



Cloud Volumes ONTAP を使用します

Cloud Volumes ONTAP

NetApp
April 12, 2022

目次

Cloud Volumes ONTAP を使用します	1
ライセンス管理	1
ボリュームと LUN の管理	11
アグリゲートの管理	40
Storage VM 管理	41
セキュリティとデータ暗号化	55
システム管理	57
システムの健全性とイベント	79

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

容量ベースのライセンスをデジタルウォレットから管理して、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があることを確認します。

_ 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。

_ Digital Wallet では、Cloud Volumes ONTAP のライセンスを 1 箇所から管理できます。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

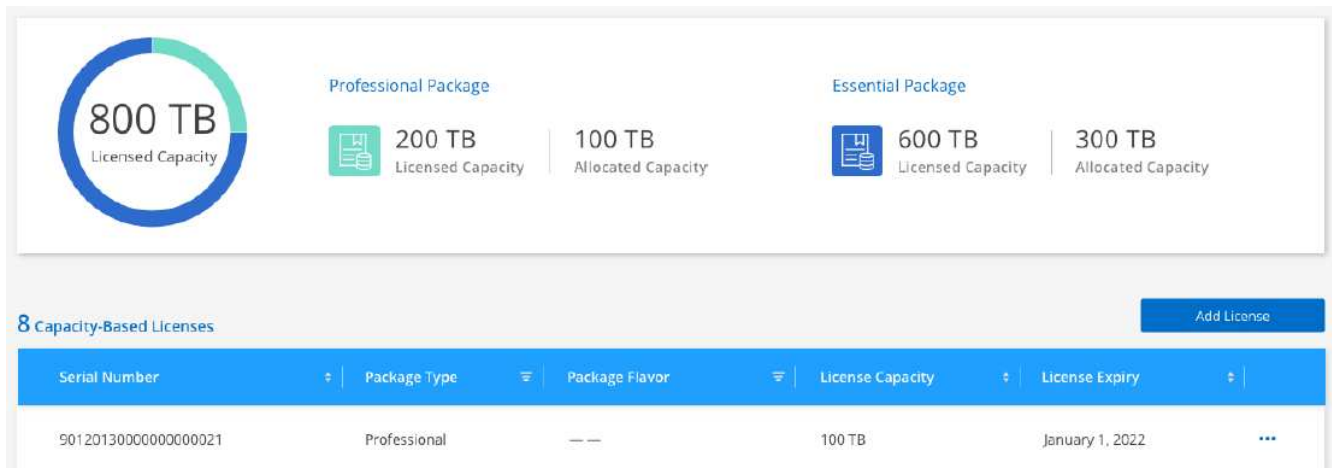
"Cloud Volumes ONTAP ライセンスの詳細については、[こちらをご覧ください](#)。"

アカウントの容量を表示します

パッケージごとにライセンスで許可された容量とプロビジョニング済み容量を表示して、データボリューム用の十分なスペースを確保します。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. Capacity Based Licenses * を選択した場合は、各パッケージのライセンス容量とプロビジョニング済み容量が表示されます。



3. 必要に応じて、ライセンスで許可された容量を追加で購入し、アカウントにライセンスを追加します。

購入済みライセンスをアカウントに追加します

ネットアップアカウントのライセンスを購入したら、Cloud Volumes ONTAP で容量を使用できるように、Cloud Manager にライセンスを追加する必要があります。

必要なもの

- Cloud Manager にライセンスのシリアル番号またはライセンスファイルを指定する必要があります。
- シリアル番号を入力する場合は、最初に必要なです ["Cloud Manager にネットアップサポートサイトのアカウントを追加します"](#)。シリアル番号へのアクセスが許可されているネットアップサポートサイトのアカウントです。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. [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期間を延長した場合は、Cloud Manager によってデジタルウォレットのライセンスが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 Cloud Manager を導入した場合は、Cloud Manager でライセンスを手動で更新する必要があります。

ライセンスファイル（HA ペアがある場合は *files*）。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。
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。

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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。
3. [削除（Remove）] をクリックして確定します。

Keystone Flex Subscriptions を管理します

Cloud Volumes ONTAP でサブスクリプションを使用できるようにすることで、デジタルウォレットから Keystone Flex Subscriptions を管理できます。コミット済み容量に対する変更を要求したり、サブスクリプションのリンクを解除したりすることもできます。

a_Keystone Flex Subscription_ は、ネットアップが提供する、ビジネスの成長に合わせて拡張できるストレージサービスです。

Digital Wallet では、Cloud Volumes ONTAP のライセンスを 1 箇所から管理できます。新しいライセンスを追加したり、既存のライセンスを更新したりできます。

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

アカウントを承認します

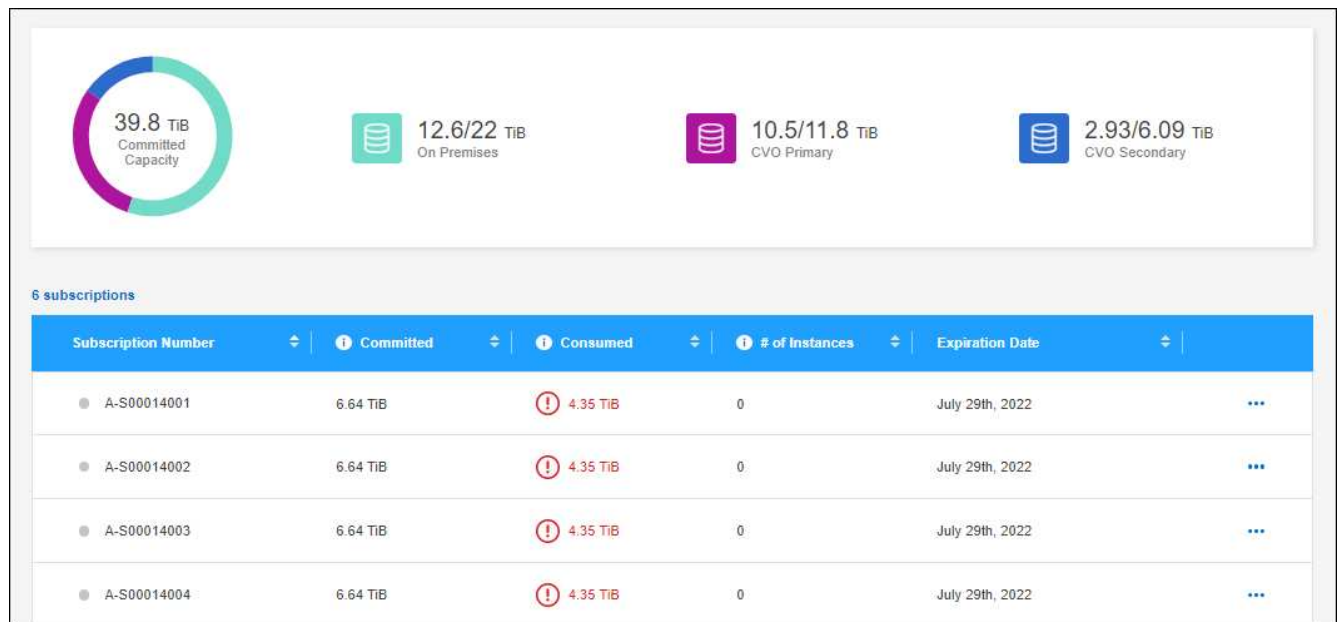
Cloud Manager で Keystone Flex Subscriptions を使用して管理する前に、ネットアップに連絡して、Keystone Flex Subscriptions で Cloud Manager ユーザアカウントを承認する必要があります。

手順

1. [* すべてのサービス] > [デジタルウォレット *] をクリックします。
2. [* Keystone Flex Subscription *] をクリックします。
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. サブスクリプションを確認するには、* Keystone Flex Subscription * に戻ってください。



Cloud Volumes ONTAP で使用するサブスクリプションをリンクします。

サブスクリプションをリンクします

ネットアップがアカウントを承認したら、Keystone Flex Subscriptions をリンクして Cloud Volumes ONTAP で使用できるようにする必要があります。この操作により、新しい Cloud Volumes ONTAP システムの充電方法としてサブスクリプションを選択できます。

手順

1. [* すべてのサービス] > [デジタルウォレット *] をクリックします。
2. [* Keystone Flex Subscription*] をクリックします。
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。

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

これで、Cloud Manager アカウントにリンクされ、Cloud Volumes ONTAP の作業環境を作成する際に選択できるようになります。



コミット済み容量を増やして申請してください

サブスクリプションのコミット済み容量を調整する必要がある場合は、Cloud Manager のインターフェイスから直接要求を送信できます。

手順

1. [* すべてのサービス] > [デジタルウォレット *] をクリックします。
2. [* Keystone Flex Subscription*] をクリックします。
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。

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	<input type="text" value="Enter amount"/> TiB
Premium	0.977 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB
Performance	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
Standard	0.732 TiB	0.439 TiB	<input type="text" value="Enter amount"/> TiB
Value	0.977 TiB	 0.879 TiB	<input type="text" value="Enter amount"/> TiB
Data Tiering	0 TiB	0 TiB	<input type="text" value="Enter amount"/> TiB
CVO Primary	1.96 TiB	 1.76 TiB	<input type="text" value="3"/> TiB
CVO Secondary	1.02 TiB	0.488 TiB	<input type="text" value="Enter amount"/> TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

Submit
Cancel


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。

リクエストに応じて、ネットアップのシステムで処理用のチケットが作成されます。

サブスクリプションのリンクを解除します

新しい Cloud Volumes ONTAP システムで Keystone Flex 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. [* すべてのサービス] > [デジタルウォレット *] をクリックします。
2. [* Keystone Flex Subscription*] をクリックします。
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。

このサブスクリプションへのリンクが Cloud Manager アカウントから解除され、Cloud Volumes ONTAP の作業環境を作成する際に選択できなくなります。

ノードベースのライセンスを管理します

デジタルウォレットでノードベースのライセンスを管理して、各 Cloud Volumes ONTAP

システムに必要な容量の有効なライセンスがあることを確認します。

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

_Digital Wallet では、Cloud Volumes ONTAP のライセンスを 1 箇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。

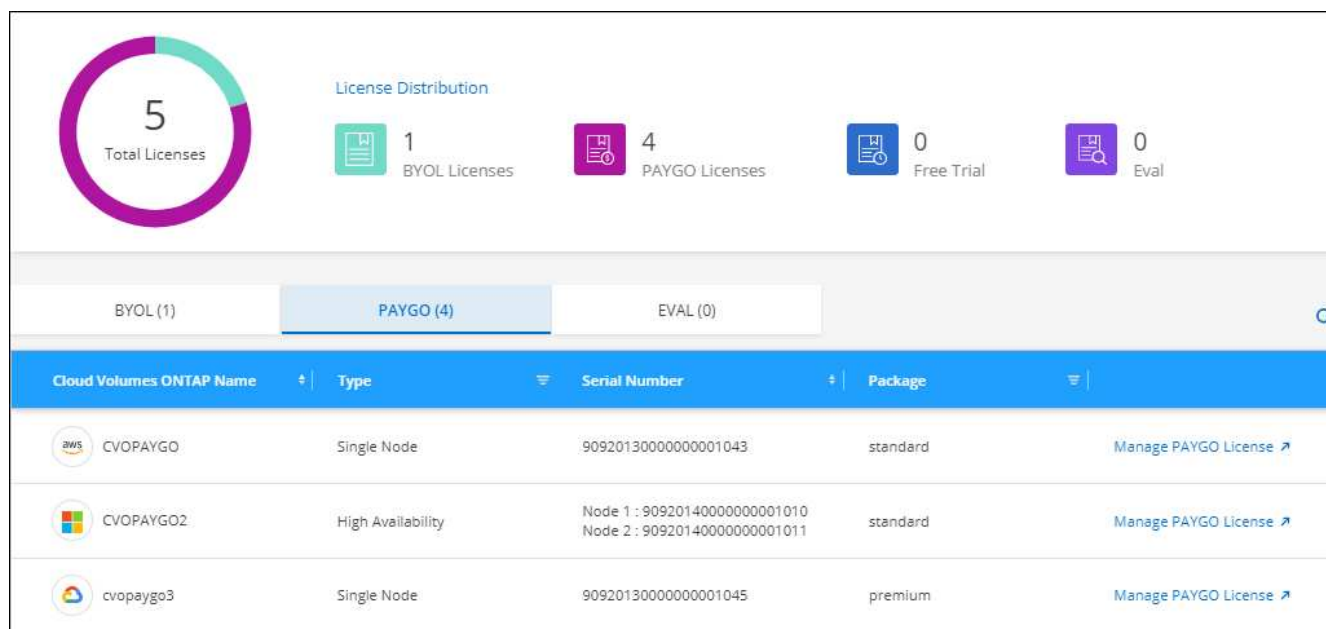
"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

PAYGO ライセンスを管理します

デジタルウォレットページでは、シリアル番号と PAYGO ライセンスタイプを含む、PAYGO Cloud Volumes ONTAP の各システムに関する詳細を表示できます。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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

ノードベースのライセンスをデジタルウォレットに追加して、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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。

Cloud Manager によってデジタルウォレットにライセンスが追加されます。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。その場合、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 用の未割り当てのノードベースライセンスがあり、使用していない場合は、そのライセンスを Cloud Backup ライセンス、Cloud Data Sense ライセンス、Cloud Tiering ライセンスに変換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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。

BYOL (14)	Eval (2)	Unassigned (3)	PAYGO (6)	<div> <div>Q</div> <div>Add Unassigned Licenses</div> </div>		
Serial Number	Type	Cloud Provider	License Expiry	Status		
012345678901234567890	Single Node	All Providers	April 20, 2022	Unassigned	Exchange License	...
012345678901234567891	Single Node	Azure	April 20, 2022	Unassigned	Exchange License	...
012345678901234567892	Single Node	AWS	January 1, 2022	Exchanged to Cloud Tiering on August 1, 2021		...

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。

Cloud Manager によって、選択したサービスに未割り当てのライセンスが変換されます。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、Cloud Manager はネットアップサポートサイトの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 *

Password*

.....

Product Line*

NetApp ONTAP Cloud BYOL for AWS

Product Serial #*

90120130000000000555

Not only is protecting your data required by law, but your privacy is also very important to us. Please read and agree to the NetApp [Data Privacy Policy](#) before you continue. For information related to NetApp's privacy policy please click here [Privacy Policy](#) or contact privacy@netapp.com.

☒ I have read NetApp's new [Global Data Privacy Policy](#) and understand how NetApp and its selected partners may use my personal data.

Submit

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、Cloud Manager は自動的にネットアップから新しいライセンスを取得し、Cloud Volumes ONTAP システムにインストールします。

Cloud Manager がセキュアなインターネット接続経由でライセンスファイルにアクセスできない場合は、ユーザがファイルを取得して、Cloud Manager に手動でアップロードできます。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。

Cloud Manager によって、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 736 TiB 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

Cloud Manager の右下にあるチャットアイコンからお問い合わせいただき、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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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

容量を追加するライセンスを延長した場合は、Cloud Manager でライセンスを更新する必要があります。

手順

1. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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、Cloud Manager 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. [* すべてのサービス]、[デジタルウォレット]、[Cloud Volumes ONTAP *] の順にクリックします。
2. 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。

Cloud Manager によって変換プロセスが開始されます。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。

ボリュームと LUN の管理

FlexVol ボリュームを作成します

初期 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、FlexVol Manager から NFS、CIFS、または iSCSI 用の新しい ボリュームを作成できます。

Cloud Manager 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 Cloud Manager で処理できるようにします。 [詳細はこちら。](#)
- 任意のデータアグリゲート上にボリュームを作成します。 [詳細はこちら。](#)
- テンプレートからボリュームを作成し、データベースやストリーミングサービスなど特定のアプリケーションのワークロード要件に合わせてボリュームを最適化します。 [詳細はこちら。](#)
- HA 構成の第 2 ノードにボリュームを作成する。 [詳細はこちら。](#)

始める前に

ボリュームのプロビジョニングに関する注意事項は次のとおりです。

- iSCSI ボリュームを作成すると、Cloud Manager 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"](#)。

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、必要なボリュームタイプを指定してから、Cloud Manager によってディスク割り当てが自動的に処理されるようにすることです。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. 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。
2. Cloud Manager 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

Volumes（ボリューム）タブで、* Add Volume * > * New volume *（ボリュームの追加*）をクリックします。

特定のアグリゲート

- メニューアイコンをクリックし、[* 詳細設定]、[詳細な割り当て*]の順にクリックします。
- アグリゲートのメニューをクリックします。
- [ボリュームの作成]をクリックします。

3. ウィザードの手順に従って、ボリュームを作成します。

- * 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
ボリュームサイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
タグ	ボリュームに追加するタグはに関連付けられます "Application Templates サービス" を使用すると、リソースの管理を整理して簡単に行うことができます。
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。

- * 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、サーバがセットアップされていない場合は、* Next * をクリックしたあとに、CIFS 接続のセットアップを求めるメッセージが Cloud Manager に表示されます。

["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、Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。

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。

参加する Active Directory ドメイン

CIFS サーバに参加させる 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"^]

DNS ドメイン

Cloud Volumes ONTAP Storage Virtual Machine（SVM）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。

NTP サーバ

Active Directory DNS を使用して NTP サーバを設定するには、「Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、API を使用してください。を参照してください ["Cloud Manager 自動化に関するドキュメント"](#) 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、Cloud Manager 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。

- c. * 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"](#)
 - ["GCP でシステムのサイジングを行う"](#)
- d. * 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。

- e. * 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。

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

テンプレートからボリュームを作成します

特定のアプリケーションのワークロード要件に最適化されたボリュームを導入できるように、組織で Cloud Volumes ONTAP ボリュームテンプレートを作成している場合は、このセクションの手順に従います。

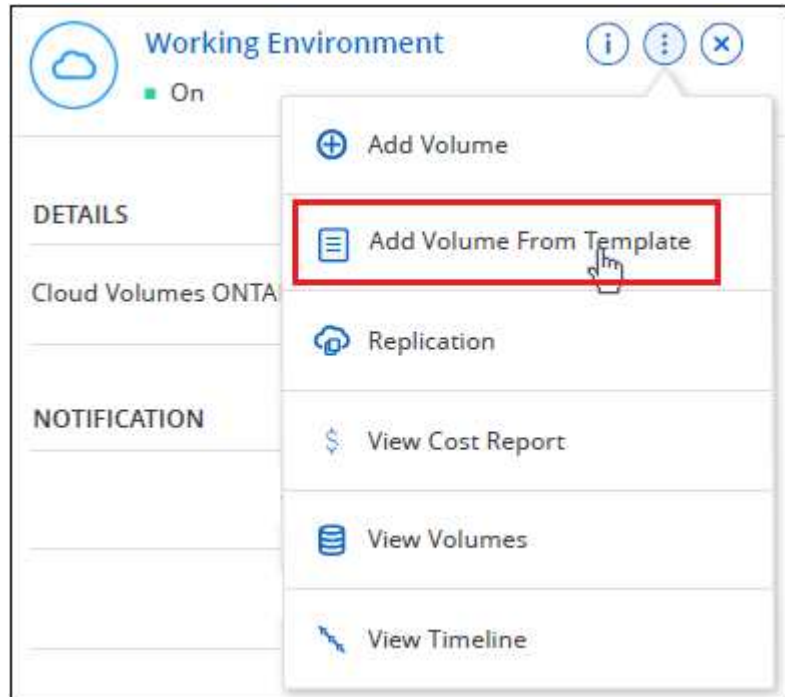
テンプレートを使用すると、ディスクタイプ、サイズ、プロトコル、スナップショットポリシー、クラウドプロバイダ、その他。パラメータがすでに事前定義されている場合は、次のボリュームパラメータに進みます。



テンプレートを使用する場合にのみ、NFS ボリュームまたは CIFS ボリュームを作成できます。

手順

1. キャンバスページで、ボリュームをプロビジョニングする Cloud Volumes ONTAP システムの名前をクリックします。
2. をクリックします > * テンプレートからボリュームを追加 *。



3. _ テンプレートの選択 _ ページで、ボリュームの作成に使用するテンプレートを選択し、* 次へ * をクリックします。



Define Parameters ページが表示されます。



[読み取り専用パラメータを表示する] チェックボックスをオンにすると、テンプレートによってロックされているすべてのフィールドを表示できます。これらのパラメータの値を表示するには、このチェックボックスをオンにします。デフォルトでは、これらの事前定義フィールドは非表示になっており、入力する必要のあるフィールドのみが表示されます。

4. `_Context_area` では、作業環境に、で開始した作業環境の名前が入力されます。ボリュームを作成する Storage VM を選択する必要があります。
5. テンプレートからハードコーディングされていないすべてのパラメータに値を追加します。を参照してください [ボリュームを作成します](#) Cloud Volumes ONTAP ボリュームを導入するために必要なすべてのパラメータの詳細については、を参照してください。
6. 定義する必要がある他のアクションがない場合（たとえば、Cloud Backup を構成する場合）は、* テンプレートを実行 * をクリックします。

他のアクションがある場合は、左ペインのアクションをクリックして、完了する必要のあるパラメータを表示します。



たとえば、クラウドバックアップを有効にする処理でバックアップポリシーを選択する必要がある場合は、ここで選択できます。

7. [テンプレートの実行] をクリックします。

Cloud Volumes ONTAP によってボリュームがプロビジョニングされ、進捗状況を確認するためのページが表示されます。

Creating your resources

This process can take a few minutes.
Keep this page open to monitor progress, or you can close this page
and check the [Timeline](#) later for details.

Actions status

Create Volume in Cloud Volumes ONTAP	Success
Enable Cloud Backup	Pending

また、テンプレートにセカンダリ操作が実装されている場合は、たとえばボリュームで Cloud Backup を有効にすると、その操作も実行されます。

HA 構成の第 2 ノードにボリュームを作成する

デフォルトでは、Cloud Manager は HA 構成の最初のノードにボリュームを作成します。両方のノードがクライアントにデータを提供するアクティブ / アクティブ構成が必要な場合は、2 番目のノードにアグリゲートとボリュームを作成する必要があります。

手順

1. 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。
2. メニューアイコンをクリックし、[* 詳細設定] > [高度な割り当て *] をクリックします。
3. Add Aggregate * をクリックして、アグリゲートを作成します。

4. Home Node には、HA ペアの 2 番目のノードを選択します。
5. Cloud Manager でアグリゲートが作成されたら、そのアグリゲートを選択して * ボリュームの作成 * をクリックします。
6. 新しいボリュームの詳細を入力し、* Create * をクリックします。

Cloud Manager によって、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


Cloud Manager では、ボリュームと CIFS サーバを管理できます。また、容量の問題を回避するためにボリュームを移動するように求められます。


ボリュームを管理します

ストレージニーズの変化に応じてボリュームを管理できます。ボリュームの表示、編集、クローン作成、リストア、削除を実行できます。

手順

1. 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。
2. ボリュームの管理：

タスク	アクション
ボリュームに関する情報を表示します	ボリュームを選択し、* 情報 * をクリックします。
ボリュームの編集（読み取り / 書き込みボリュームのみ）	<ol style="list-style-type: none"> a. ボリュームを選択し、* 編集 * をクリックします。 b. ボリュームの Snapshot ポリシー、NFS 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、* Update * をクリックします。 <div>  <p>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。</p> </div>

タスク	アクション
ボリュームのクローンを作成します	<p>a. ボリュームを選択し、 * Clone * をクリックします。</p> <p>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。</p> <p>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。</p> <p>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"。</p>
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	<p>a. ボリュームを選択し、 * Snapshot コピーからリストア * をクリックします。</p> <p>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。</p>
オンデマンドで Snapshot コピーを作成します	<p>a. ボリュームを選択し、 * Snapshot コピーの作成 * をクリックします。</p> <p>b. 必要に応じて名前を変更し、 * 作成 * をクリックします。</p>
nfs mount コマンドを取得します	<p>a. ボリュームを選択し、 * コマンドのマウント * をクリックします。</p> <p>b. [* コピー (Copy)] をクリックします</p>
iSCSI ボリュームのターゲット IQN を表示します	<p>a. ボリュームを選択し、 * Target IQN * をクリックします。</p> <p>b. [* コピー (Copy)] をクリックします</p> <p>c. "IQN を使用して、から LUN に接続します ホスト"。</p>
基になるディスクタイプを変更します	<p>a. ボリュームを選択し、 * ディスクタイプと階層化ポリシーの変更 * をクリックします。</p> <p>b. ディスクタイプを選択し、 * Change * をクリックします。</p> <div>  <p>Cloud Manager は、選択したディスクタイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。</p> </div>

タスク	アクション
階層化ポリシーを変更します	<p>a. ボリュームを選択し、* ディスクタイプと階層化ポリシーの変更 * をクリックします。</p> <p>b. [* ポリシーの編集 *] をクリックします。</p> <p>c. 別のポリシーを選択し、* 変更 * をクリックします。</p> <div>  <p>Cloud Manager は、選択したディスクタイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。</p> </div>
ボリュームを削除します	<p>a. ボリュームを選択し、* 削除 * をクリックします。</p> <p>b. 再度 * Delete * をクリックして確定します。</p>

ボリュームのサイズを変更する

デフォルトでは、スペースが不足したときにボリュームが最大サイズに自動的に拡張されます。デフォルト値は 1、000 で、ボリュームはサイズの 11 倍まで拡張できます。この値はコネクタの設定で設定できます。

ボリュームのサイズを変更する必要がある場合は、を使用して変更できます ["ONTAP システムマネージャ"](#)。ボリュームのサイズを変更する際は、システムの容量制限を考慮してください。にアクセスします ["Cloud Volumes ONTAP リリースノート"](#) 詳細：

CIFS サーバを変更

DNS サーバまたは Active Directory ドメインを変更した場合は、クライアントへのストレージの提供を継続できるように、Cloud Volumes ONTAP で CIFS サーバを変更する必要があります。

手順

1. 作業環境で、メニューアイコンをクリックし、* Advanced > CIFS setup * をクリックします。
2. CIFS サーバの設定を指定します。

タスク	アクション
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（SRV）が含まれている必要があります。
参加する Active Directory ドメイン	CIFS サーバを参加させる Active Directory（AD）ドメインの FQDN。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（OU）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

タスク	アクション
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバとして設定する場合は、このフィールドに「* OU=computers、OU=corp *」と入力します。
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine（SVM）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。

3. [保存（ Save ）] をクリックします。

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ペリエンスガイド"](#)。

Cloud Manager に「 Action Required 」メッセージが表示されたら、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の移動が必要であることを通知する「 Action Required 」メッセージが Cloud Manager に表示されることがありますが、問題の修正は手動で行う必要があります。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、Cloud Manager に「 Action Required 」メッセージが表示され、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. [問題を解決する方法を認識する。](#)
2. 分析に基づいて、容量の問題を回避するためにボリュームを移動します。
 - [ボリュームを別のシステムに移動します。](#)
 - [ボリュームを同じシステム上の別のアグリゲートに移動します。](#)

容量の問題を解決する方法を特定する

容量の問題を回避するためにボリュームの移動が必要で、Cloud Manager から推奨される処理が提示されな

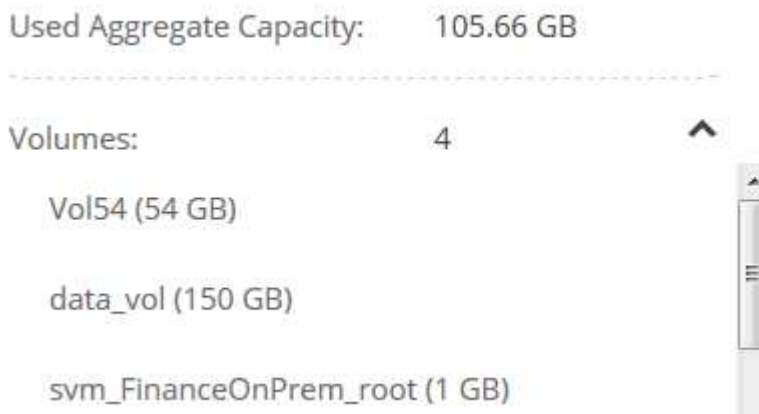
い場合、移動が必要なボリュームと、そのボリュームを同じシステムの別のアグリゲートまたは別のシステムのどちらに移動すべきかを特定する必要があります。

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、メニューアイコンをクリックし、* 詳細設定 > 高度な割り当て * をクリックします。
 - b. アグリゲートを選択し、* Info * をクリックします。
 - c. ボリュームのリストを展開します。



- d. 各ボリュームのサイズを確認し、アグリゲートから移動するボリュームを 1 つ以上選択します。

将来的に容量の問題が発生しないように、アグリゲート内の空きスペースに十分な大きさのボリュームを選択する必要があります。

3. システムがディスク制限に達していない場合は、ボリュームを同じシステム上の既存のアグリゲートまたは新しいアグリゲートに移動する必要があります。

詳細については、を参照してください ["ボリュームを別のアグリゲートに移動して、容量の問題を回避します"](#)。

4. システムがディスクの上限に達した場合は、次のいずれかを実行します。

- a. 未使用のボリュームを削除します。
- b. ボリュームを再配置して、アグリゲートの空きスペースを確保します。

詳細については、を参照してください ["ボリュームを別のアグリゲートに移動して、容量の問題を回避します"](#)。

- c. スペースがある別のシステムに 2 つ以上のボリュームを移動します。

詳細については、を参照してください ["容量の問題を回避するためにボリュームを別のシステムに移動する"](#)。

容量の問題を回避するためにボリュームを別のシステムに移動します

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。

このタスクの手順に従って、次のアクションが必要なメッセージを修正できます。

Moving a volume is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you because the system has reached the disk limit.

. 手順

- . 使用可能な容量を持つ Cloud Volumes ONTAP システムを特定するか、新しいシステムを導入します。
- . ソースの作業環境をターゲットの作業環境にドラッグアンドドロップして、ボリュームの 1 回限りのデータレプリケーションを実行します。

+

詳細については、を参照してください ["システム間でのデータのレプリケーション"](#)。

1. [Replication Status] ページに移動し、SnapMirror 関係を解除して、レプリケートされたボリュームをデータ保護ボリュームから読み取り / 書き込みボリュームに変換します。

詳細については、を参照してください ["データレプリケーションのスケジュールと関係の管理"](#)。

2. データアクセス用にボリュームを設定します。

データアクセス用のデスティネーションボリュームの設定については、を参照してください ["ONTAP 9 ボリュームディザスタリカバリエクスプレスガイド"](#)。

3. 元のボリュームを削除します。

詳細については、を参照してください ["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。

このタスクの手順に従って、次のアクションが必要なメッセージを修正できます。

Moving two or more volumes is necessary to avoid capacity issues; however, Cloud Manager cannot perform this action for you.

. 手順

- . 既存のアグリゲートに、移動する必要があるボリュームの使用可能な容量があるかどうかを確認します。

+

.. 作業環境で、メニューアイコンをクリックし、* 詳細設定 > 高度な割り当て * をクリックします。

.. 各アグリゲートを選択し、* Info * をクリックして、使用可能な容量（アグリゲート容量から使用済みアグリゲート容量を引いた容量）を確認します。

+

aggr1

Aggregate Capacity: 442.94 GB

Used Aggregate Capacity: 105.66 GB

1. 必要に応じて、既存のアグリゲートにディスクを追加します。
 - a. アグリゲートを選択し、* ディスクの追加 * をクリックします。
 - b. 追加するディスクの数を選択し、* 追加 * をクリックします。
2. 使用可能な容量を持つアグリゲートがない場合は、新しいアグリゲートを作成します。

詳細については、を参照してください ["アグリゲートの作成"](#)。

3. System Manager または CLI を使用して、ボリュームをアグリゲートに移動します。
4. ほとんどの場合、System Manager を使用してボリュームを移動できます。

手順については、を参照してください ["ONTAP 9 ボリューム移動エクスペリエンスガイド"](#)。

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。

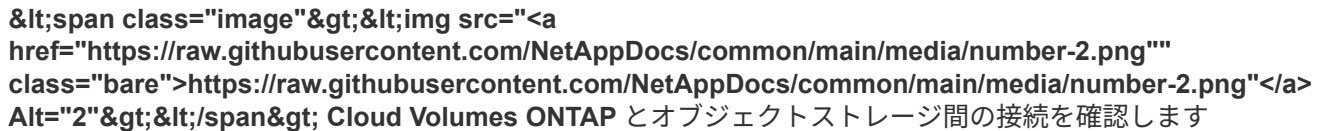
- ボリュームがクローンである。
 - ボリュームがクロンの親です。
 - ソースアグリゲートまたはデスティネーションアグリゲートには、スループットが最適化された HDD （st1）が 1 本含まれています。
 - Cloud Volumes ONTAP システムが AWS にあり、1 つのアグリゲートがオブジェクトに古い命名規則を使用します。両方のアグリゲートで同じ名前形式を使用する必要があります。
- 9.4 リリース以前のアグリゲートでデータの階層化が有効になっている場合は、古い命名規則が使用されます。
- 暗号化設定がソースアグリゲートとデスティネーションアグリゲートで一致しないか、キ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。

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 テクノロジー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。

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"](#)。

 Cloud Volumes ONTAP とオブジェクトストレージ間の接続を確認します

- AWS では、S3 への VPC エンドポイントが必要です。 [詳細はこちら](#)。
- Azure では、Cloud Manager に必要な権限が付与されていれば何も実行する必要はありません。 [詳細はこちら](#)。
- GCP の場合、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](#)。

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](#)。

ボリュームを作成、変更、またはレプリケートするときに、Cloud Manager から階層化ポリシーを選択するよう求められます。

- ["読み取り / 書き込みボリュームでのデータの階層化"](#)
- ["データ保護ボリューム上のデータの階層化"](#)

データ階層化に不要なもの

- データの階層化を有効にするために機能ライセンスをインストールする必要はありません。
- 大容量階層（S3 バケット、Azure BLOB コンテナ、GCP バケット）を作成する必要はありません。クラウドマネージャーがそれを実現します。
- 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。

Cloud Manager は、システム作成時にコールドデータ用のオブジェクトストアを作成し、[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

特定の構成と機能を使用する場合は、データ階層化を有効にできます。

- Cloud Volumes ONTAP では、次のバージョン以降でデータ階層化がサポートされます。

- AWS でバージョン 9.2 を実行します
- Azure のシングルノードシステムの場合はバージョン 9.4
- Azure バージョン 9.6 （ HA ペアを使用）
- GCP のバージョン 9.6
- AWS では、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 では、Premium SSD Managed Disks 、 Standard SSD Managed Disks 、 Standard HDD Managed Disks のいずれかです。
- GCP では、SSD 永続ディスク、分散型永続ディスク、または標準的な永続ディスクのいずれかを使用できます。
- データ階層化は暗号化テクノロジー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

必要な権限が Cloud Manager に割り当てられていれば、パフォーマンス階層と大容量階層の間に接続を設定する必要はありません。Cloud Manager ポリシーに以下の権限が設定されている場合、Cloud Manager は VNet サービスエンドポイントを有効にします。

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

権限は最新のに含まれています ["Cloud Manager ポリシー"](#)。

コールドデータを **Google Cloud Storage** に階層化するための要件 バケット

- 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」](#)"。
- 次の要件を満たすサービスアカウントが必要です。
 - 事前に定義された Storage Admin ロールが必要です。
 - Connector サービスアカウントは、この階層化サービスアカウントの _ サービスアカウント User_ である必要があります。

"[サービスアカウントの設定方法について説明します](#)"。

- 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

接続や権限に問題がなければ、Cloud Manager 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を作成します。システムを作成するまで上記の要件を満たしていない場合は、階層化を手動で有効にする必要があります。これにより、オブジェクトストアが作成されます。

手順

1. [すべての要件を満たしていることを確認します](#)。
2. キャンバスページで、Cloud Volumes ONTAP インスタンスの名前をダブルクリックします。
3. メニューアイコンをクリックし、* 容量階層化を有効にする * を選択します。



このオプションが表示されるのは、Cloud Manager システムの作成時にデータの階層化を有効にできなかった場合のみです。

4. Enable * をクリックします。これにより、この Cloud Volumes ONTAP システムで階層化データに使用するオブジェクトストアが Cloud Manager で作成されます。

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 *

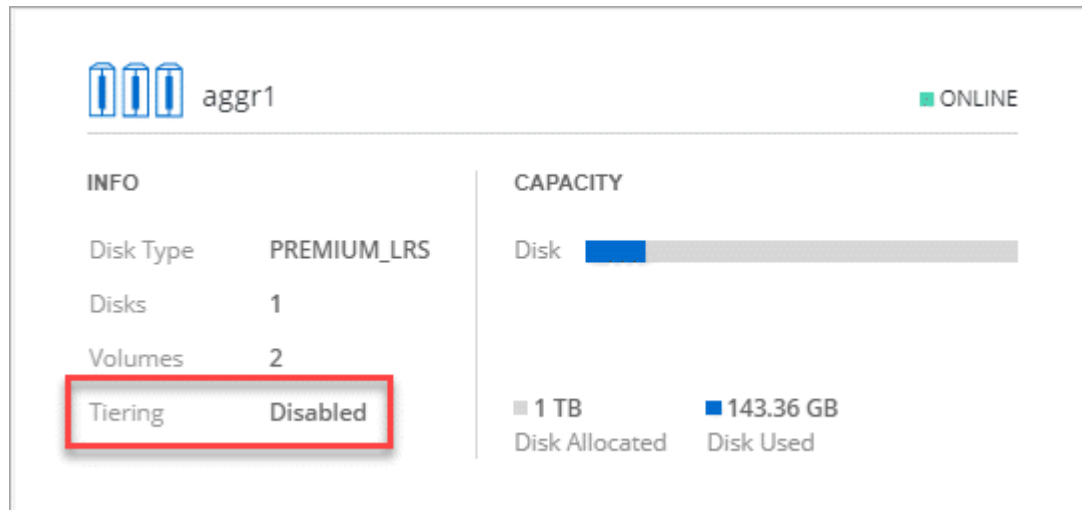
新しいボリュームでデータ階層化を有効にする場合、アグリゲートでデータ階層化を有効にする必要はありません。Cloud Manager では、階層化が有効になっている既存のアグリゲートにボリュームが作成されます。データ階層化が有効になっているアグリゲートがない場合は、ボリューム用の新しいアグリゲートが作成されます。

• * 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. Cloud Manager で作業環境を開きます。
2. メニューアイコンをクリックし、* 詳細設定 * をクリックして、* 詳細設定 * をクリックします。
3. 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. 作業環境で、新しいボリュームを作成するか、既存のボリュームの階層を変更します。

タスク	アクション
新しいボリュームを作成します	[新しいボリュームの追加] をクリックします。
既存のボリュームを変更します	ボリュームを選択し、* ディスクタイプと階層化ポリシーの変更 * をクリックします。

2. 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 *



S3 Tiering data to object storage

Volume Tiering Policy

- ☒ **All** - Immediately tiers all data (not including metadata) to object storage.
- ☐ **Auto** - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
- ☐ **Snapshot Only** - Tiers cold Snapshot copies to object storage
- ☐ **None** - Data tiering is disabled.

Working Environment S3 Storage classes: Standard

データ階層化対応のアグリゲートがまだ存在しない場合、Cloud Manager はボリュームの新しいアグリゲートを作成します。

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

- 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。
- 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 *



S3 Tiering

Enabled ☒ **Disabled** ☐

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

[What are storage tiers?](#)

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。その後、追加の容量が必要になったときに（アグリゲートのディスクの上限に達するまで）、Cloud Manager 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. Cloud Manager コンソールの右上にある * Settings * アイコンをクリックし、* Connector Settings * 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 のみを使用してサポートされます。

クーリング期間とは、ボリューム内のユーザーデータが「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、Cloud Manager 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。

- Cloud Manager の自動容量管理は、LUN には適用されません。Cloud Manager 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. 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。
2. ボリュームを選択し、* Target IQN * をクリックします。
3. [* Copy*] をクリックして IQN 名をコピーします。
4. 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"](#)

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（またはソース）ボリュームから NFS 読み取りデータをキャッシュするストレージボリュームです。その後キャッシュされたデータを読み取ることで、そのデータへのアクセスが高速になります。

FlexCache を使用すると、データアクセスを高速化したり、アクセス頻度の高いボリュームのトラフィック負荷を軽減したりできます。FlexCache ボリュームを使用すると、元のボリュームにアクセスせずに直接データを使用できるため、特にクライアントが同じデータに繰り返しアクセスする場合に、パフォーマンスの向上に役立ちます。FlexCache ボリュームは、読み取り処理が大量に発生するシステムワークロードに適しています。

現時点では、Cloud Manager で FlexCache ボリュームを管理することはできませんが、FlexCache CLI または ONTAP System Manager を使用して、ONTAP ボリュームを作成および管理できます。

- ["『FlexCache Volumes for Faster Data Access Power Guide』を参照してください"](#)
- ["System Manager での FlexCache ボリュームの作成"](#)

3.7.2 リリース以降、Cloud Manager はすべての新しい Cloud Volumes ONTAP システムに対して FlexCache ライセンスを生成します。ライセンスの使用量は 500GiB に制限されています。



Kubernetes 用の永続的ストレージとしての Cloud Volumes ONTAP の使用

Cloud Manager では、Kubernetes クラスタへの NetApp Trident の導入を自動化できるため、Cloud Volumes ONTAP をコンテナ用の永続的ストレージとして使用できます。



この機能は廃止予定で、今後のリリースで削除される予定です。高度なデータ管理のための作業環境として、管理対象 Kubernetes クラスタを Canvas に追加する機能に置き換えられました。"[詳細はこちら](#)。"

Trident は、ネットアップが管理する、完全にサポートされているオープンソースプロジェクトです。Trident は、Kubernetes と Persistent Volume フレームワークとネイティブに統合されており、ネットアップのストレージプラットフォームを任意に組み合わせて実行されるシステムからボリュームのプロビジョニングと管理をシームレスに行います。"[Trident の詳細をご確認ください](#)。"

クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

Kubernetes クラスタと Cloud Volumes ONTAP の接続、Kubernetes クラスタとコネクタの間の接続、1.14 以上の Kubernetes バージョン、クラスタ内の少なくとも 1 つのワーカーノードなど、環境が前提条件を満たしていることを確認します。 [すべてのリストを参照してください](#)。

Cloud Manager で、* K8s * をクリックしてクラウドプロバイダの管理サービスからクラスタを直接検出するか、または kubeconfig ファイルを指定してクラスタをインポートします。

Kubernetes クラスタを追加したら、* 作業環境への接続 * をクリックして、クラスタを 1 つ以上の Cloud Volumes ONTAP システムに接続します。

Kubernetes の標準のインターフェイスと構成要素を使用して、永続ボリュームを要求および管理できます。Cloud Manager では、NFS ストレージクラスと iSCSI ストレージクラスが作成されます。このクラスは、永続的ボリュームのプロビジョニング時に使用できます。

["Trident で最初のボリュームをプロビジョニングする方法をご確認ください Kubernetes"](#)。

前提条件の確認

開始する前に、Kubernetes クラスタとコネクタが特定の要件を満たしていることを確認してください。

Kubernetes クラスタの要件

- Kubernetes クラスタとコネクタの間、および Kubernetes クラスタと Cloud Volumes ONTAP の間には、ネットワーク接続が必要です。

Connector と Cloud Volumes ONTAP の両方で Kubernetes API エンドポイントへの接続が必要です。

- 管理対象クラスタの場合は、クラスタの VPC と、コネクタと Cloud Volumes ONTAP が存在する VPC の間にルートを設定します。
- 他のクラスタの場合は、プライマリノードまたはロードバランサの IP アドレス（kubeconfig ファイルに一覧表示）にコネクタおよび Cloud Volumes ONTAP から到達可能で、有効な TLS 証明書を提供する必要があります。
- Kubernetes クラスタは、上記のネットワーク接続を持つ任意の場所に配置できます。
- Kubernetes クラスタで少なくともバージョン 1.14 が実行されている必要があります。

サポートされる最大バージョンは Trident によって定義されています。 ["サポートされる Kubernetes の最大バージョンについては、こちらをクリックしてください"](#)。

- Kubernetes クラスタには、少なくとも 1 つのワーカーノードが必要です。
- Amazon Elastic Kubernetes Service（Amazon EKS）で実行されているクラスタの場合、権限のエラーを解決するために、各クラスタに IAM ロールを追加する必要があります。クラスタの追加後、Cloud Manager は、エラーを解決する eksctl コマンドでプロンプトを表示します。

["IAM 権限の境界について説明します"](#)。

- Azure Kubernetes Service（AKS）で実行されているクラスタには、これらのクラスタに _Azure Kubernetes Service RBAC Cluster Admin_role を割り当てる必要があります。これは、Cloud Manager が Trident をインストールし、クラスタにストレージクラスを設定するために必要です。

コネクタの要件

コネクタに対する次の権限が設定されていることを確認します。

EKS クラスタを検出および管理するために必要な権限

Connector は、Amazon Elastic Kubernetes Service（EKS）で実行されている Kubernetes クラスタを検出して管理するために Admin 権限を必要とします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "eks:*",
      "Resource": "*"
    }
  ]
}
```

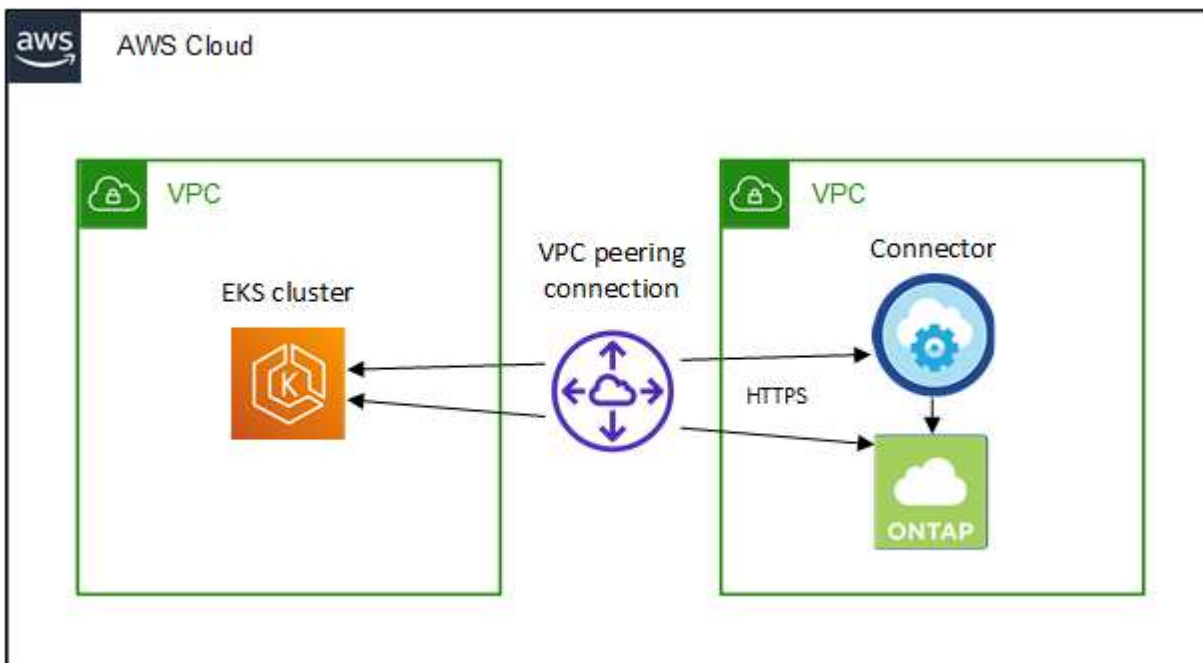
GKE クラスタの検出と管理に必要な権限

Connector は、Google Kubernetes Engine（GKE）で実行されている Kubernetes クラスタを検出して管理するために次の権限を必要とします。

```
container.*
```

セットアップ例

次の図は、Amazon Elastic Kubernetes Service（Amazon EKS）で実行されている Kubernetes クラスタとコネクタおよび Cloud Volumes ONTAP への接続の例を示しています。この例では、VPC ピアリングによって、EKS クラスタの VPC とコネクタおよび Cloud Volumes ONTAP の VPC 間の接続が確立されます。



Kubernetes クラスタを追加しています

クラウドプロバイダの管理対象の Kubernetes サービスで実行されているクラスタを検出するか、クラスタの kubeconfig ファイルをインポートして、Kubernetes クラスタを Cloud Manager に追加します。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. [Add Cluster*] をクリックします。
3. 次のいずれかのオプションを選択します。
 - [* クラスタの検出 *] をクリックして、Cloud Manager がコネクタに指定した権限に基づいてアクセスできる管理対象クラスタを検出します。

たとえば、Connector が Google Cloud で実行されている場合、Cloud Manager は、Connector のサービスアカウントの権限を使用して、Google Kubernetes Engine（GKE）で実行されているクラスタを検出します。
 - * クラスタのインポート * をクリックして、kubeconfig ファイルを使用してクラスタをインポートします。

ファイルをアップロードすると、Cloud Manager はクラスタへの接続を検証し、暗号化された kubeconfig ファイルのコピーを保存します。

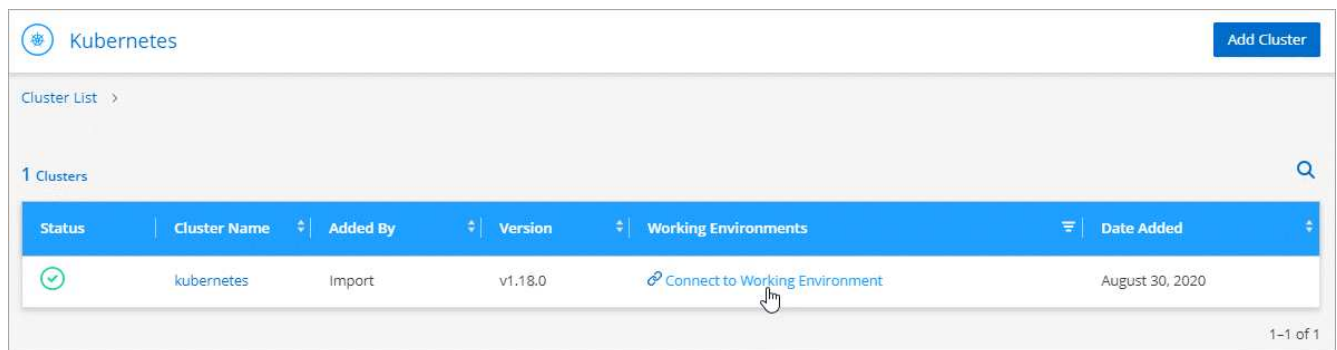
Cloud Manager によって Kubernetes クラスタが追加されます。これで、クラスタを Cloud Volumes ONTAP に接続できるようになります。

クラスタを Cloud Volumes ONTAP に接続しています

Kubernetes クラスタを Cloud Volumes ONTAP に接続し、Cloud Volumes ONTAP をコンテナ用の永続的ストレージとして使用できるようにします。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. 追加したクラスタの [Connect to Working Environment] をクリックします。



3. 作業環境を選択し、* 続行 * をクリックします。
4. Kubernetes クラスタのデフォルトのストレージクラスとして使用するネットアップストレージクラスを選択し、「* Continue *」をクリックします。

ユーザが永続ボリュームを作成すると、Kubernetes クラスタはこのストレージクラスをデフォルトでバックエンドストレージとして使用できます。

5. デフォルトの自動エクスポートポリシーを使用するか、カスタムの CIDR ブロックを追加するかを選択します。

Select Storage Class Type

Working Environment Information

Name	ishaiOntap4k8
Connected Clusters	None
Region	asia-east1
Zones	asia-east1-a
High Availability	Not Supported
Storage Classes	NFS Single Node Default ISCSI Single Node

Export Policy Information

If you plan to use NFS volumes you will need to set an export policy to allow connectivity between your clusters and your volumes.

☒ Use the default auto-export policies. (Suitable for most cases.)

OR

General Network CIDR ①

0.0.0.0/0

6. * 作業環境の追加 * をクリックします。

Cloud Manager によって作業環境がクラスタに接続されます。この処理には最大 15 分かかることがあります。

クラスタの管理

Cloud Manager では、Kubernetes クラスタを管理するために、デフォルトのストレージクラスの変更、Trident のアップグレードなどを行うことができます。

デフォルトのストレージクラスを変更する

クラスタがバックエンドストレージとして Cloud Volumes ONTAP を使用するように、Cloud Volumes ONTAP ストレージクラスをデフォルトのストレージクラスとして設定していることを確認します。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. Kubernetes クラスタの名前をクリックします。
3. ストレージクラス * の表で、デフォルトとして設定するストレージクラスの右端にあるアクションメニューをクリックします。

6 Storage Classes

Storage Class ID	Provisioner	Volumes	Labels
Gp2	aws	0	...
NFS Single Node	NetApp	0	...
NFS High Availability Default	NetApp	0	...
iSCSI High Availability	NetApp	0	...
iSCSI Single Node	NetApp	0	...

Set as Default

4. * デフォルトに設定 * をクリックします。

Trident のアップグレード

Trident の新しいバージョンが利用可能になったら、Cloud Manager から Trident をアップグレードできます。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. Kubernetes クラスタの名前をクリックします。
3. 新しいバージョンが利用可能な場合は、Trident バージョンの横にある * アップグレード * をクリックします。

Cluster List > Cluster Details >

kubernetes-baldwin

Connect to Working Environment Remove Cluster

Status Running	Cluster Version 1.15	Added by Discovery	Volumes 2	VPC vpc-0485a0b201c3a1f2d	Date Added September 3, 2020	Trident version v20.04 Upgrade	Provider aws
-------------------	-------------------------	-----------------------	--------------	------------------------------	---------------------------------	--	-----------------

kubeconfig ファイルを更新しています

クラスタを Cloud Manager に追加したときに kubeconfig ファイルをインポートすると、いつでも最新の kubeconfig ファイルを Cloud Manager にアップロードできます。この処理は、クレデンシャルを更新した場合、ユーザやロールを変更した場合、またはクラスタ、ユーザ、ネームスペース、認証に影響する変更を加えた場合に実行します。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. Kubernetes クラスタの名前をクリックします。
3. [* Update Kubeconfig *] をクリックします。
4. Web ブラウザからプロンプトが表示されたら、更新された kubeconfig ファイルを選択し、* Open * をクリックします。

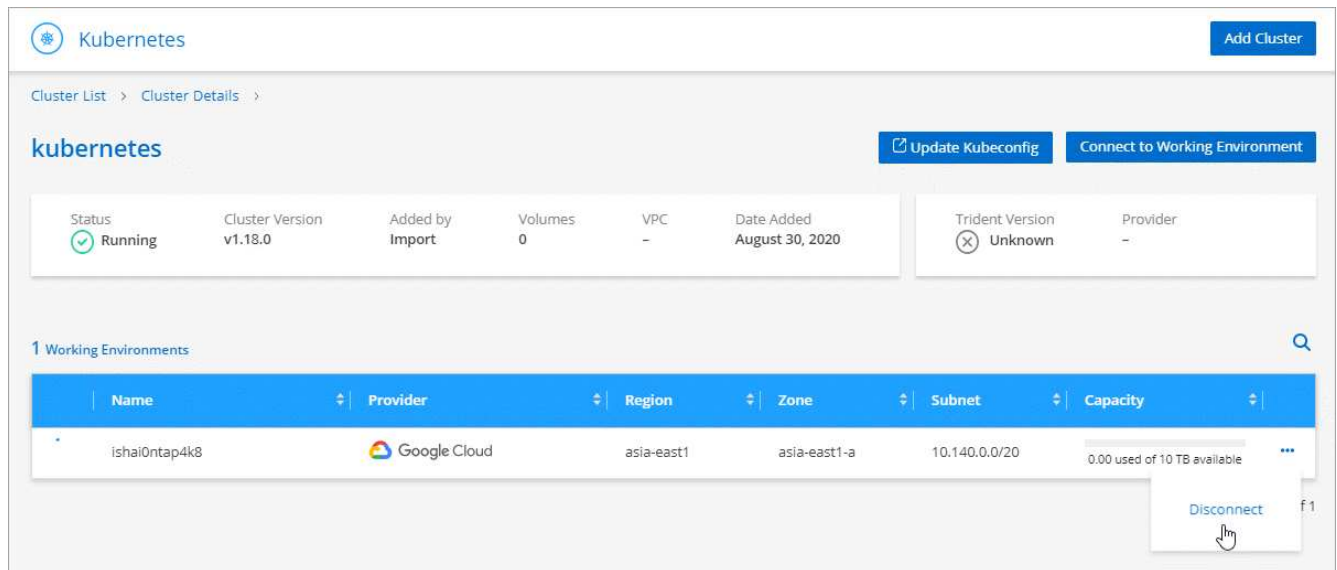
Cloud Manager は、最新の kubeconfig ファイルに基づいて Kubernetes クラスタに関する情報を更新します。

クラスタを切断しています

クラスタを Cloud Volumes ONTAP から切断すると、その Cloud Volumes ONTAP システムをコンテナ用の永続的ストレージとして使用できなくなります。既存の永続ボリュームは削除されません。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. Kubernetes クラスタの名前をクリックします。
3. [* 作業環境 * (Working Environments *)] テーブルで、切断する作業環境の右端にあるアクションメニューをクリックします。



アクションが表示される作業環境テーブルのスクリーンショット。"]

4. [切断 (Disconnect)] をクリックする。

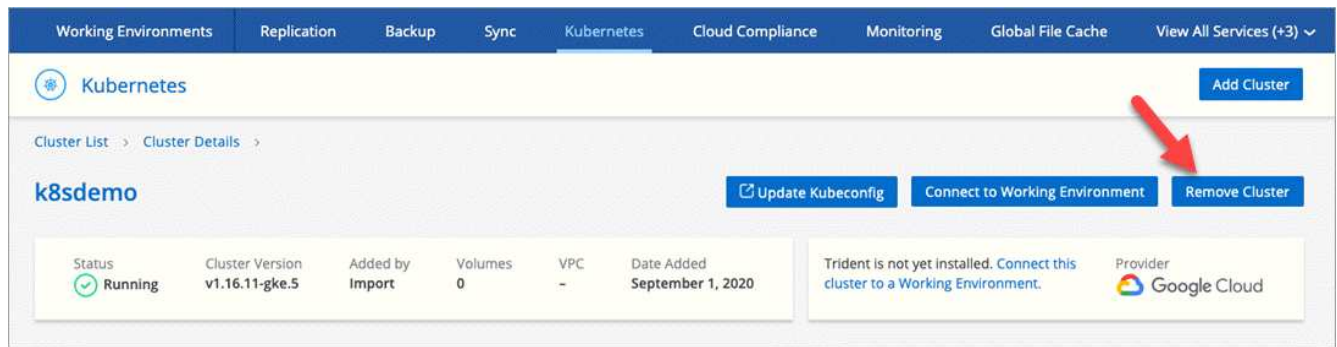
Cloud Manager によってクラスタが Cloud Volumes ONTAP システムから切断されます。

クラスタを削除しています

すべての作業環境をクラスタから切断したら、運用停止したクラスタを Cloud Manager から削除します。

手順

1. Cloud Manager の上部で、* K8s * をクリックします。
2. Kubernetes クラスタの名前をクリックします。
3. [クラスタの削除] をクリックします。



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、自分で作成することも、Cloud Manager でボリュームを作成するときにも作成することもできます。アグリゲートを手動で作成することのメリットは、基盤となるディスクサイズを選択して、必要な容量またはパフォーマンスに合わせてアグリゲートをサイジングできることです。



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

手順

1. 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。
2. メニューアイコンをクリックし、[* 詳細設定]、[詳細な割り当て *] の順にクリックします。
3. Add Aggregate * をクリックして、アグリゲートの詳細を指定します。

ディスクタイプとディスクサイズについては、を参照してください ["構成の計画"](#)。

4. [* Go *] をクリックし、[* 承認して購入 *] をクリックします。

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

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。

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. 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。
2. メニューアイコンをクリックし、[* 詳細設定] > [高度な割り当て *] をクリックします。
3. アグリゲートの管理：

タスク	アクション
アグリゲートに関する情報を表示します	アグリゲートを選択し、* Info * をクリックします。
特定のアグリゲートにボリュームを作成します	アグリゲートを選択し、* ボリュームの作成 * をクリックします。
アグリゲートにディスクを追加します	<div><div>a. アグリゲートを選択し、* AWS ディスクの追加 * または * Azure ディスクの追加 * をクリックします。</div><div>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。</div></div> <div> 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。</div>
アグリゲートを削除します	<div>a. ボリュームを含まないアグリゲートを選択し、* Delete * をクリックします。</div> <div>b. 再度 * Delete * をクリックして確定します。</div>

Storage VM 管理

Cloud Manager 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

特定の構成の Cloud Volumes ONTAP では、AWS および Azure 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。

複数の Storage VM を使用できます

Cloud Manager では、System Manager または CLI から追加で作成する Storage VM をサポートします。

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。

Details & Protection

Storage VM Name ⓘ
svm_name1 ✓

Volume Name Size (GiB) ⓘ
 Volume size

Snapshot Policy
default ✓

ⓘ Default Policy

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。

Destination Volume Name
volume_copy

Destination Storage VM Name
svm_name1 ✓

Destination Aggregate
Automatically select the best aggregate ▼

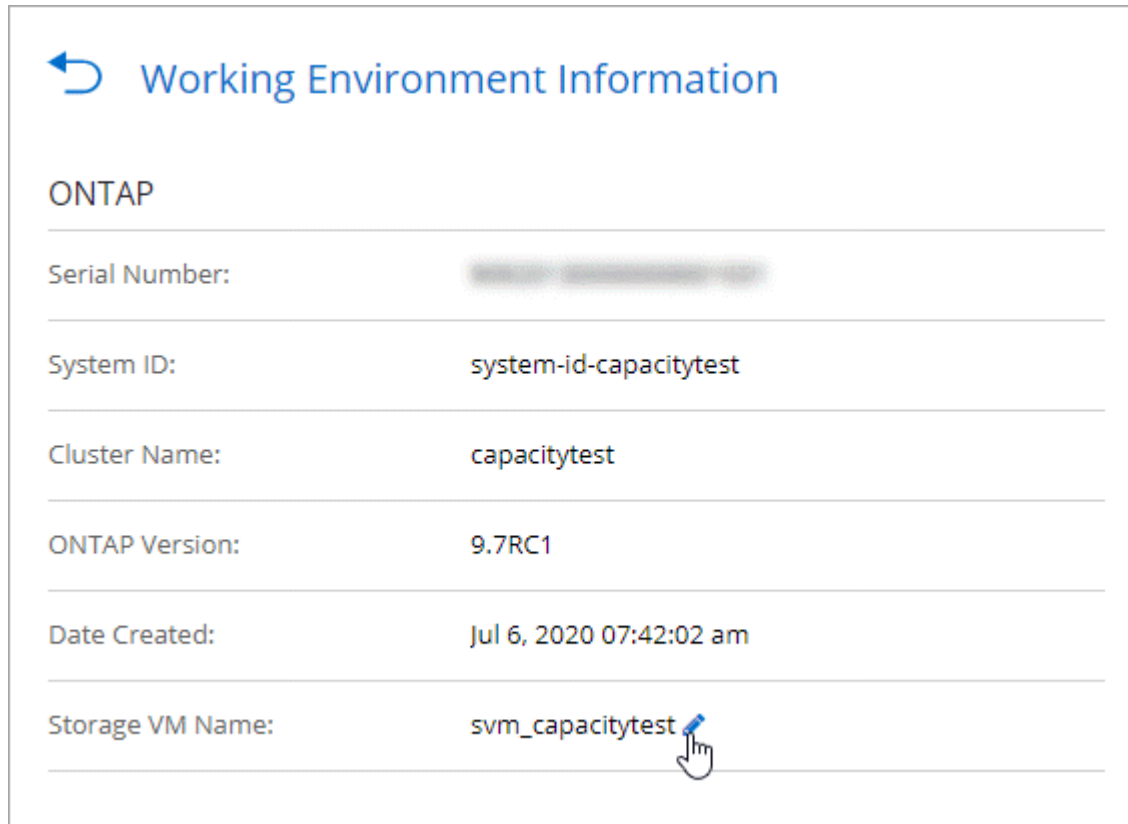
デフォルトの **Storage VM** の名前を変更します


Cloud Manager は、Cloud Volumes ONTAP 用に作成した単一の Storage VM に自動的に名前を付けます。厳密な命名基準がある場合は、Storage VM の名前を変更できます。たとえば、ONTAP クラスターの Storage VM の命名規則に沿った名前に変更できます。

Cloud Volumes ONTAP 用に追加の Storage VM を作成した場合、その Storage VM の名前を Cloud Manager から変更することはできません。Cloud Volumes ONTAP から直接実行する必要があります。そのためには、System Manager または CLI を使用します。

手順

1. 作業環境で、メニューアイコンをクリックし、* 情報 * をクリックします。
2. Storage VM 名の右にある編集アイコンをクリックします。



 Working Environment Information

ONTAP


Serial Number: XXXXXXXXXXXX

System ID: system-id-capacitytest

Cluster Name: capacitytest

ONTAP Version: 9.7RC1

Date Created: Jul 6, 2020 07:42:02 am

Storage VM Name: svm_capacitytest 

3. SVM 名の変更ダイアログボックスで名前を変更し、* 保存 * をクリックします。

ディザスタリカバリ用に **Storage VM** を管理する

Cloud Manager では、Storage VM ディザスタリカバリのセットアップやオーケストレーションはサポートされていません。System Manager または CLI を使用する必要があります。

- ["SVM ディザスタリカバリ設定エクスペスガイド"](#)
- ["『SVM ディザスタリカバリエクスペスガイド』"](#)

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

Cloud Volumes ONTAP の BYOL では、9.7 リリース以降、複数の Storage VM がアドオンライセンスで AWS でサポートされます。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。

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。

	Name	Insta...	Instance state	Instance type	Status check
<input type="checkbox"/>	danielleAws	i-070...	Running	m5.2xlarge	2/2 check
<input type="checkbox"/>	occmTiering0702	i-0a7...	Stopped	m5.2xlarge	-
<input checked="" type="checkbox"/>	cvoTiering1	i-02a...	Stopped	m5.2xlarge	-

Interface ID	Description
 eni-07c301...	Interface for Node & Cluster Management, Inter-Cluster Communication, and Data - e0a



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。

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

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 node1Mask -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。

Azure で Cloud Volumes ONTAP 用のデータ提供用 Storage VM を作成します

Storage VM は ONTAP 内で実行される仮想マシンであり、クライアントにストレージサービスとデータサービスを提供します。これは、`_SVM_` または `_SVM_` であることがわかります。Cloud Volumes ONTAP にはデフォルトで 1 つの Storage VM が設定されていますが、Azure で Cloud Volumes ONTAP を実行している場合は追加の Storage VM がサポートされます。

データを提供する Storage VM を追加で作成するには、Azure で IP アドレスを割り当ててから、ONTAP コマンドを実行して Storage VM とデータ LIF を作成する必要があります。

サポートされている Storage VM 数

Azure では、9.9.0 リリース以降、複数の Storage VM が Cloud Volumes ONTAP BYOL でサポートされており、アドオンライセンスが付与されています。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。

Azure で IP アドレスを割り当てます

構成に応じて、シングルノードシステム、iSCSI を使用する HA ペア、NFS / SMB を使用する HA ペアのいずれかの手順を実行します。

シングルノード

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。

9. 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。

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。

iSCSI を使用した HA ペア

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。

データ LIF からアクセスするための IP アドレスはノード 1 から、データ LIF からノード 2 のアクセス用の別の IP アドレス、および Storage VM （SVM）管理 LIF の別のオプションの IP アドレスで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. 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。

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。

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。

NFS / SMB を使用した HA ペア

NFS データおよび 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。

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 構成をノード 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 構成（HA ペアのみ）と、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 を作成します。
 - 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て、* Dynamic * を選択したままにします。

Microsoft Azure

Search resources, services, and docs (G+)

Home > Load balancers > azureha1011s3-rg-lb >

Add frontend IP address

azureha1011s3-rg-lb

Name * ip-for-svm2 ✓

Virtual network Default-Networking-vnet

Subnet default (172.19.2.0/24) ▾

Assignment ☒ Dynamic ☐ Static

- 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。

Home > Load balancers > azureha1011s3-rg-lb >

Add health probe ...

azureha1011s3-rg-lb

Name *	svm2-health-probe1 ✓
Protocol *	TCP ▼
Port * ⓘ	63005 ✓
Interval * ⓘ	5 seconds
Unhealthy threshold * ⓘ	2 consecutive failures
Used by ⓘ	Not used

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。

Add load balancing rule

chandanaTcpRst3-rg-lb

i A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name *

jimmy_new_rule ✓

IP Version *

☒ IPv4 ☐ IPv6

Frontend IP address * ⓘ

10.1.0.156 (dataAFIP) ▼

☒ HA Ports ⓘ

Backend pool ⓘ

backendPool (2 virtual machines) ▼

Health probe ⓘ

dataProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

☐ Disabled ☒ Enabled

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。

Storage VM と LIF を作成

以下の手順では、シングルノードシステムまたは HA ペアに新しい Storage VM を作成します。ノード 1 からのデータ LIF へのアクセスには、ノード 2（HA ペアのみ）からのデータ LIF へのアクセスに使用する別の IP アドレス、および Storage VM（SVM）の管理 LIF のオプションの IP アドレスが 1 つ必要です。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。

次のコマンドは、Storage VM のデータアクセスプロトコルである NAS または iSCSI に一致するものを使用してください。

手順

1. Storage VM と Storage VM へのルートを作成してください。

```
vserver create -vserver <svm-name> -subtype default -rootvolume <root-volume-name> -rootvolume-security-style unix
```

```
network route create -destination 0.0.0.0/0 -vserver <svm-name> -gateway  
<ip-of-gateway-server>
```

2. データ LIF を作成します。

- a. 次のコマンドを使用して、ノード 1 に NAS LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs--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>
```

シングルノードシステムの場合は、`-failover-policy` パラメータの値を *disabled* に変更する必要があります。

- 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（HA ペアの場合のみ）。

```
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>
```

- c. 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> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

- d. 次のコマンドを使用して、ノード 2 に iSCSI LIF を作成します（HA ペアの場合のみ）。

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -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 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>
```

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、Cloud Manager は HA ペアのロードバランサの設定を 12 時間おきにスキャンします。新しい SVM がある場合、Cloud Manager はより短い計画外フェイルオーバーを実現する設定を有効にします。

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。NVE を使用する場合、Azure Key Vault (AKV) または Google Cloud Key Management Service を使用して ONTAP 暗号化キーを保護することもできます。

外部キー管理ツールを設定すると、新しいアグリゲートで NAE がデフォルトで有効になります。NAE アグリゲートに含まれない新しいボリュームでは、NVE がデフォルトで有効になります（たとえば、外部キー管理ツールを設定する前に作成された既存のアグリゲートがある場合）。

Cloud Volumes ONTAP はオンボードキー管理をサポートしていません。

Cloud Volumes ONTAP システムがネットアップサポートに登録されている必要があります。ネットアップサポートに登録されている各 Cloud Volumes ONTAP システムには、NetApp Volume Encryption ライセンスが自動的にインストールされます。

- ["Cloud Manager へのネットアップサポートサイトのアカウントの追加"](#)
- ["従量課金制システムの登録"](#)



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

手順

1. でサポートされているキー管理ツールのリストを確認します ["NetApp Interoperability Matrix Tool で確認できます"](#)。



Key Managers * ソリューションを検索します。

2. ["Cloud Volumes ONTAP CLI に接続します"](#)。
3. 外部キー管理を設定

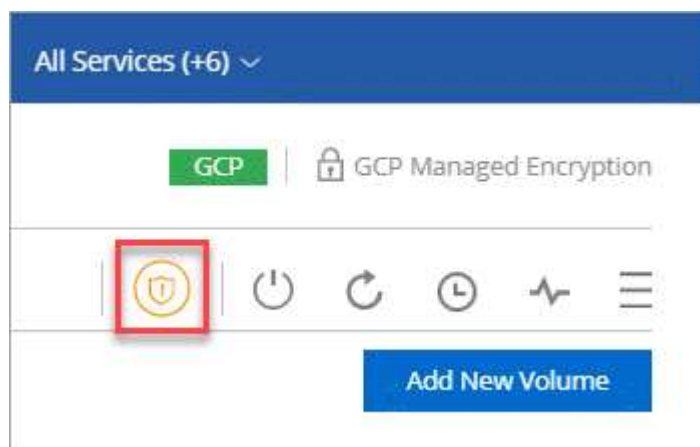
["手順については、ONTAP のドキュメントを参照してください"](#)。

ランサムウェアからの保護を強化

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

手順

1. 作業環境で、「* ランサムウェア *」アイコンをクリックします。



2. ネットアップのランサムウェア向けソリューションを導入する：
 - a. Snapshot ポリシーが有効になっていないボリュームがある場合は、* Snapshot ポリシーのアクティブ化 * をクリックします。

NetApp Snapshot テクノロジは、ランサムウェアの修復に業界最高のソリューションを提供します。リカバリを成功させるには、感染していないバックアップからリストアすることが重要です。Snapshot コピーは読み取り専用であり、ランサムウェアによる破損を防止します。単一のファイルコピーまたは完全なディザスタリカバリソリューションのイメージを作成する際の単位を提供することもできます。

- b. FPolicy のアクティブ化 * をクリックして ONTAP の FPolicy ソリューションを有効にします。これに

より、ファイルの拡張子に基づいてファイル操作をブロックできます。

この予防ソリューションは、ランサムウェア攻撃からの保護を強化する一般的なランサムウェアファイルタイプをブロックします。

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 Manager では、Cloud Volumes ONTAP で FPolicy をアクティブ化するときこのスコープを作成します。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。

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

View Denied File Names

Activate FPolicy

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 Cloud Manager からアップグレードすると、最新の新機能と機能拡張を利用できます。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。

Cloud Manager からのみアップグレード

Cloud Volumes ONTAP のアップグレードが Cloud Manager から完了している必要があります。System Manager または CLI を使用して Cloud Volumes ONTAP をアップグレードしないでください。これを行うと、システムの安定性に影響を与える可能性

アップグレード方法

Cloud Volumes ONTAP をアップグレードする方法は 2 種類あります。

- 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、その URL を Cloud Manager に提供する

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
9.10.0	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、Cloud Manager は、サポートされるアップグレードパスに準拠するリリースへのアップグレードを求めます。
- 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。

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にも、新しいバージョンが利用可能になったときに Cloud Manager に表示されるソフトウェア更新通知が送信されます。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

AWS または Google Cloud の HA システムの場合、Cloud Volumes ONTAP のアップグレードプロセス中に、必要に応じてメディエーターインスタンスも更新されます。

アップグレードを準備

アップグレードを実行する前に、システムの準備ができていることを確認し、必要な設定の変更を行ってください。

- [\[Plan for downtime\]](#)
- [\[Verify that automatic giveback is still enabled\]](#)
- [\[Suspend SnapMirror transfers\]](#)
- [\[Verify that aggregates are online\]](#)

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。

HA ペアのアップグレードは無停止で、I/O が中断されません。無停止アップグレードでは、各ノードが連携してアップグレードされ、クライアントへの I/O の提供が継続されます。

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。



Cloud Backup は SnapMirror を使用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。

ここでは、System Manager for Version 9.3 以降の使用方法について説明します。

手順

1. "System Manager にログインします。" デスティネーションシステムから作成します。
2. [* 保護] > [関係 *] の順にクリックします。
3. 関係を選択し、* Operations > Quiesce * をクリックします。

アグリゲートがオンライン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。

ここでは、System Manager for Version 9.3 以降の使用方法について説明します。

手順

1. 作業環境で、メニューアイコンをクリックし、* 詳細設定 > 高度な割り当て * をクリックします。
2. アグリゲートを選択し、* Info * をクリックして、状態がオンラインであることを確認します。

aggr1		
Aggregate Capacity:	88.57 GB	

Used Aggregate Capacity:	1.07 GB	

Volumes:	2	▼

AWS Disks:	1	▼

State:	online	

3. アグリゲートがオフラインの場合は、System Manager を使用してアグリゲートをオンラインにします。
 - a. "System Manager にログインします。"。
 - b. ストレージ > アグリゲートとディスク > アグリゲート * をクリックします。
 - c. アグリゲートを選択し、* その他の操作 > ステータス > オンライン * をクリックします。

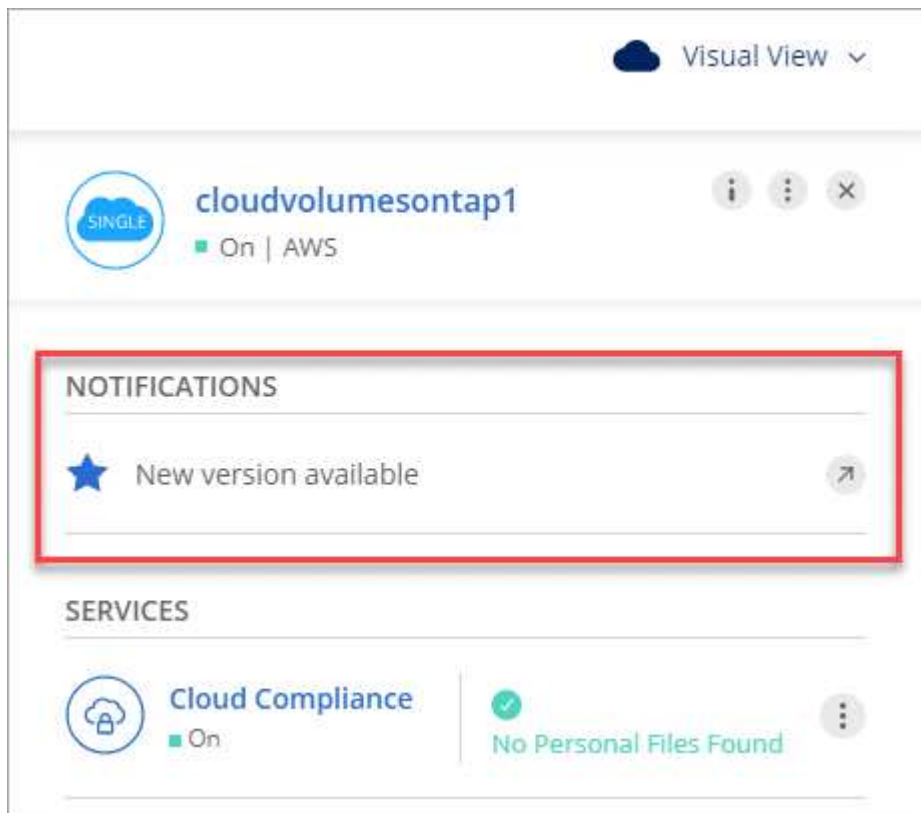
Cloud Volumes ONTAP をアップグレードします

新しいバージョンがアップグレード可能になると、Cloud Manager 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 [\[Upgrade from Cloud Manager notifications\]](#)。

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、Cloud Manager が S3 バケットにアクセスしてソフトウェアをアップグレードできない場合、またはパッチを適用して提供された場合に役立ちます。詳細については、を参照してください [\[Upgrade from an image available at a URL\]](#)。

Cloud Manager の通知からアップグレードします

Cloud Manager は、Cloud Volumes ONTAP の新しいバージョンが利用可能になると、Cloud Volumes ONTAP の作業環境に次の通知を表示します。



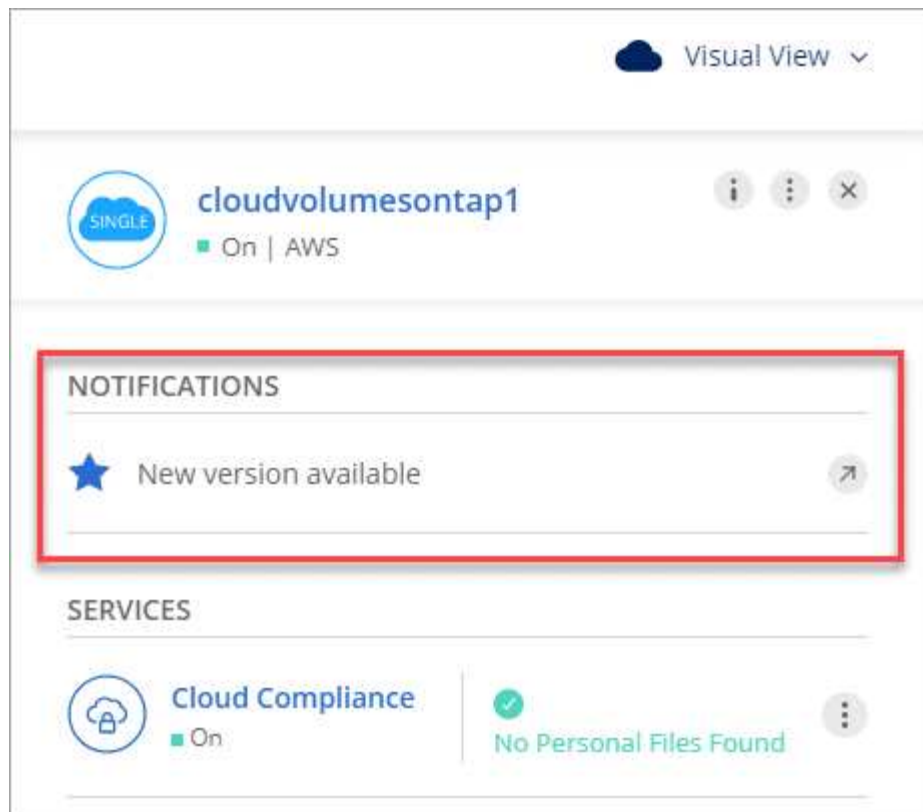
この通知からアップグレードプロセスを開始できます。アップグレードプロセスを自動化するには、S3 バケットからソフトウェアイメージを取得し、イメージをインストールしてから、システムを再起動します。

ボリュームやアグリゲートの作成などの Cloud Manager の処理が Cloud Volumes ONTAP システムで実行されていないことを確認します。

手順

1. 「* キャンバス *」をクリックします。
2. 作業環境を選択します。

新しいバージョンが使用可能になると、右側のペインに通知が表示されます。



3. 新しいバージョンが利用可能な場合は、* アップグレード * をクリックします。
4. [リリース情報] ページで、リンクをクリックして、指定したバージョンのリリースノートを読み、[* 読み ... *] チェックボックスをオンにします。
5. エンドユーザライセンス契約（EULA）ページで EULA を読んでから、「* I read and approve the EULA *」を選択します。
6. [レビューと承認] ページで、重要なメモを読み、[* I understand ... *] を選択して、[* Go *] をクリックします。

Cloud Manager がソフトウェアのアップグレードを開始します。ソフトウェアの更新が完了したら、作業環境に対してアクションを実行できます。

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、Cloud Manager からのソフトウェアのアップグレードを開始できます。Cloud Manager が S3 バケットにアクセスしてソフトウェアをアップグレードできない場合に、この方法を使用できます。

ボリュームやアグリゲートの作成などの Cloud Manager の処理が Cloud Volumes ONTAP システムで実行されていないことを確認します。

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。

たとえば、ソフトウェアイメージをコネクタ上の次のパスにコピーできます。

```
/opt/application/NetApp/cloudmanager/docx_occm/data/ontap/images/
```

5. Cloud Manager の作業環境で、メニューアイコンをクリックし、* Advanced > Update Cloud Volumes ONTAP * をクリックします。
6. アップデートソフトウェアのページで、URL を入力し、* イメージの変更 * 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>;
```

7. [* Proceed](続行) をクリックして確定します

Cloud Manager がソフトウェアの更新を開始します。ソフトウェアの更新が完了したら、作業環境に対してアクションを実行できます。

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、Cloud Manager 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にも、新しいバージョンが利用可能になったときに Cloud Manager に表示されるソフトウェア更新通知が送信されます。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. Cloud Manager にネットアップサポートサイトのアカウントをまだ追加していない場合は、「* Account Settings *」に移動して追加します。

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

2. カンバスページで、登録するシステムの名前をダブルクリックします。
3. メニューアイコンをクリックし、* Support registration registration *（サポート登録*）をクリックします。



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

Cloud Manager によってシステムがネットアップに登録されます。

Cloud Volumes ONTAP の状態の管理

Cloud Manager から Cloud Volumes ONTAP を停止して起動し、クラウドコンピューティングコストを管理できます。

Cloud Volumes ONTAP の自動シャットダウンのスケジュール設定

特定の時間間隔で Cloud Volumes ONTAP をシャットダウンして、コンピューティングコストを削減できます。これを手動で行う代わりに、Cloud Manager を設定して、システムを自動的にシャットダウンし、特定の時間に再起動することができます。

このタスクについて

- Cloud Volumes ONTAP システムの自動シャットダウンをスケジュールする際、アクティブなデータ転送が実行中の場合のシャットダウンは延期されます。

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

- このタスクでは、HA ペアの両方のノードの自動シャットダウンをスケジュールリングします。
- 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

- 作業環境で、時計アイコンをクリックします。



- シャットダウンスケジュールを指定します。

- 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。
- システムをオフにするタイミングと、オフにする期間を指定します。

▪ 例 *

次の図は、毎週土曜日の午前 0 時にシステムをシャットダウンするように Cloud Manager に指示するスケジュールを示しています48 時間。Cloud Manager は、毎週月曜日の午前 0 時にシステムを再起動します

☐ Turn off every weekday
Mon, Tue, Wed, Thu, Fri

turn off at 08 : 00 PM for 12 Hours (1-24)

☒ Turn off every weekend
Sat

turn off at 12 : 00 AM for 48 Hours (1-48)

- [保存 (Save)] をクリックします。

Cloud Manager はスケジュールを保存します。時計アイコンが変化して、スケジュールが設定されたことを

示します。



Cloud Volumes ONTAP を停止しています

Cloud Volumes ONTAP を停止すると、計算コストの発生を抑えることができ、ルートディスクとブートディスクの Snapshot が作成されます。これはトラブルシューティングに役立ちます。



コストを削減するため、Cloud Manager はルートディスクおよびブートディスクの古い Snapshot を定期的に削除します。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。

HA ペアを停止すると、Cloud Manager は両方のノードをシャットダウンします。

手順

1. 作業環境で、* 電源オフ * アイコンをクリックします。



2. Snapshot を作成するオプションを有効にしておくと、システムのリカバリが可能になります。
3. [オフにする *] をクリックします。

システムの停止には、最大数分かかる場合があります。システムは、後で [作業環境] ページから再起動できます。

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 "[Cloud Manager API の略](#)" 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](#)".

たとえば、AWS のシングルノードシステム用の API は次のようになります。

POST /vsa/working-environments/{workingEnvironmentId}/ntp

Setup NTP server.
Operation may only be performed on working environments whose status is: ON, DEGRADED.

Parameters

Parameter	Value	Description	Parameter Type	Data Type
workingEnvironmentId	<input type="text"/>	Public Id of working environment	path	string
body	<div>(required)</div> <div></div>	NTP Configuration request	body	Model Model Schema NTPConfigurationRequest { ntpServer (string): NTPS server }

Parameter content type: application/json ▼

Try it out!

システムの書き込み速度を変更する

Cloud Manager では、Cloud Volumes ONTAP に対して通常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でサポートされています。特定のインスタンスまたは VM タイプを使用する場合は、AWS と Azure の HA ペアでもサポートされます。GCP の HA ペアでは、高速の書き込み速度はサポートされていません。["詳細については、Cloud Volumes ONTAP のリリースノートを参照してください"](#)。

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. 作業環境で、メニューアイコンをクリックし、* 詳細設定 > 書き込み速度 * をクリックします。
2. 「* Normal *」または「* High *」を選択します。

「高」を選択した場合は、「I understand ...」文を読んで、チェックボックスをオンにして確認する必要があります。

3. [保存] をクリックし、確認メッセージを確認して、[続行] をクリックします。

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、Cloud Manager からこのアカウントのパスワードを変更できます。



System Manager または CLI を使用して admin アカウントのパスワードを変更しないでください。パスワードは Cloud Manager に反映されません。その結果、Cloud Manager はインスタンスを適切に監視できません。

手順

1. 作業環境で、メニューアイコンをクリックし、* 詳細設定 > パスワードの設定 * をクリックします。
2. 新しいパスワードを 2 回入力し、[保存] をクリックします。

新しいパスワードは、最後に使用した 6 つのパスワードのうちの 1 つと異なるものにする必要があります。

システムを追加、削除、または削除します

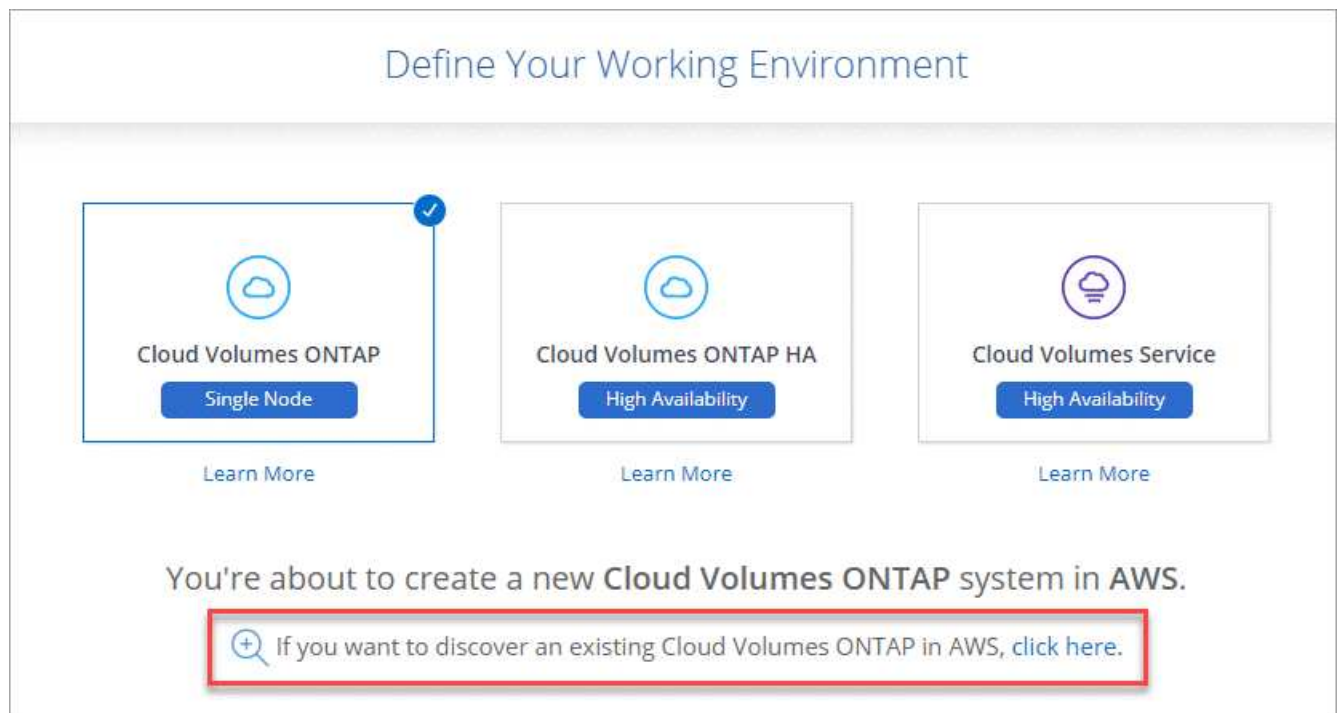
Cloud Manager に既存の Cloud Volumes ONTAP システムを追加

既存の Cloud Volumes ONTAP システムを検出して Cloud Manager に追加できます。この処理は、新しい Cloud Manager システムを導入した場合に実行できます。

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. キャンバスページで、* 作業環境の追加 * をクリックします。
2. システムが配置されているクラウドプロバイダを選択します。
3. Cloud Volumes ONTAP システムのタイプを選択します。
4. 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。



5. [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。

6. [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。

Cloud Manager によって Cloud Volumes ONTAP インスタンスがワークスペースに追加されます。

Cloud Volumes ONTAP 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。

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

Cloud Manager から作業環境を削除すると、次のことが可能になります。

- 作業環境を別のワークスペースで再検出します
- 別の Cloud Manager システムから再検出します
- 初期検出中に問題が発生した場合は、再検出します

手順

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



2. [ツール] ページで、[* 起動 *] をクリックします。
3. 削除する Cloud Volumes ONTAP の作業環境を選択します。
4. [レビューと承認] ページで、[* 移動] をクリックします。

Cloud Manager 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

Cloud Volumes ONTAP システムは、クラウドプロバイダのコンソールからではなく、必ず Cloud Manager 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 Cloud Manager から削除する必要があります。

作業環境を削除すると、Cloud Volumes ONTAP インスタンスが終了し、ディスクと Snapshot が削除されます。

作業環境を削除しても、Cloud Backup のバックアップや Cloud Data Sense のインスタンスや監視など、他のサービスによって管理されているリソースは削除されません。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。



Cloud Manager がクラウドプロバイダに Cloud Volumes ONTAP を導入すると、インスタンスでの終了保護が有効になります。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 Cloud Backup を有効にした場合は、バックアップしたデータが引き続き必要かどうかを確認してから **"必要に応じて、バックアップを削除します"**。

クラウドバックアップは、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、Cloud Backup はバックアップを自動的に削除しません。また、システムを削除した後でバックアップを削除するための UI で現在サポートされていません。

2. この作業環境で Cloud Data Sense または Monitoring を有効にし、他の作業環境でこれらのサービスを使用していない場合は、それらのサービスのインスタンスを削除する必要があります。
 - **"Cloud Data Sense インスタンスの詳細については、こちらをご覧ください"**。
 - **"Monitoring Acquisition Unit の詳細については、こちらを参照してください"**。
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. メニューアイコンをクリックし、*** 削除 *** をクリックします。



- c. 作業環境の名前を入力し、*** 削除 *** をクリックします。

作業環境を削除するには、最大 5 分かかります。

AWS での管理

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、Cloud Manager 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. 作業環境でメニューアイコンをクリックし、* インスタンスの変更 * を選択します。
2. ノードベースの PAYGO ライセンスを使用する場合は、必要に応じて別のライセンスを選択できます。
3. インスタンスタイプを選択し、チェックボックスを選択して、変更の影響を理解したことを確認し、* OK * をクリックします。

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. 作業環境で、メニューアイコンをクリックし、* 情報 * をクリックします。
2. * ルートテーブル * をクリックします。
3. 選択したルーティングテーブルのリストを変更し、* 保存 * をクリックします。

Cloud Manager は AWS 要求を送信してルートテーブルを変更します。

AWS のリソースコストを監視する

Cloud Manager では、AWS での Cloud Volumes ONTAP の実行に関連するリソースコストを確認できます。また、ネットアップの機能を使用してストレージコストを削減し、どれだけのコストを節約したかを確認することもできます。

ページを更新すると、Cloud Manager によってコストが更新されます。最終的なコストの詳細については、AWS を参照してください。

ステップ

1. Cloud Manager から AWS からコスト情報を取得できることを確認します。
 - a. Cloud Manager に権限を提供する IAM ポリシーに次の操作が含まれていることを確認します。

```
"ce:GetReservationUtilization",  
"ce:GetDimensionValues",  
"ce:GetCostAndUsage",  
"ce:GetTags"
```

これらのアクションは最新のに含まれています **"Cloud Manager ポリシー"**。これらの権限は、NetApp Cloud Central から自動的に導入された新しいシステムに含まれます。

- b. **"* WorkingEnvironmentId* タグをアクティブにします"**。

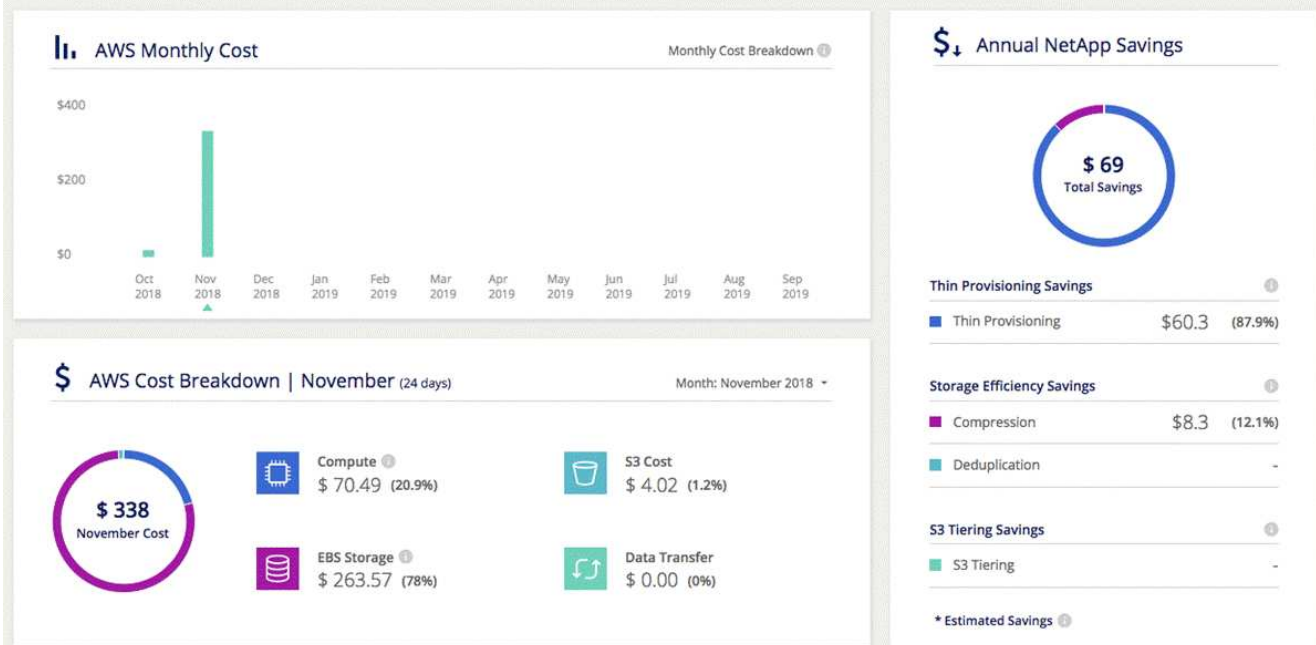
AWS のコストを追跡するために、Cloud Manager はコスト割り当てタグを Cloud Volumes ONTAP インスタンスに割り当てます。最初の作業環境を作成したら、* WorkingEnvironmentId * タグをアクティブ化します。ユーザ定義のタグは、請求とコスト管理のコンソールでアクティブ化するまでは AWS 請求レポートに表示されません。

2. キャンバスページで Cloud Volumes ONTAP 作業環境を選択し、コスト * をクリックします。

ボリュームでコスト削減機能を有効にしている場合、過去数カ月のコストと、ネットアップによる年間削減量が表示されます。

次の図は、コストページの例を示しています。

Cloud Manager obtains AWS resource costs by using the AWS Cost Explorer service



Azure での管理

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、Cloud Manager 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。

1. 作業環境で、メニューアイコンをクリックし、* VM の変更 * を選択します。
2. ノードベースの PAYGO ライセンスを使用する場合は、必要に応じて別のライセンスを選択できます。
3. VM 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確認し、* OK * をクリックします。

Cloud Volumes ONTAP が新しい設定でリブートします。

Azure での Cloud Volumes ONTAP HA の CIFS ロックの無効化

アカウント管理者は、Cloud Manager で設定を有効にして、Azure メンテナンスイベント時の 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。

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。

Cloud Manager の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. Cloud Manager コンソールの右上にある設定アイコンをクリックし、* コネクタ設定 * 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。

Cloud Volumes ONTAP で Azure プライベートリンクを使用する

デフォルトでは、Cloud Manager は Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間の Azure Private Link 接続を有効にします。プライベートリンクは Azure のエンドポイント間の接続を保護し、パフォーマンスを向上させます。"[詳細はこちら](#)"。

ほとんどの場合、実行する必要はありません。Cloud Manager は Azure Private Link を管理します。ただし、Azure Private DNS 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。必要に応じて、プライベートリンク接続を無効にすることもできます。

Azure のコネクタの場所

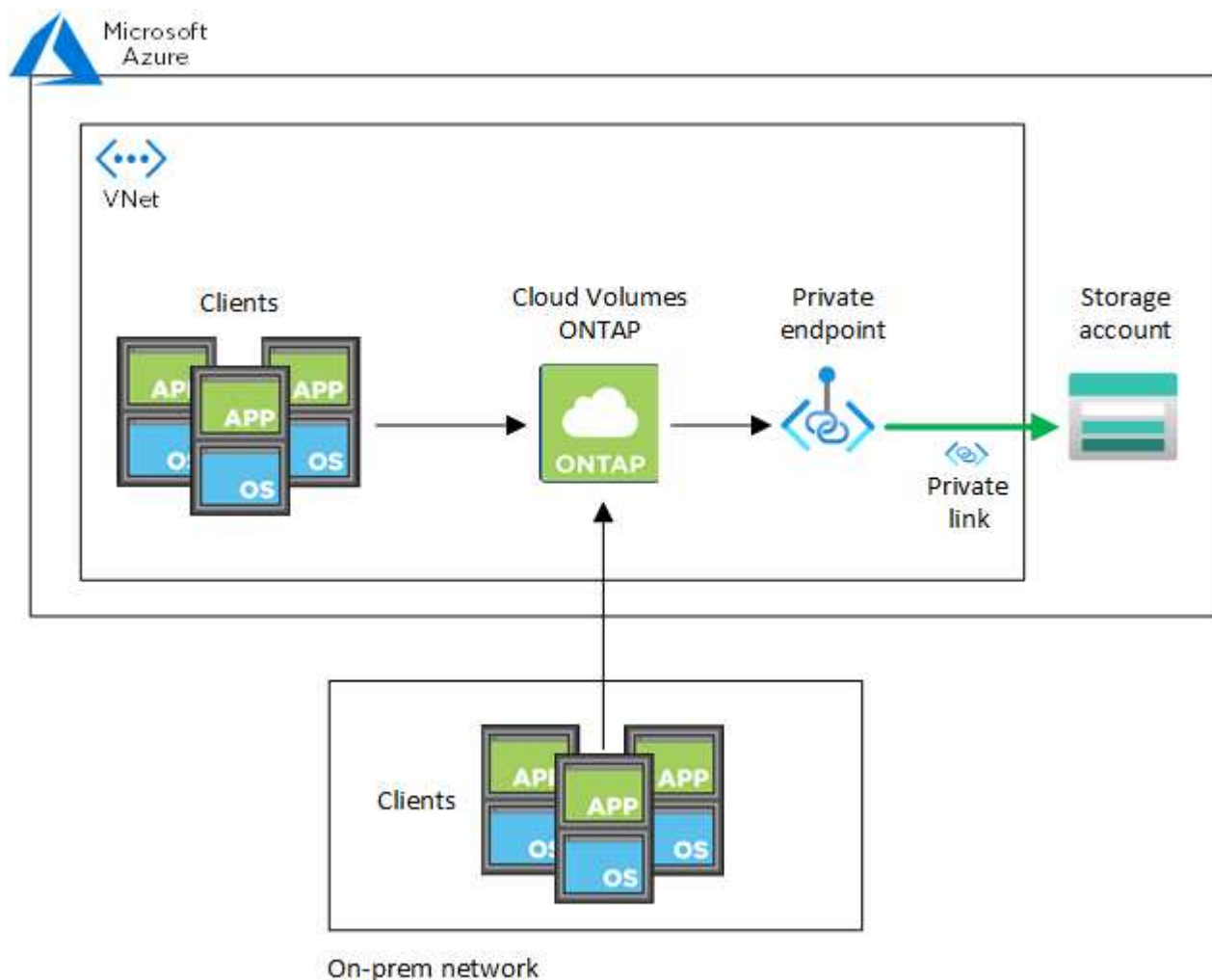
コネクタは、管理対象の Cloud Volumes ONTAP システムまたはにある Azure リージョンと同じ Azure リージョンに導入する必要があります ["Azure リージョンペア"](#) Cloud Volumes ONTAP システム用。この要件により、Cloud Volumes ONTAP とそれに関連付けられたストレージアカウント間で Azure Private Link 接続が使用されるようになります。 ["Cloud Volumes ONTAP での Azure プライベートリンクの使用方法をご確認ください"](#)。

Cloud Volumes ONTAP でのプライベートリンク接続の動作

Cloud Manager 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。



Cloud Manager に Azure プライベート DNS の詳細を指定します

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。そうしないと、Cloud Manager で 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. 次のパラメータを図のように変更して app.conf を編集します。

```
"user-private-dns-zone-settings": {  
  "use-existing": true,  
  "resource-group": "<resource group name of the DNS zone>",  
  "subscription": "<subscription ID>"  
}
```

Subscription パラメータが必要なのは、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だけです。

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

Cloud Manager が特定のアクションの一部として Azure Private Link の作成に失敗すると、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。

Cloud Manager で Azure Private Link を作成できない場合、このデフォルトの動作を変更するためにロールバックを有効にすることができます。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、Cloud Manager は処理を停止し、処理の一環として作成されたすべてのリソースをロールバックします。

ロールバックの有効化は API でのみサポートされます。

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 }
```

Azure Private Link 接続を無効にする

Azure 構成で必要な場合は、Cloud Volumes ONTAP アカウントとストレージアカウント間の Azure プライベートリンク接続を無効にできます。

手順

1. Cloud Manager コンソールの右上にある設定アイコンをクリックし、* コネクタ設定 * 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。

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、Cloud Manager 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. 作業環境でメニューアイコンをクリックし、* マシンの変更 * を選択します。
2. ノードベースの PAYGO ライセンスを使用する場合は、必要に応じて別のライセンスを選択できます。
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たことを確認し、* OK * をクリックします。

Cloud Volumes ONTAP が新しい設定でリブートします。

Cloud Volumes ONTAP に接続しています

Cloud Volumes ONTAP の高度な管理を実行する必要がある場合は、ONTAP System Manager またはコマンドラインインターフェイスを使用します。

System Manager に接続しています

一部の Cloud Volumes ONTAP タスクを System Manager から実行する必要がある場合があります。System Manager は、Cloud Volumes ONTAP システム上で稼働するブラウザベースの管理ツールです。たとえば、LUN を作成する場合は、System Manager を使用する必要があります。

Cloud Manager にアクセスするコンピュータは、Cloud Volumes ONTAP にネットワーク接続している必要があります。たとえば、クラウドプロバイダネットワークにあるジャンプホストから Cloud Manager へのログインが必要になることがあります。



複数の AWS 可用性ゾーンに導入されている場合、Cloud Volumes ONTAP HA 構成では、クラスタ管理インターフェイスにフローティング IP アドレスが使用されます。つまり、外部ルーティングは使用できません。同じルーティングドメインの一部であるホストから接続する必要があります。

手順

1. キャンバスページで、System Manager で管理する Cloud Volumes ONTAP システムをダブルクリックします。
2. メニューアイコンをクリックし、* Advanced > System Manager * をクリックします。
3. [* 起動 *] をクリックします。

System Manager が新しいブラウザタブにロードされます。

4. ログイン画面で、[ユーザー名] フィールドに「* admin *」と入力し、作業環境の作成時に指定したパスワードを入力して、[* サインイン *] をクリックします。

System Manager コンソールがロードされます。これで、Cloud Volumes ONTAP の管理に使用できるようになりました。

Cloud Volumes ONTAP CLI に接続しています

Cloud Volumes ONTAP CLI 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。

SSH を使用して Cloud Volumes に接続するホスト ONTAP は、Cloud Volumes ONTAP にネットワーク接続している必要があります。たとえば、AWS または Azure の Jump ホストから SSH を使用する必要がある場合があります。



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

手順

1. Cloud Manager で、クラスタ管理インターフェ이스の IP アドレスを特定します。
 - a. キャンバスページで、Cloud Volumes ONTAP システムを選択します。
 - b. 右側のペインに表示されるクラスタ管理 IP アドレスをコピーします。
2. SSH を使用して、admin アカウントを使用してクラスタ管理インターフェ이스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、システムの健全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。

インスタンスを起動する前に Cloud Manager Account Admin がプロキシサーバを Cloud Manager に追加していた場合、AutoSupport はそのプロキシサーバを Cloud Volumes ONTAP メッセージに使用するように設定されます。

必要な設定手順は、Cloud Volumes ONTAP インスタンスまたは環境のプロキシサービスを介してアウトバウンドのインターネット接続を確立することだけです。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。

- ["AWS ネットワークの要件"](#)
- ["Azure ネットワークの要件"](#)
- ["Google Cloud のネットワーク要件"](#)

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」](#)。

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"](#)。

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.