instance Type | m5.xlarge  |
| Write Speed | Normal  |
| Ransomware Protection | Off  |
| Support Registration | Not Registered  |
| CIFs Setup |  |

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ルリングします。
- 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。

| Information | Features |
|--------------------------|--|
| Working Environment Tags | Tags  |
| Scheduled Downtime | Off  |
| S3 Storage Classes | Standard-Infrequent Access  |
| Instance Type | m5.xlarge  |
| Write Speed | Normal  |
| Ransomware Protection | Off  |
| Support Registration | Not Registered  |
| CIFs Setup |  |

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

Schedule Downtime

Cloud Manager Time Zone: 17:58 UTC

Select when to turn off your Working Environment:

Turn off every day at 20 : 00 for 12 hours (1-24)
Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays at 20 : 00 for 12 hours (1-24)
Mon, Tue, Wed, Thu, Fri

Turn off every weekend at 20 : 00 for 12 hours (1-48)
Sat

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。



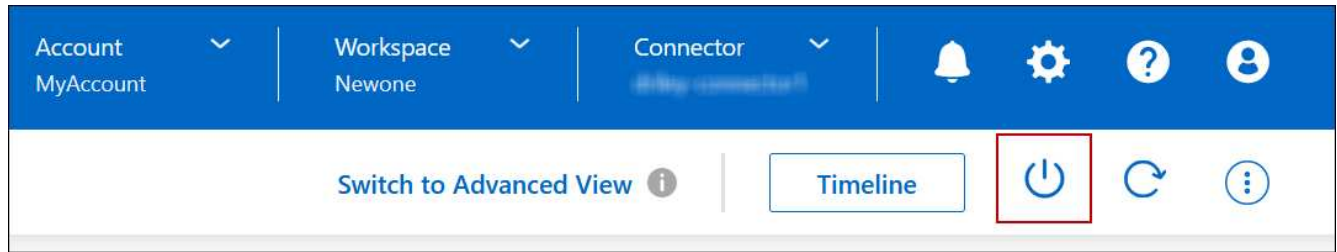
コストを削減するため、BlueXPは定期的にルートディスクと起動ディスクの古いスナップショットを削除します。ルートディスクとブートディスクの両方に対して、最新の2つの Snapshot のみが保持されます。

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、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、リポ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。

| Information | | Features |
|--------------------------|----------------------------|---|
| Working Environment Tags | | Tags  |
| Scheduled Downtime | | Off  |
| S3 Storage Classes | Standard-Infrequent Access |  |
| Instance Type | m5.xlarge |  |
| Write Speed | Normal |  |
| Ransomware Protection | | Off  |
| Support Registration | Not Registered |  |
| CIFs Setup | |  |

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

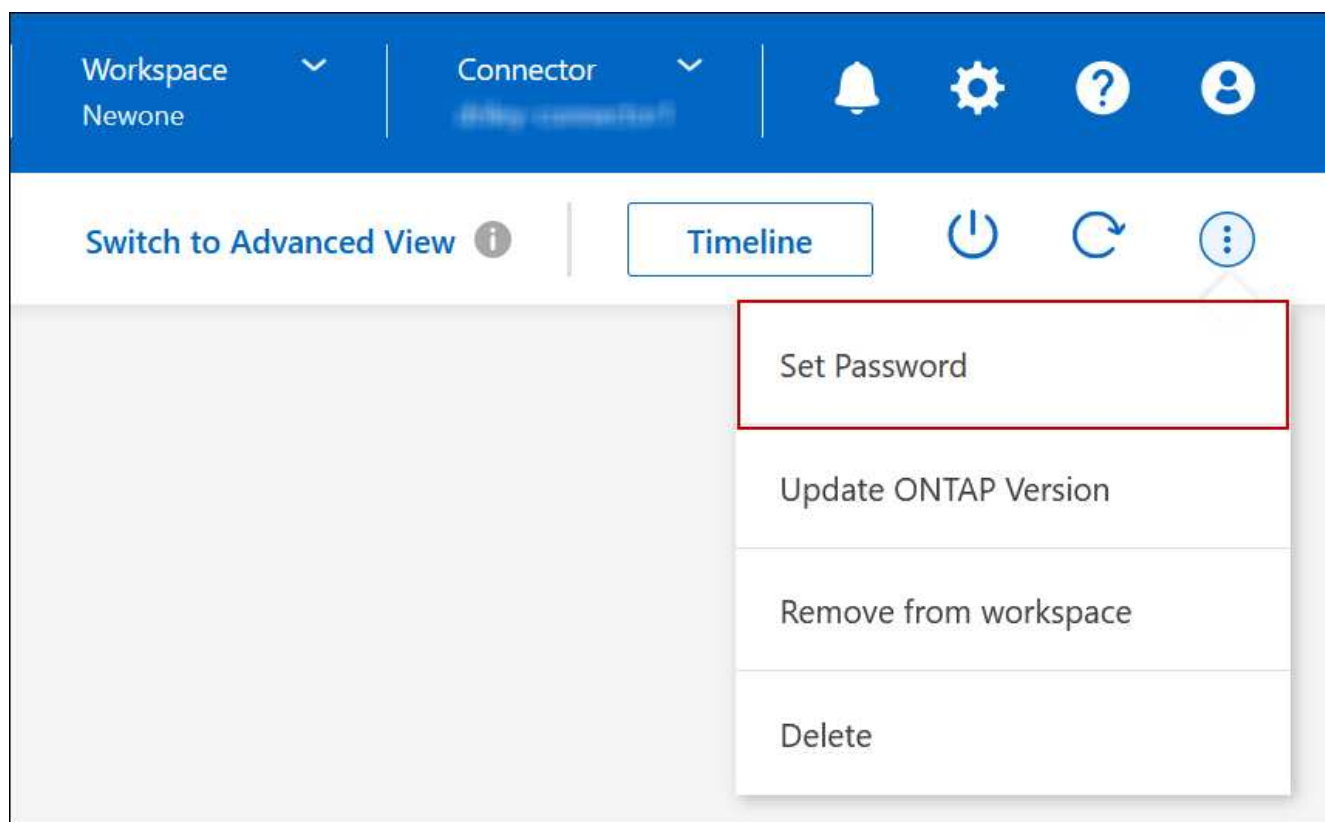
Cloud Volumes ONTAP にはクラスタ管理者アカウントが含まれています。必要に応じて、このアカウントのパスワードをBlueXPから変更できます。



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。

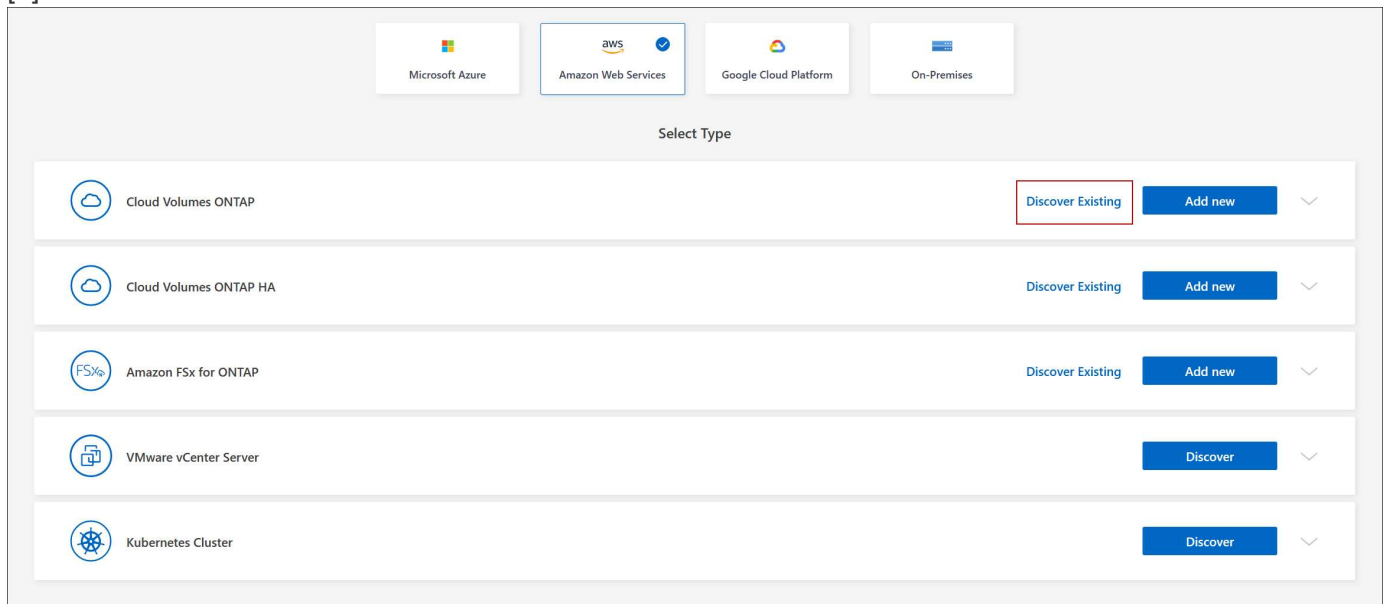
作業を開始する前に

Cloud Volumes ONTAP 管理者ユーザー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

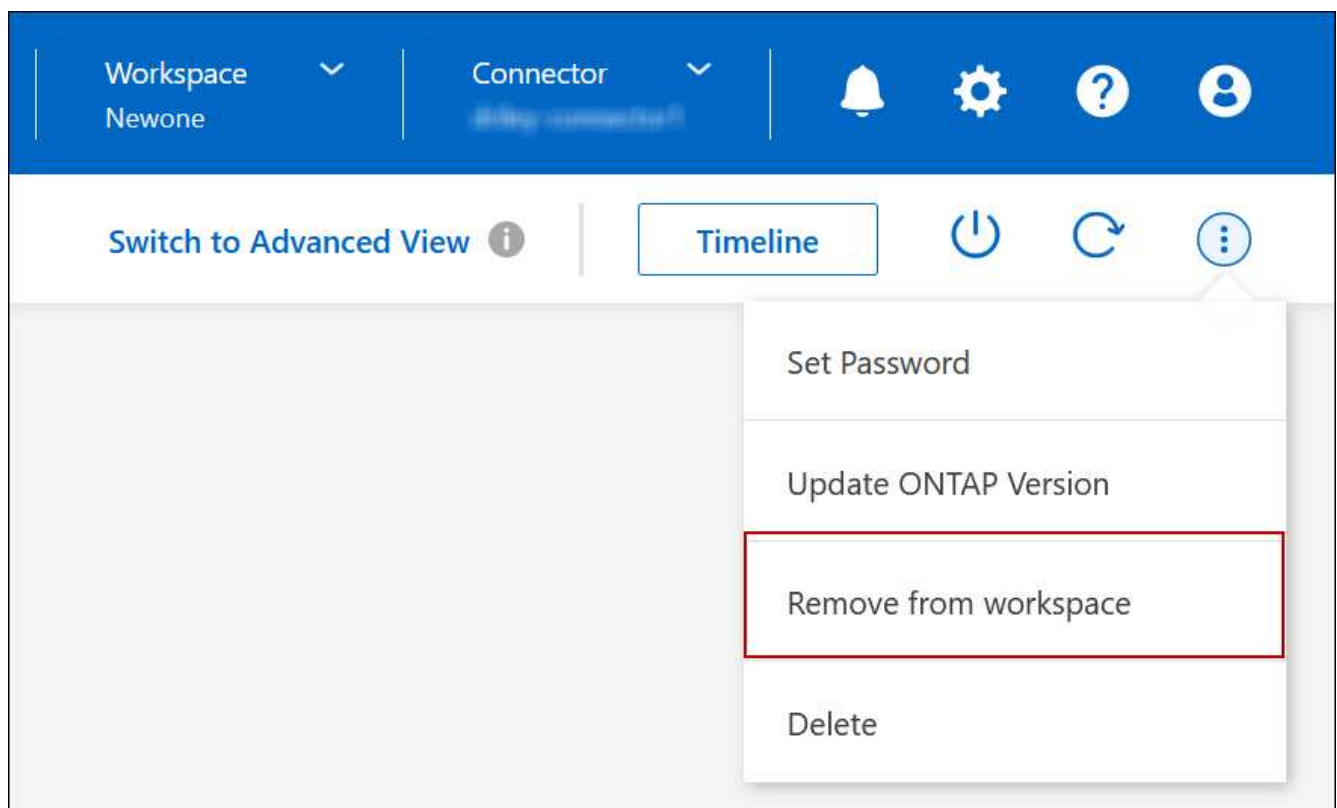
Cloud Volumes ONTAP 作業環境を削除するとBlueXPから削除されます。Cloud Volumes ONTAP システムは削除されません。作業環境は後で再検出できます。

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

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

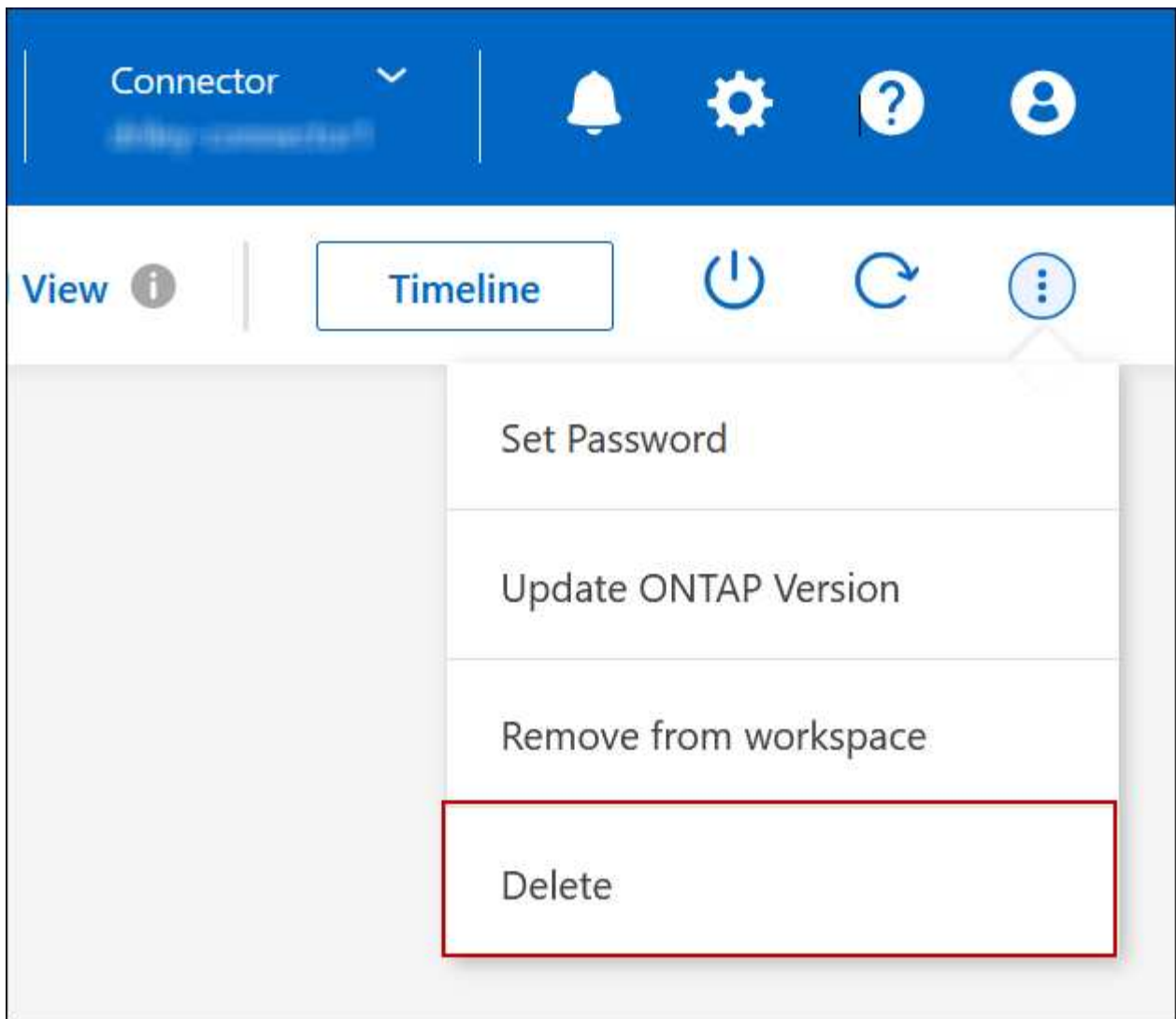
1. 作業環境でBlueXPのバックアップとリカバリを有効にした場合は、バックアップデータが引き続き必要かどうかを確認し、実行します ["必要に応じて、バックアップを削除します"](#)。

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、技術情報アート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。

| Information | Features |
|--------------------------|--|
| Working Environment Tags | Tags  |
| Scheduled Downtime | Off  |
| S3 Storage Classes | Standard-Infrequent Access  |
| Instance Type | m5.xlarge  |
| Write Speed | Normal  |
| Ransomware Protection | Off  |
| Support Registration | Not Registered  |
| CIFs Setup |  |

- 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

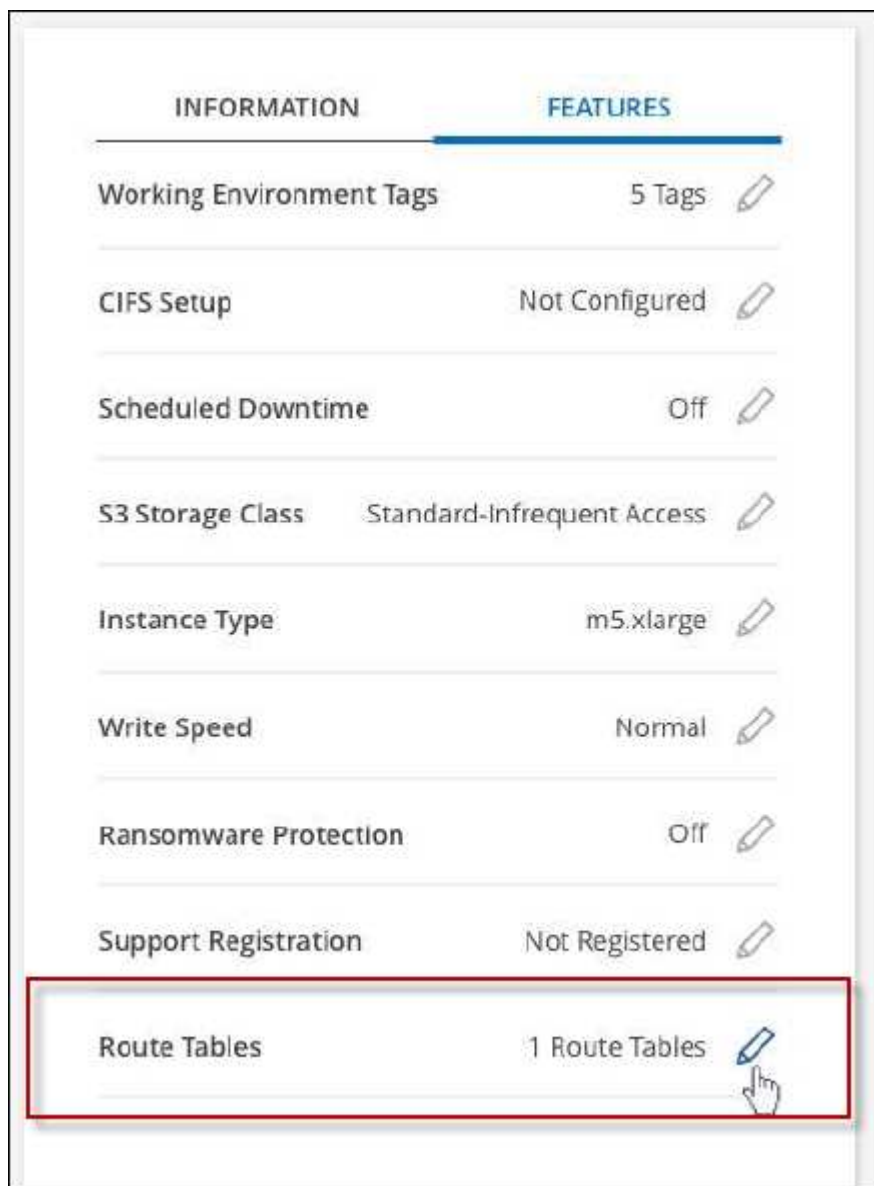
Cloud Volumes ONTAP が新しい設定でリブートします。

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。

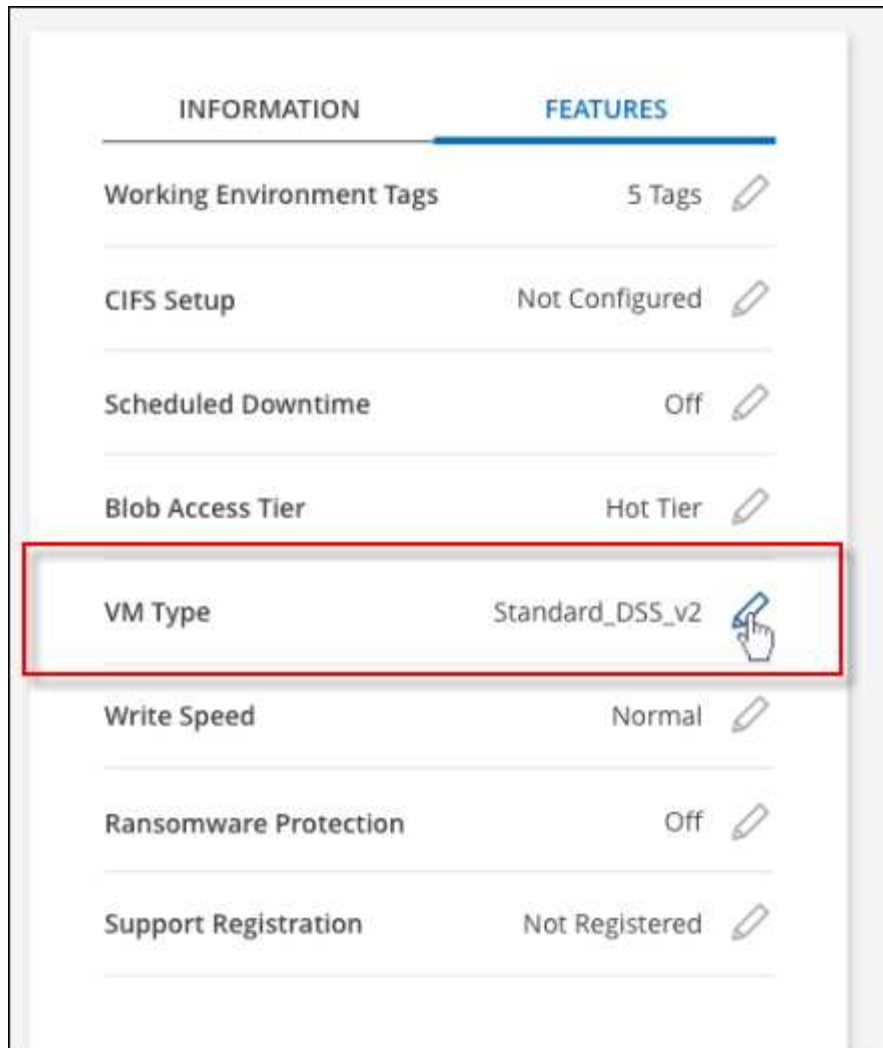
HA ペアの場合、変更は中断されません。HA ペアは引き続きデータを提供します。



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 が新しい設定でリポートします。

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。



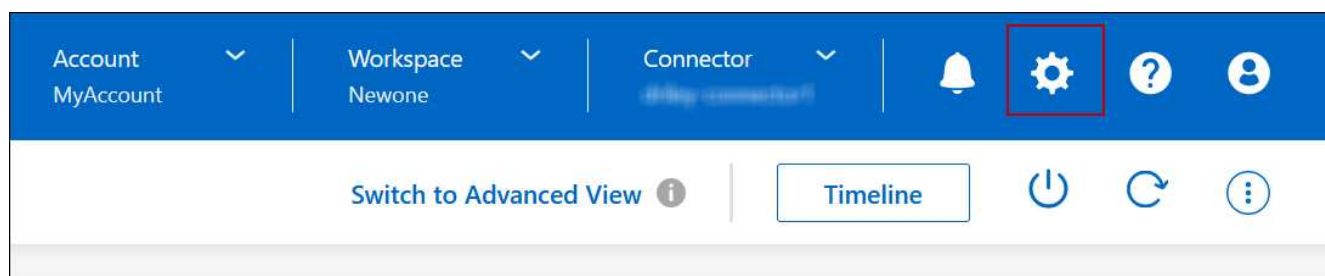
このプロセスは、CIFS クライアントの処理を中断する可能性があります。CIFS クライアントからコミットされていないデータは失われる可能性があります。

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

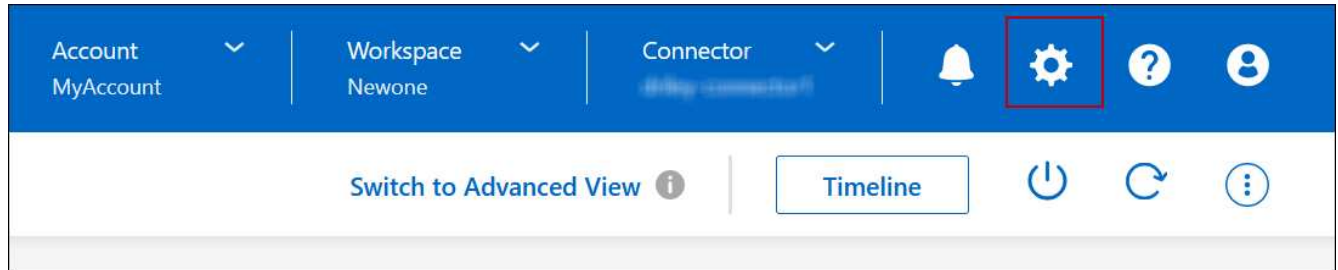
ビジネスで必要な場合は、BlueXPの設定を変更して、Azureプライベートリンクの代わりにサービスエンドポイントを使用するようにCloud Volumes ONTAP を設定できます。この設定を変更すると、新しく作成した環

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

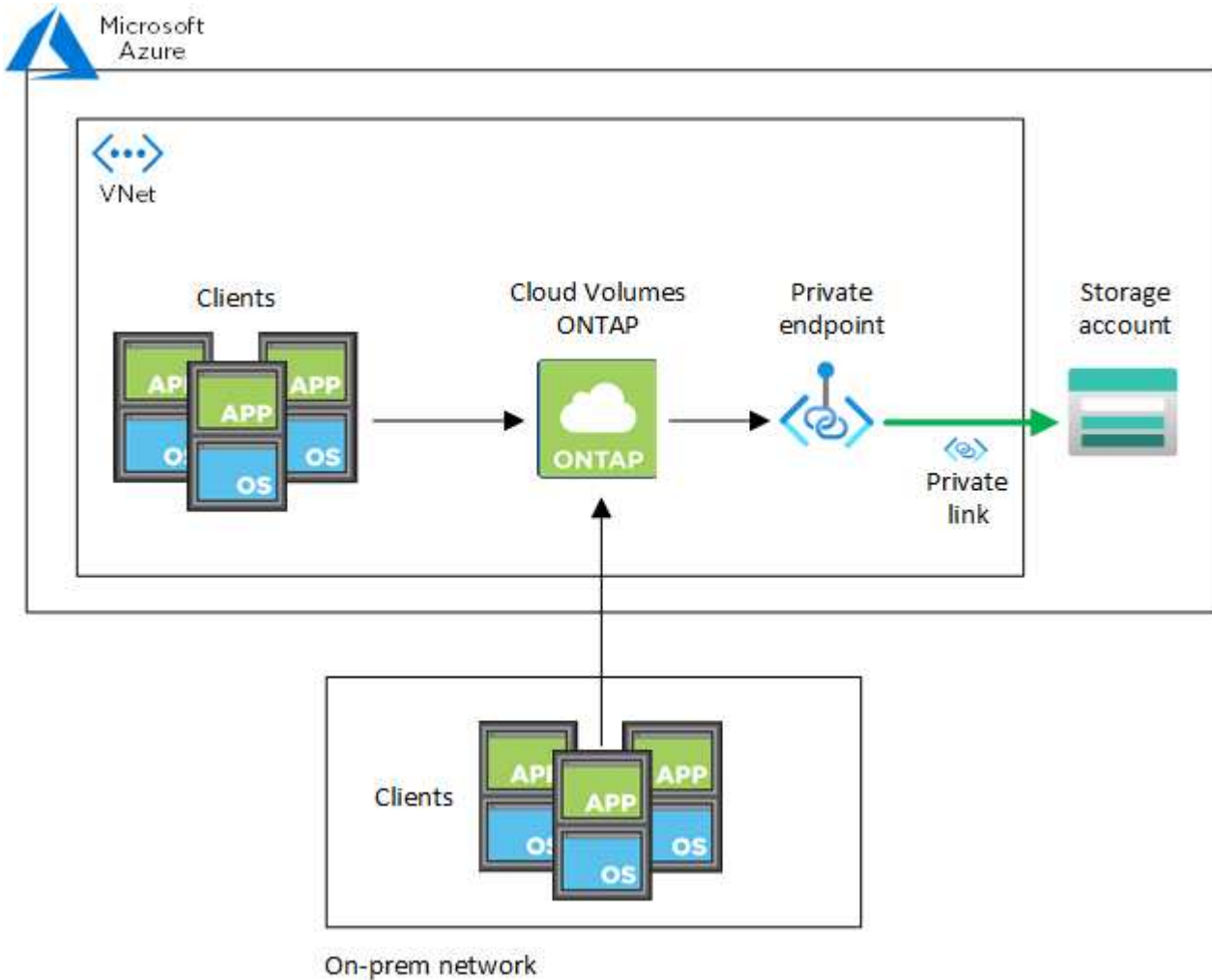
必要に応じて、カスタムDNSを使用する場合は、カスタムDNSサーバからAzureプライベートDNSゾーンに対する条件付きフォワーダを作成する必要があります。詳細については、[を参照してください "DNSフォワーダを使用するAzureのドキュメント"](#)。

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ー間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。

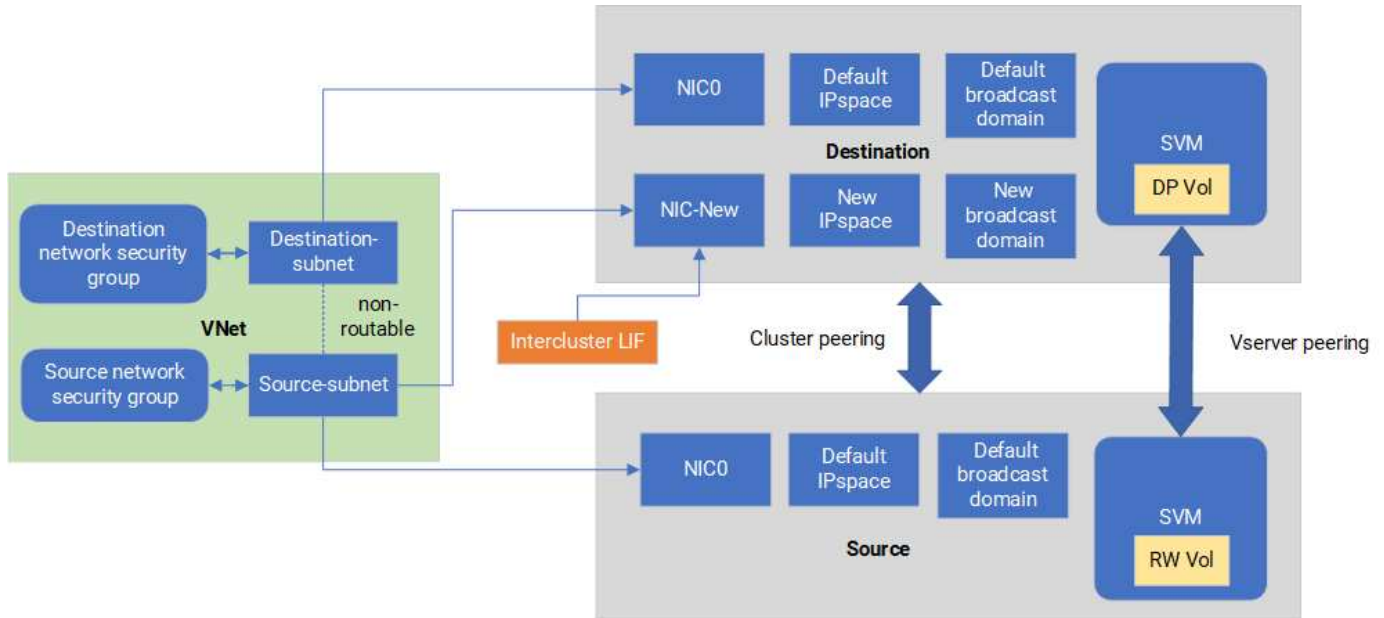
AzureでのSnapMirrorトラフィックの分離について

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ー間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。
- ソースクラスターとデスティネーションクラスター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ーはAzure内のCloud Volumes ONTAPシステムです。ソースクラスターには、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。 [フロートキャストトメイン](#)、[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-addr`s。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-addr`s。

```
dest::> cluster peer create -peer-addr s <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-addr`s。HAペアの場合は、両方のノードのデステ

イネーションクラスタ間LIFのIPアドレスを `-peer-addr`。

```
src::> cluster peer create -peer-addr <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。

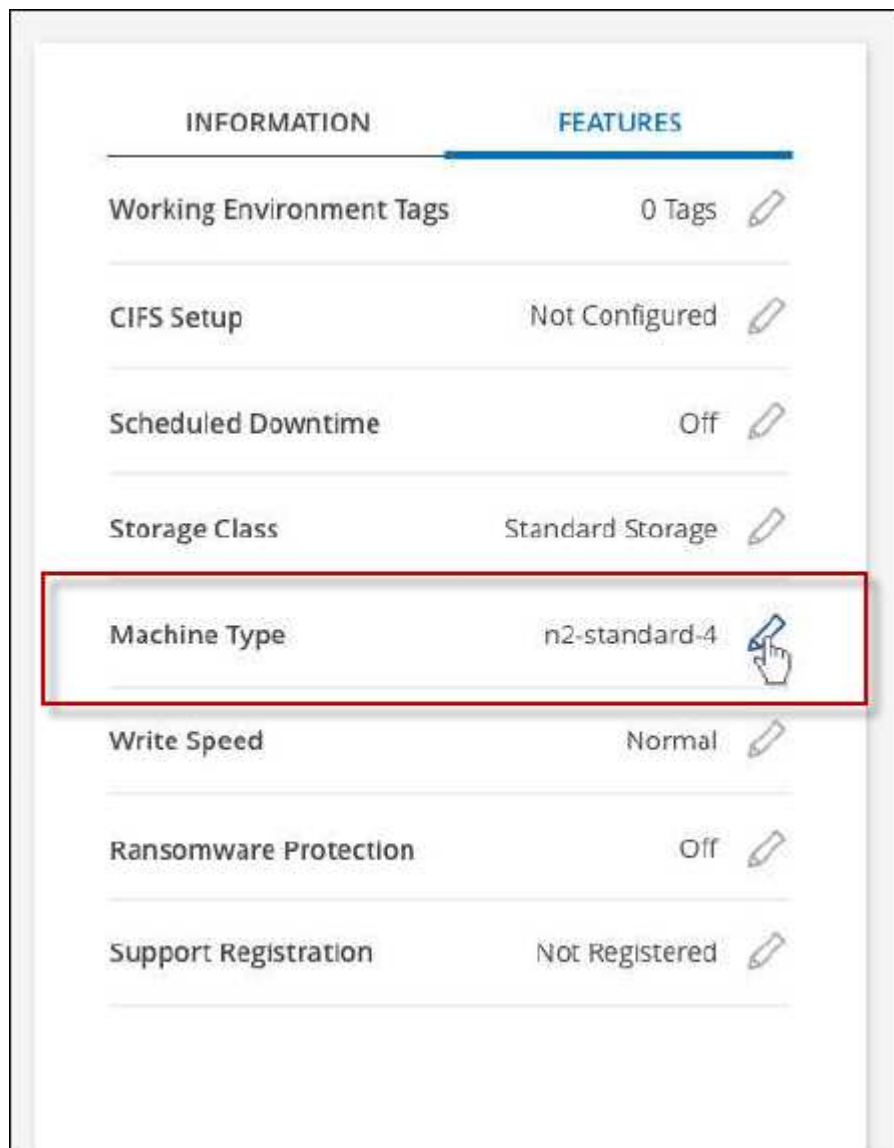
HA ペアの場合、変更は中断されません。HA ペアは引き続きデータを提供します。



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。

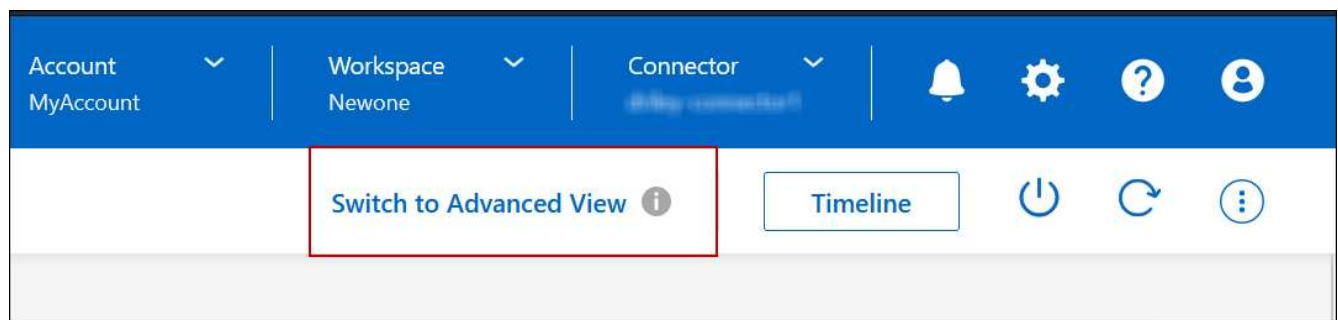
また、System Managerからのロールベースアクセス制御はサポートされていません。

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::>

著作権に関する情報

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

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

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

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

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

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

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

商標に関する情報

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