



Cloud Volumes ONTAP のドキュメント

Cloud Volumes ONTAP

NetApp
June 01, 2022

This PDF was generated from <https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes-ontap/azure/index.html> on June 01, 2022. Always check docs.netapp.com for the latest.

目次

Cloud Volumes ONTAP のドキュメント	1
リリースノート	2
新機能	2
既知の制限	12
Cloud Volumes ONTAP リリースノート	13
はじめに	14
Cloud Volumes ONTAP の詳細をご覧ください	14
Microsoft Azure で利用を開始しましょう	15
Cloud Volumes ONTAP を使用します	44
ライセンス管理	44
ボリュームと LUN の管理	54
アグリゲートの管理	75
Storage VM 管理	76
セキュリティとデータ暗号化	96
システム管理	107
システムの健全性とイベント	125
概念	127
Cloud Volumes ONTAP ライセンス	127
ストレージ	131
ハイアベイラビリティペア	143
セキュリティ	146
パフォーマンス	148
ノードベースの BYOL のライセンス管理	149
AutoSupport と Active IQ デジタルアドバイザー	151
Cloud Volumes ONTAP のデフォルト設定	152
知識とサポート	155
サポートに登録します	155
ヘルプを表示します	156
法的通知	158
著作権	158
商標	158
特許	158
プライバシーポリシー	158
オープンソース	158

Cloud Volumes ONTAP のドキュメント

リリースノート

新機能

Cloud Manager の Cloud Volumes ONTAP 管理の新機能について説明します。

このページで説明する機能拡張は、Cloud Volumes ONTAP の管理を可能にする Cloud Manager の機能に固有のものです。Cloud Volumes ONTAP ソフトウェア自体の新機能については、"[Cloud Volumes ONTAP のリリースノートに移動します](#)"

2022年5月2日

コネクタの3.9.18リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.11.0

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

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

メディアエーターのアップグレードに関する機能拡張

Cloud ManagerによってHAペアのメディアエーターがアップグレードされると、ブートディスクを削除する前に新しいメディアエーターイメージが使用可能であるかどうかを検証されるようになりました。この変更により、アップグレードプロセスが失敗した場合でもメディアエーターは正常に動作し続けることができます。

K8sタブが削除されました

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

["Cloud ManagerでのKubernetesのデータ管理について説明します"](#)

Azureの年間契約

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

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

["ライセンスの詳細については、こちらをご覧ください"](#)。

2022 年 4 月 3 日

System Manager のリンクが削除されました

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

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

WORM ストレージの充電

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

"[WORM ストレージの価格設定については、こちらをご覧ください](#)"。

2022 年 2 月 27 日

コネクタの3.9.16リリースでは、次の変更が加えられました。

ボリュームウィザードの再設計

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

"[特定のアグリゲートにボリュームを作成する方法について説明します](#)"。

2022 年 2 月 9 日

市場の最新情報

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

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

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

新規のお客様の場合、Cloud Manager は新しい作業環境の作成時に登録を求めるプロンプトを表示します。

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

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

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

2022 年 2 月 6 日

未割り当ての **Exchange** ライセンス

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

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

["未割り当てのノードベースライセンスを交換する方法について説明します"](#)。

2022 年 1 月 30 日

コネクタの3.9.15リリースでは、次の変更が加えられました。

ライセンスの選択を再設計

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

デジタルウォレットの更新

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

ネットアップアカウントあたり **20** システム

Cloud Volumes ONTAP システムの最大数は、使用しているライセンスモデルに関係なく、ネットアップアカウントあたり 20 に制限されます。

a_system_には、HA ペアまたはシングルノードシステムを指定します。たとえば、2 つの Cloud Volumes ONTAP HA ペアと 2 つのシングルノードシステムがある場合、合計 4 つのシステムがあり、アカウントに 16 のシステムを追加で配置できます。

ご質問がある場合は、アカウント担当者または営業チームにお問い合わせください。

["ネットアップアカウントの詳細については、こちらをご覧ください"](#)

2022 年 1 月 2 日

コネクタの3.9.14リリースでは、次の変更が加えられました。

追加の**Azure VM**タイプがサポートされます

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

- E4ds_v4
- E8ds_v4

- E32ds_v4
- E48ds_v4

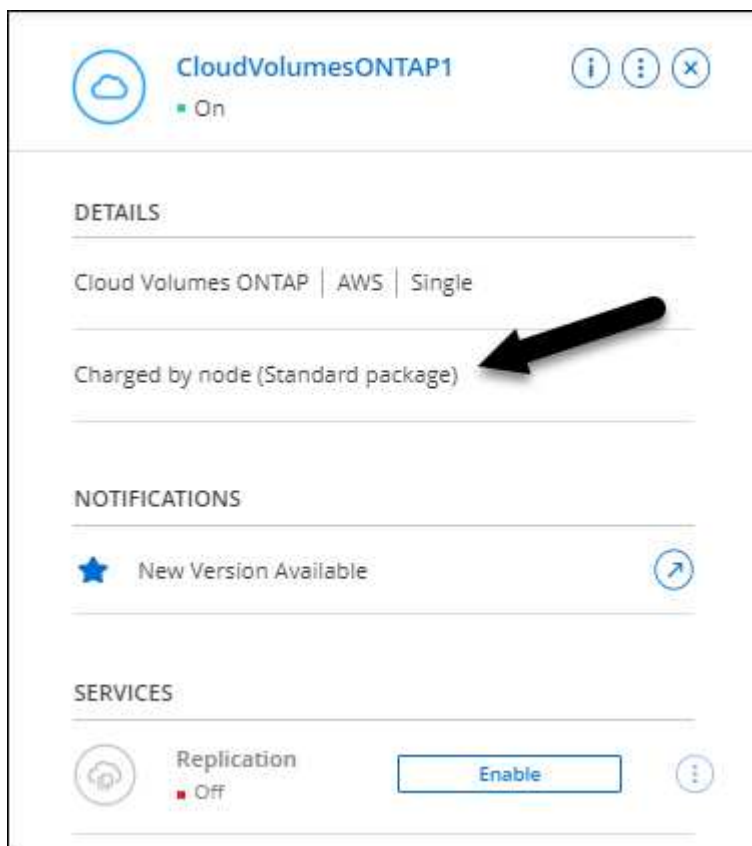
にアクセスします ["Cloud Volumes ONTAP リリースノート"](#) サポートされる構成の詳細については、を参照してください。

FlexClone による課金の更新

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

充電方法が表示されます

Cloud Volumes ONTAP ワーク環境ごとの充電方法がキャンパスの右側のパネルに表示されるようになりました。



ユーザ名を選択します

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

Credentials

User Name

customusername

Password

.....

Confirm Password

.....

ボリューム作成の機能拡張

ボリューム作成機能がいくつか強化されました。

- 使いやすいようにボリューム作成ウィザードの設計が変更されました。
- ボリュームに追加するタグがアプリケーションテンプレートサービスに関連付けられ、リソースの管理を整理して簡単にすることができます。
- これで、NFS 用のカスタムエクスポートポリシーを選択できるようになりました。

✓ Details, Protection & Tags

2 Protocol

3 Disk Type

4 Usage Profile & Tiering Policy

5 Review

Volumes Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol ☐ iSCSI Protocol

Access Control

Custom export policy

Export Policy (1 rule defined)

[Manage volume's export policy](#)

2021 年 11 月 28 日

コネクタの3.9.13リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.10.1

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

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

Keystone Flex サブスクリプション

Keystone Flex Subscriptions を使用して、Cloud Volumes ONTAP HA ペアの料金を支払うことができるようになりました。

Keystone Flex サブスクリプションは、成長に合わせて購入できるサブスクリプションベースのサービスです。OPEX 消費モデルを希望するお客様に、設備投資やリースを先に行うお客様にシームレスなハイブリッドクラウドエクスペリエンスを提供します。

Keystone Flex サブスクリプションは、Cloud Manager から導入可能なすべての新しいバージョンの Cloud Volumes ONTAP でサポートされます。

- ["Keystone Flex Subscriptions の詳細をご覧ください"](#)。
- ["Cloud Manager の Keystone Flex Subscriptions を活用する方法をご紹介します"](#)。

ポート削減

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

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

2021 年 10 月 4 日

コネクタの 3.9.11 リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.10.0

Cloud Manager で Cloud Volumes ONTAP 9.10.0 の導入と管理が可能になりました。

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

2021 年 9 月 2 日

コネクタの 3.9.10 リリースでは、次の変更が加えられました。

Azure のお客様が管理する暗号化キー

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

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

["これらの手順の詳細については、こちらをご覧ください"](#)。

2021 年 7 月 7 日

3.9.8リリースのコネクタには、次の変更が加えられています。

新しい充電方法

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


- * 容量ベースの BYOL * : 容量ベースのライセンスでは、TiB あたりの Cloud Volumes ONTAP 料金を支払うことができます。このライセンスはネットアップアカウントに関連付けられており、ライセンスで十分な容量が確保されていれば、複数の Cloud Volumes ONTAP システムを作成できるようになっています。容量ベースのライセンスは、*Essentials_or_Professional* のいずれかのパッケージ形式で提供されます。
- * Freemium offering * : Freemium により、ネットアップのすべての Cloud Volumes ONTAP 機能が無償で使用できます（クラウドプロバイダの料金は引き続き適用されます）。システムあたりのプロビジョニング可能な容量は 500 GiB に制限されており、サポート契約はありません。最大 10 個の Freemium システムを使用できます。


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

以下に、充電方法の例を示します。

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

☐ Pay-As-You-Go by the hour


☒ Bring your own license

Bring your own license type

Capacity-Based

Package

Professional

☐ Freemium (Up to 500GB)

一般的に使用できる **WORM** ストレージ

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

既存の **Azure** リソースグループを選択します

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



導入に失敗したり削除したりした場合、Cloud Manager は次の権限を使用してリソースグループから Cloud Volumes ONTAP リソースを削除します。

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

Cloud Manager に追加した Azure クレデンシャルの各セットに、これらの権限を必ず付与してください。最新の権限のリストは、[で確認できます "Cloud Manager のポリシーのページです"](#)。

Blob パブリックアクセスが **Azure** で無効になりました

セキュリティの強化として、Cloud Volumes ONTAP 用のストレージアカウントの作成時に Cloud Manager で * Blob パブリックアクセス * が無効になるようになりました。

Azure Private Link の機能強化

デフォルトで、Cloud Manager は、新しい Cloud Volumes ONTAP システムのブート診断ストレージアカウントで Azure Private Link 接続を有効にするようになりました。

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

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

2021年5月30日

コネクタの3.9.7リリースでは、次の変更が加えられました。

auto 階層化ポリシーの最小クーリング期間

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

["最小クーリング期間の調整方法について説明します。"](#)

カスタムエクスポートポリシーの機能拡張

新しい NFS ボリュームを作成すると、カスタムのエクスポートポリシーが昇順に表示されるようになり、必要なエクスポートポリシーが簡単に見つかります。

古いクラウド Snapshot の削除

Cloud Volumes ONTAP システムの導入時および電源をオフにするたびに作成されたルートディスクとブートディスクの古いクラウド Snapshot が Cloud Manager で削除されるようになりました。ルートボリュームとブートボリュームの両方に対して最新の 2 つの Snapshot のみが保持されます。

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

Azure スナップショットを削除するには、Connector で新しい権限が必要になることに注意してください。

["Azure の最新の Cloud Manager ポリシーを表示します"](#)。

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

2021 年 5 月 24 日

Cloud Volumes ONTAP 9.9.1

Cloud Volumes ONTAP 9.9.9.1. を導入および管理できるようになりました。

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

2021 年 4 月 11 日

コネクタの3.9.5リリースでは、次の変更が加えられました。

論理スペースのレポート

Cloud Manager で、Cloud Volumes ONTAP 用に作成した最初の Storage VM の論理スペースのレポートを有効にするようになりました。

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

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

Cloud Manager が Azure for Cloud Volumes ONTAP でストレージアカウントを作成する際に、ストレージアカウントの TLS のバージョンが 1.2 になりました。

2021 年 3 月 8 日

コネクタの3.9.4リリースでは、次の変更が加えられました。

Cloud Volumes ONTAP 9.9.

Cloud Volumes ONTAP 9.9.9.0 を導入および管理できるようになりました。

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

Azure DoD のサポート

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

2021年1月4日

コネクタの3.9.2リリースでは、次の変更が加えられています。

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

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

VNV RAM により、書き込みパフォーマンスが向上します。

Azure でアベイラビリティゾーンを選択してください

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

Location

Azure Region

West US

Availability Zone (Optional)

Select an Availability Zone

None

1

2

3

Subnet

Select a subnet

2020年11月3日

コネクタの3.9.0リリースでは、次の変更が加えられています。

Azure Private Link for Cloud Volumes ONTAP の略

デフォルトでは、Cloud Manager が 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 接続を有効にするようになりました。プライベートリンクは、Azure のエンドポイント間の接続を保護します。

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

既知の制限

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

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

Cloud Manager は FlexGroup ボリュームをサポートしていません

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

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

一部のクラウドプロバイダでは、Cloud Volumes ONTAP がS3をスケールアウトストレージのオプションとしてサポートしていますが、Cloud Managerはこの機能の管理機能を提供していません。CLI を使用すること
が、Cloud Volumes ONTAP からの S3 クライアントアクセスを設定するためのベストプラクティスです。詳細については、を参照してください ["S3 構成パワーガイド"](#)。

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

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

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』"](#)

Cloud Volumes ONTAP リリースノート

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

["Cloud Volumes ONTAP のリリースノートに移動します"](#)

はじめに

Cloud Volumes ONTAP の詳細をご覧ください

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

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

- ストレージの効率化

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

- 高可用性

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

- データ保護

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

また、Cloud Volumes ONTAP はクラウドバックアップと統合されているため、保護のためのバックアップとリストア機能を提供し、クラウドデータの長期アーカイブを実現できます。

["Cloud Backup の詳細については、こちらをご覧ください"](#)

- データの階層化

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

- アプリケーションの整合性

NetApp SnapCenter を使用して、NetApp Snapshot コピーの整合性を確保します。

["SnapCenter の詳細については、こちらをご覧ください"](#)

- データセキュリティ

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

- プライバシーコンプライアンスの管理

クラウドデータセンストとの統合により、データコンテキストを把握し、機密データを識別できます。

"クラウドデータセンスの詳細をご確認ください"



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

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

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

Microsoft Azure で利用を開始しましょう

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

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

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

最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合は、Cloud Manager からコネクタの導入を求められます。

Cloud Manager には、ワークロードの要件に応じた事前設定パッケージが用意されています。または、独自の設定を作成することもできます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。 **"詳細はこちら"**。

 ネットワークを設定します

1. VNet とサブネットがコネクタと Cloud Volumes ONTAP 間の接続をサポートすることを確認します。
2. ターゲット VNet からのアウトバウンドインターネットアクセスを有効にして、コネクタと Cloud Volumes ONTAP が複数のエンドポイントに接続できるようにします。

コネクタはアウトバウンドのインターネットアクセスがないと Cloud Volumes ONTAP を管理できないため、この手順は重要です。アウトバウンド接続を制限する必要がある場合は、のエンドポイントのリストを参照してください **"コネクタと Cloud Volumes ONTAP"**。

"ネットワーク要件の詳細については、こちらをご覧ください"。

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

関連リンク

- **"Cloud Manager からコネクタを作成します"**
- **"Azure Marketplace からコネクタを作成する"**
- **"Linux ホストへの Connector ソフトウェアのインストール"**
- **"Cloud Manager が権限で実行できる処理"**

AzureでCloud Volumes ONTAP 構成を計画

Azure で Cloud Volumes ONTAP を導入する場合は、ワークロード要件に一致する事前設定済みのシステムを選択するか、または独自の設定を作成できます。独自の設定を選択する場合は、使用可能なオプションを理解しておく必要があります。

Cloud Volumes ONTAP ライセンスを選択します

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

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

サポートされているリージョンを選択します

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

サポートされているVMタイプを選択してください

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

["Azure で Cloud Volumes ONTAP がサポートされている構成"](#)

ストレージの制限を確認

Cloud Volumes ONTAP システムの未フォーマット時の容量制限は、ライセンスに関連付けられています。追加の制限は、アグリゲートとボリュームのサイズに影響します。設定を計画する際には、これらの制限に注意する必要があります。

["Azure での Cloud Volumes ONTAP のストレージの制限"](#)

Azureでシステムのサイズを設定します

Cloud Volumes ONTAP システムのサイジングを行うことで、パフォーマンスと容量の要件を満たすのに役立ちます。VM タイプ、ディスクタイプ、およびディスクサイズを選択する際には、次の点に注意してください。

仮想マシンのタイプ

でサポートされている仮想マシンタイプを確認します ["Cloud Volumes ONTAP リリースノート"](#) サポートされている各 VM タイプの詳細を確認します。各 VM タイプがサポートするデータディスクの数には制限があることに注意してください。

- ["Azure のドキュメント：「汎用仮想マシンのサイズ」"](#)
- ["Azure のドキュメント：「Memory optimized virtual machine sizes」"](#)

Azure のディスクタイプ

Cloud Volumes ONTAP 用のボリュームを作成する場合は、ONTAP がディスクとして使用する基盤となるクラウドストレージを選択する必要があります。

HA システムでは、Premium ページ BLOB を使用します。一方、シングルノードシステムでは、次の 2 種類の Azure Managed Disks を使用できます。

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

これらのディスクのユースケースの詳細については、を参照してください "[Microsoft Azure のドキュメント](#) : 「What disk types are available in Azure ?」"。

Azure のディスクサイズ

Cloud Volumes ONTAP インスタンスを起動するときは、アグリゲートのデフォルトのディスクサイズを選択する必要があります。Cloud Manager では、このディスクサイズを初期アグリゲートに使用します。また、簡易プロビジョニングオプションを使用した場合に作成される追加のアグリゲートにも使用します。別のディスクサイズを使用するアグリゲートを作成できます デフォルトでは、です "[高度な割り当てオプションを使用する](#)"。



アグリゲート内のディスクはすべて同じサイズである必要があります。

ディスクサイズを選択する際には、いくつかの要素を考慮する必要があります。ディスクサイズは、ストレージのコスト、アグリゲートに作成できるボリュームのサイズ、Cloud Volumes ONTAP で使用可能な総容量、ストレージパフォーマンスに影響します。

Azure Premium ストレージのパフォーマンスは、ディスクサイズに依存します。ディスク容量が大きいほど、IOPS とスループットが向上します。たとえば、1 TiB のディスクを選択すると、500 GiB のディスクよりも高いパフォーマンスを低コストで実現できます。

標準ストレージのディスクサイズにはパフォーマンスの違いはありません。必要な容量に基づいてディスクサイズを選択する必要があります。

ディスクサイズ別の IOPS とスループットについては、Azure を参照してください。

- "[Microsoft Azure : Managed Disks の価格](#)"
- "[Microsoft Azure : Page Blob の価格設定](#)"

デフォルトのシステムディスクを表示します

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

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



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

ネットワーク情報を収集

Cloud Volumes ONTAP を Azure に導入する場合は、仮想ネットワークの詳細を指定する必要があります。ワークシートを使用して、管理者から情報を収集できます。

Azure の情報	あなたの価値
地域	
仮想ネットワーク (Vnet)	
サブネット	
Network Security Group (独自のグループを使用している場合)	

書き込み速度を選択します

Cloud Manager では、Cloud Volumes ONTAP の書き込み速度を選択できます。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。"[書き込み速度の詳細については、こちらをご覧ください。](#)"。

ボリュームの使用プロファイルを選択してください

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。Cloud Manager でボリュームを作成する場合は、これらの機能を有効にするプロファイルを選択するか、無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

NetApp Storage Efficiency 機能には、次のようなメリットがあります。

シンプロビジョニング

物理ストレージプールよりも多くの論理ストレージをホストまたはユーザに提供します。ストレージスペースは、事前にストレージスペースを割り当てる代わりに、データの書き込み時に各ボリュームに動的に割り当てられます。

重複排除

同一のデータブロックを検索し、単一の共有ブロックへの参照に置き換えることで、効率を向上します。この手法では、同じボリュームに存在するデータの冗長ブロックを排除することで、ストレージ容量の要件を軽減します。

圧縮

プライマリ、セカンダリ、アーカイブストレージ上のボリューム内のデータを圧縮することで、データの格納に必要な物理容量を削減します。

Azure の Cloud Volumes ONTAP のネットワーク要件

Cloud Volumes ONTAP システムが適切に動作するように Azure ネットワークをセットアップします。これには、コネクタと Cloud Volumes ONTAP のネットワークも含まれます。

Cloud Volumes ONTAP の要件

Azure では、次のネットワーク要件を満たしている必要があります。

アウトバウンドインターネットアクセス

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

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

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

"AutoSupport の検証方法について説明します"。

IP アドレス

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

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

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



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

Azure サービスへのセキュアな接続

Cloud Manager は、Cloud Volumes ONTAP がプライベートで Azure サービスに接続できるように、VNet サービスエンドポイントと Azure プライベートリンクエンドポイントを設定します。

サービスエンドポイント

Cloud Manager を使用すると、VNet サービスエンドポイントはデータ階層化用に Cloud Volumes ONTAP から Azure Blob ストレージへのセキュアな接続を確立できます。Cloud Volumes ONTAP から Azure サービスへの追加のサービスエンドポイントはサポートされません。

Cloud Manager ポリシーに以下の権限が設定されている場合、Cloud Manager は VNet サービスエンドポイントを有効にします。

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

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

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

プライベートエンドポイント

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。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 プライベート DNS を使用している場合は、構成ファイルを編集する必要があります。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 プライベートリンクとクラウドの使用の詳細については、こちらをご覧ください Volume ONTAP の略"](#)。

他の ONTAP システムへの接続

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

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

HA インターコネクトのポート

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

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

Azure リソースグループには **HA** ペアが 1 つしかありません

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

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

セキュリティグループ

セキュリティグループを作成する必要はありません。セキュリティグループは Cloud Manager で自動的に作成されます。独自のルールを使用する必要がある場合は、以下のセキュリティグループルールを参照してください。

セキュリティグループのルール

Cloud Manager で作成される Azure セキュリティグループには、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドとアウトバウンドのルールが含まれています。テスト目的でポートを参照したり、独自のセキュリティグループを使用したりする場合に使用します。

Cloud Volumes ONTAP のセキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。

シングルノードシステムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの 2 つです	説明
1000 inbound_ssh	22 TCP	Any から Any	クラスタ管理 LIF または ノード管理 LIF の IP アドレスへの SSH アクセス
1001 INBOUND _http	80 TCP	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
1002 INBOUND _111_TCP	111 TCP	Any から Any	NFS のリモートプロシージャコール
1003 INBONED_111_UDP	111 UDP	Any から Any	NFS のリモートプロシージャコール
1004 INBOUND _139	139 TCP	Any から Any	CIFS の NetBIOS サービスセッション
1005 inbound_161-162_TCP	161-162 TCP	Any から Any	簡易ネットワーク管理プロトコル
1006 INBOUND _161-162_UDP	UDP 161-162	Any から Any	簡易ネットワーク管理プロトコル
1007 INBOUND _443	443 tcp	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
1008 INBOUND _445	445 TCP	Any から Any	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
1009 INBOUND _635_TCP	635 TCP	Any から Any	NFS マウント
1010 INBOUND _635_UDP	635 UDP	Any から Any	NFS マウント
1011 INBOUND _749	749 TCP	Any から Any	Kerberos
1012 INBOUND _2049_TCP	2049 TCP	Any から Any	NFS サーバデーモン
1013 INBOUND _2049_UDP	2049 UDP	Any から Any	NFS サーバデーモン
1014 インバウンド _3260	3260 TCP	Any から Any	iSCSI データ LIF を介した iSCSI アクセス

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの 2 つです	説明
1015 INBOUND _4045-4046_tcp の略	4045-4046 TCP	Any から Any	NFS ロックデーモンとネットワークステータスマニタ
1016 INBOUND _4045-4046_UDP	4045-4046 UDP	Any から Any	NFS ロックデーモンとネットワークステータスマニタ
1017 INBOUND _10000	10000 TCP	Any から Any	NDMP を使用したバックアップ
1018 INBOUND _11104-11105	11104-11105 TCP	Any から Any	SnapMirror によるデータ転送
3000 inbound_deny_all_tcp	任意のポート TCP	Any から Any	他のすべての TCP インバウンドトラフィックをブロックします
3001 INBOUND _DENY_ALL_UDP	任意のポート UDP	Any から Any	他のすべての UDP 着信トラフィックをブロックします
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoadBalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

HA システムのインバウンドルール

次のルールでは、説明で特定の着信トラフィックがブロックされている場合を除き、トラフィックは許可されます。



HA システムのインバウンドデータトラフィックは Azure Standard Load Balancer を経由するため、シングルノードシステムよりもインバウンドルールが少なくなります。そのため、「AllowAzureLoadBalancerInBound」ルールに示されているように、ロードバランサからのトラフィックがオープンである必要があります。

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの 2 つです	説明
100 インバウンド _443	443 : 任意のプロトコル	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
101 INBOUND _111_TCP	111 すべてのプロトコル	Any から Any	NFS のリモートプロシージャコール

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの 2 つです	説明
102 インバウンド _2049_TCP	2049 任意のプロトコル	Any から Any	NFS サーバデーモン
111 inbound_ssh	22 すべてのプロトコル	Any から Any	クラスタ管理 LIF または ノード管理 LIF の IP アドレスへの SSH アクセス
121 INBOUND _53	53 任意のプロトコル	Any から Any	DNS と CIFS
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

アウトバウンドルール

Cloud Volumes 用の事前定義済みセキュリティグループ ONTAP は、すべての発信トラフィックをオープンします。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

Cloud Volumes ONTAP 用の定義済みセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、Cloud Volumes ONTAP による発信通信に必要なポートのみを開くことができます。



source は、Cloud Volumes ONTAP システムのインターフェイス（IP アドレス）です。

サービス	ポート	プロ トコ ル	ソース	宛先	目的
Active Directory	88	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V 認証
	137	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	ノード管理 LIF	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP およ び UDP	ノード管理 LIF	Active Directory フォレスト	LDAP
	445	TCP	ノード管理 LIF	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	ノード管理 LIF	Active Directory フォレスト	Kerberos キー管理
	749	TCP	ノード管理 LIF	Active Directory フォレスト	Kerberos V Change & Set Password (RPCSEC_GSS)
	88	TCP	データ LIF (NFS、CIFS、iSCSI)	Active Directory フォレスト	Kerberos V 認証
	137	UDP	データ LIF (NFS、CIFS)	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	データ LIF (NFS、CIFS)	Active Directory フォレスト	NetBIOS データグラムサービス
	139	TCP	データ LIF (NFS、CIFS)	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP およ び UDP	データ LIF (NFS、CIFS)	Active Directory フォレスト	LDAP
	445	TCP	データ LIF (NFS、CIFS)	Active Directory フォレスト	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
	464	TCP	データ LIF (NFS、CIFS)	Active Directory フォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	データ LIF (NFS、CIFS)	Active Directory フォレスト	Kerberos キー管理
	749	TCP	データ LIF (NFS、CIFS)	Active Directory フォレスト	Kerberos V Change & Set Password (RPCSEC_GSS)

サービス	ポート	プロトコル	ソース	宛先	目的
AutoSupport	HTTPS	443	ノード管理 LIF	support.netapp.com	AutoSupport（デフォルトは HTTPS）
	HTTP	80	ノード管理 LIF	support.netapp.com	AutoSupport（転送プロトコルが HTTPS から HTTP に変更された場合のみ）
DHCP	68	UDP	ノード管理 LIF	DHCP	初回セットアップ用の DHCP クライアント
DHCP	67	UDP	ノード管理 LIF	DHCP	DHCP サーバ
DNS	53	UDP	ノード管理 LIF とデータ LIF（NFS、CIFS）	DNS	DNS
NDMP	18600 ~ 18699	TCP	ノード管理 LIF	宛先サーバ	NDMP コピー
SMTP	25	TCP	ノード管理 LIF	メールサーバ	SMTP アラート。AutoSupport に使用できます
SNMP	161	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	161	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	TCP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
	162	UDP	ノード管理 LIF	サーバを監視します	SNMP トラップによる監視
SnapMirror	11104	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror のクラスタ間通信セッションの管理
	11105	TCP	クラスタ間 LIF	ONTAP クラスタ間 LIF	SnapMirror によるデータ転送
syslog	514	UDP	ノード管理 LIF	syslog サーバ	syslog 転送メッセージ

コネクタの要件

コネクタがパブリッククラウド環境内のリソースやプロセスを管理できるように、ネットワークを設定します。最も重要なステップは、さまざまなエンドポイントへのアウトバウンドインターネットアクセスを確保することです。



ネットワークでインターネットへのすべての通信にプロキシサーバを使用している場合は、[設定] ページでプロキシサーバを指定できます。を参照してください ["プロキシサーバを使用するようにコネクタを設定します"](#)。

ターゲットネットワークへの接続

コネクタには、Cloud Volumes ONTAP を導入する VPC および VNet へのネットワーク接続が必要です。

たとえば、企業ネットワークにコネクタを設置する場合は、Cloud Volumes ONTAP を起動する VPC または VNet への VPN 接続を設定する必要があります。

アウトバウンドインターネットアクセス

Connector では、パブリッククラウド環境内のリソースとプロセスを管理するためにアウトバウンドインターネットアクセスが必要です。

エンドポイント	目的
\ https://support.netapp.com	ライセンス情報を取得し、ネットアップサポートに AutoSupport メッセージを送信するため。
\ https://*.cloudmanager.cloud.netapp.com	Cloud Manager 内で SaaS の機能やサービスを提供できます。
¥ https://cloudmanagerinfraproduct.azurecr.io ¥ https://*.blob.core.windows.net	をクリックして、Connector と Docker コンポーネントをアップグレードします。

セキュリティグループのルール

コネクタのセキュリティグループには、インバウンドとアウトバウンドの両方のルールが必要です。

インバウンドルール

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

アウトバウンドルール

コネクタの事前定義されたセキュリティグループは、すべての発信トラフィックを開きます。これが可能な場合は、基本的なアウトバウンドルールに従います。より厳格なルールが必要な場合は、高度なアウトバウンドルールを使用します。

基本的なアウトバウンドルール

コネクタの事前定義されたセキュリティグループには、次のアウトバウンドルールが含まれています。

ポート	プロトコル	目的
すべて	すべての TCP	すべての発信トラフィック
すべて	すべての UDP	すべての発信トラフィック

高度なアウトバウンドルール

発信トラフィックに固定ルールが必要な場合は、次の情報を使用して、コネクタによる発信通信に必要なポートだけを開くことができます。



送信元 IP アドレスは、コネクタホストです。

サービス	ポート	プロトコル	宛先	目的
API コールと AutoSupport	443	HTTPS	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	APIがAzure とONTAP にコールし、クラウドデータを検知してランサムウェアサービスに感染し、AutoSupport メッセージをネットアップに送信
DNS	53	UDP	DNS	Cloud Manager による DNS 解決に使用されます

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

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

データ暗号化の概要

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

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

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

キーローテーション

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

データの暗号化方法

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

HA ペア

- Cloud Volumes ONTAP 用のすべての Azure ストレージアカウントは、お客様が管理するキーを使用して暗号化されます。
- 新しいストレージアカウント（ディスクやアグリゲートを追加する場合など）も同じキーを使用します。

シングルノード

- Cloud Volumes ONTAP 用のすべての Azure ストレージアカウントは、お客様が管理するキーを使用して暗号化されます。
- ルートディスク、ブートディスク、およびデータディスクの場合、Cloud Manager はを使用します "[ディスク暗号化セット](#)"を使用して、管理対象ディスクで暗号化キーを管理できます。
- 新しいデータディスクでも同じディスク暗号化セットが使用されます。
- NVRAM とコアディスクは、お客様が管理するキーではなく、Microsoft が管理するキーを使用して暗号化されます。

キーボールドを作成し、キーを生成します

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

手順

1. "[Azure サブスクリプションでキーヴォールトを作成します](#)".

キーヴォールトの次の要件に注意してください。

- キーヴォールトは、Cloud Volumes ONTAP システムと同じリージョンに配置する必要があります。
- 次のオプションを有効にする必要があります。
 - * Soft -delete * （このオプションはデフォルトで有効ですが、DISABLE_NOT BE 無効にする必要があります）
 - * パージ保護 *
 - * Azure Disk Encryption for Volume Encryption * （シングルノード Cloud Volumes ONTAP システムのみ）

2. "[キーボールドでキーを生成します](#)".

キーに関する次の要件に注意してください。

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

暗号化キーを使用する作業環境を作成します

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

シングルノードの Cloud Volumes ONTAP システムでお客様が管理するキーを使用する場合は、Cloud Manager Connector で次の権限を確認します。

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

最新の権限のリストは、で確認できます ["Cloud Manager のポリシーのページです"](#)。



最初の3つの権限はHAペアには必要ありません。

手順

1. 次の Cloud Manager API 呼び出しを使用して、Azure サブスクリプション内の主要なバックアップのリストを取得します。

HA ペアの場合：「GET /azure-ha/ma/metadata/vaults」

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

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

["この API 呼び出しの詳細を確認してください"](#)。

2. 次の Cloud Manager API 呼び出しを使用して、バックアップ内のキーのリストを取得します。

HA ペアの場合：「GET /azure-ha/ma/metadata/keys - vault」

シングルノードの場合：「get/azure-vsa/metadata/keys - vault」

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

["この API 呼び出しの詳細を確認してください"](#)。

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

a. HA ペアの場合：

「POST/Azure/HA/ 作業環境」

要求の本文には次のフィールドを含める必要があります。

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

["この API 呼び出しの詳細を確認してください"](#)。

b. シングルノードシステムの場合：

「POST/Azure/VSA/Working-Environments」

要求の本文には次のフィールドを含める必要があります。

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

+
["この API 呼び出しの詳細を確認してください"](#)。

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

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

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

フリーミアム

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

手順

1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
 - a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+

 Add Subscription

Apply

Cancel

- a. Cloud Managerに戻ったら、課金方法のページが表示されたら「* Freemium *」を選択します。

Select Charging Method

☐ Professional

By capacity

▼

☐ Essential

By capacity

▼

☒ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

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

容量単位のライセンスです

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

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

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

"容量単位のライセンスに関する詳細は、こちらをご覧ください"。

以降のセクションでは、これらの各消費モデルの使用方法について説明します。

BYOL

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

手順

1. "ライセンスの取得については、ネットアップの営業部門にお問い合わせください"
2. "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"

Cloud Managerは、ネットアップのライセンスサービスを自動的に照会して、ネットアップサポートサイトのアカウントに関連付けられているライセンスに関する詳細を取得します。エラーがなければ、Cloud Managerはライセンスをデジタルウォレットに自動的に追加します。

Cloud Volumes ONTAP で使用するには、ライセンスがデジタルウォレットから入手できる必要があります。必要に応じて、を実行できます "手動でライセンスをDigital Walletに追加します"。

3. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
 - a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev (Default)

Marketplace Subscription

ⓘ A marketplace subscription isn't associated with the selected Azure subscription.

+ Add Subscription

Apply Cancel

- a. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。

Select Charging Method

<input checked="" type="radio"/> Professional	By capacity	▼
<input type="radio"/> Essential	By capacity	▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity	▼
<input type="radio"/> Per Node	By node	▼

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

PAYGOサブスクリプション

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

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

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

手順

1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。
 - a. [詳細とクレデンシャル]ページで、[クレデンシャルの編集]、[サブスクリプションの追加]の順にクリックし、プロンプトに従ってAzure Marketplaceで従量課金制サービスに登録します。

The screenshot shows the 'Edit Credentials & Add Subscription' page. It has a title bar with the text 'Edit Credentials & Add Subscription'. Below the title bar is a section titled 'Associate Subscription to Credentials' with an information icon. Under this section, there are two dropdown menus: 'Credentials' with 'Managed Service Identity' selected, and 'Azure Subscription' with 'OCCM Dev (Default)' selected. Below these is a box labeled 'Marketplace Subscription' containing a message: 'A marketplace subscription isn't associated with the selected Azure subscription.' Below this box is a button with a plus icon and the text 'Add Subscription'. At the bottom of the page are two buttons: 'Apply' (blue) and 'Cancel' (grey).

- b. Cloud Managerに戻ったら、課金方法のページで容量ベースのパッケージを選択します。

The screenshot shows the 'Select Charging Method' page. It has a title bar with the text 'Select Charging Method'. Below the title bar is a list of four options, each with a radio button, a label, a charging method button, and a dropdown arrow. The options are: 'Professional' (selected with a blue checkmark), 'Essential', 'Freemium (Up to 500 GiB)', and 'Per Node'. The 'Professional' option has a blue 'By capacity' button. The 'Essential' option has a blue 'By capacity' button. The 'Freemium (Up to 500 GiB)' option has a blue 'By capacity' button. The 'Per Node' option has a purple 'By node' button.

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



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

年間契約

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

手順

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

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

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

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

Select Charging Method	
<input checked="" type="radio"/> Professional	By capacity ▼
<input type="radio"/> Essential	By capacity ▼
<input type="radio"/> Freemium (Up to 500 GiB)	By capacity ▼
<input type="radio"/> Per Node	By node ▼

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

Keystone Flex サブスクリプション

Keystone Flexサブスクリプションは、ビジネスの成長に合わせて拡張できるサブスクリプションベースのサービスです。 ["Keystone Flex Subscriptions の詳細をご覧ください"](#)。

手順

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

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1 v

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

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

Azure で Cloud Volumes ONTAP を起動します

Cloud Manager で Cloud Volumes ONTAP の作業環境を作成することで、Azure で単一ノードシステムまたは HA ペアを起動できます。

作業環境を作成するには、次の作業が必要です。

- 稼働中のコネクタ。
 - を用意しておく必要があります "[ワークスペースに関連付けられているコネクタ](#)".
 - "[コネクタをで実行したままにする準備をしておく必要があります 常時](#)".

- 使用する構成についての理解。

設定を選択し、ネットワーク管理者から Azure ネットワーク情報を入手しておく必要があります。詳細については、[を参照してください "Cloud Volumes ONTAP 構成を計画"](#)。

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

["ライセンスの設定方法について説明します"](#)。

Azure で Cloud Volumes ONTAP システムを作成すると、リソースグループ、ネットワークインターフェイス、ストレージアカウントなどの Azure オブジェクトがいくつか作成されます。ウィザードの最後にあるリソースの概要を確認できます。



データ損失の可能性があります

Cloud Volumes ONTAP システムごとに新しい専用のリソースグループを使用することを推奨します。

データ損失のリスクがあるため、既存の共有リソースグループに Cloud Volumes ONTAP を導入することは推奨されません。導入の失敗や削除が発生した場合、Cloud Manager は共有リソースグループから Cloud Volumes ONTAP リソースを削除できますが、Azure ユーザが誤って共有リソースグループから Cloud Volumes ONTAP リソースを削除してしまう可能性があります。

手順

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

次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
作業環境名	Cloud Manager は、作業環境名を使用して、Cloud Volumes ONTAP システムと Azure 仮想マシンの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
リソースグループタグ	タグは、Azure リソースのメタデータです。このフィールドにタグを入力すると、Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、 を参照してください "Microsoft Azure のドキュメント：「Using tags to organize your Azure resources" 。

フィールド	説明
ユーザ名とパスワード	Cloud Volumes ONTAP クラスタ管理者アカウントのクレデンシャルです。このクレデンシャルを使用して、System Manager またはその CLI から Cloud Volumes ONTAP に接続できます。default_admin_user の名前をそのまま使用するか ' カスタム・ユーザー名に変更します
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 " クレデンシャルを追加する方法について説明します "。

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

▶ <https://docs.netapp.com/ja-jp/cloud-manager-cloud-volumes->

5. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
 - ["クラウドデータセンスの詳細をご確認ください"](#)。
 - ["Cloud Backup の詳細については、こちらをご覧ください"](#)。
 - ["監視サービスの詳細については、こちらをご覧ください"](#)。
6. * 場所と接続 *: 場所、リソースグループ、セキュリティグループを選択し、チェックボックスを選択して、コネクタとターゲットの場所間のネットワーク接続を確認します。

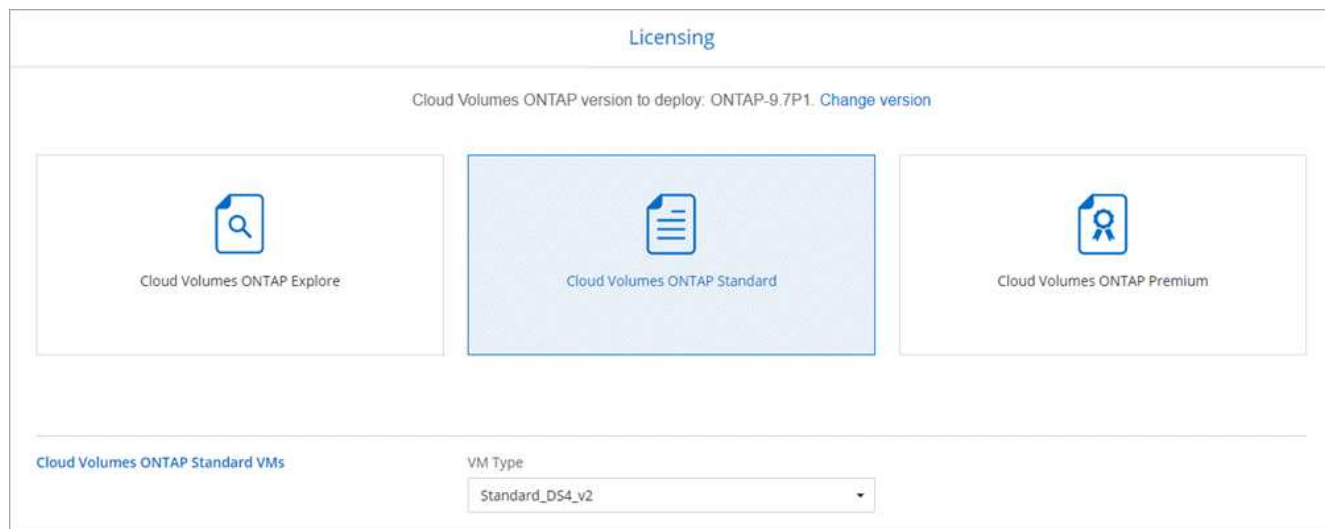
次の表では、ガイダンスが必要なフィールドについて説明します。

フィールド	説明
場所	シングルノードシステムの場合は、 Cloud Volumes ONTAP を導入するアベイラビリティゾーンを選択できます。AZ を選択しない場合は、 Cloud Manager によってその AZ が選択されます。
リソースグループ	<p>Cloud Volumes ONTAP の新しいリソースグループを作成するか、既存のリソースグループを使用します。Cloud Volumes ONTAP には、新しい専用のリソースグループを使用することを推奨します。既存の共有リソースグループに Cloud Volumes ONTAP を導入することは可能ですが、データ損失のリスクがあるため推奨されません。詳細については、上記の警告を参照してください。</p> <p>Azure に導入する Cloud Volumes ONTAP HA ペアごとに専用のリソースグループを使用する必要があります。リソースグループでサポートされる HA ペアは 1 つだけです。Azure リソースグループに 2 つ目の Cloud Volumes ONTAP HA ペアを導入しようとすると、Cloud Manager で接続の問題が発生します。</p> <div style="display: flex; align-items: center;">  <div> <p>使用している Azure アカウントに割り当てられている場合 "必要な権限"導入の失敗や削除が発生した場合、Cloud Manager はリソースグループから Cloud Volumes ONTAP リソースを削除します。</p> </div> </div>
セキュリティグループ	既存のセキュリティグループを選択する場合は、Cloud Volumes ONTAP の要件を満たす必要があります。 "デフォルトのセキュリティグループを表示します" 。

7. * 充電方法と NSS アカウント *: このシステムで使用する充電オプションを指定し、ネットアップサポートサイトのアカウントを指定します。
 - ["Cloud Volumes ONTAP のライセンスオプションについて説明します"](#)。
 - ["ライセンスの設定方法について説明します"](#)。
8. * 構成済みパッケージ *: Cloud Volumes ONTAP システムを迅速に導入するパッケージを 1 つ選択するか、* 独自の構成を作成 * をクリックします。

いずれかのパッケージを選択した場合は、ボリュームを指定してから、設定を確認して承認するだけで済みます。

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



システムの起動後に必要な変更があった場合は、後でライセンスまたは仮想マシンのタイプを変更できません。



選択したバージョンで新しいリリース候補、一般的な可用性、またはパッチリリースが利用可能な場合は、作業環境の作成時に Cloud Manager によってシステムがそのバージョンに更新されます。たとえば、Cloud Volumes ONTAP 9.6 RC1 と 9.6 GA を選択した場合、更新が行われます。たとえば、9.6 から 9.7 への更新など、あるリリースから別のリリースへの更新は行われません。

10. * Azure Marketplace からサブスクリプション * : Cloud Manager で Cloud Volumes ONTAP のプログラムによる導入を有効にできなかった場合は、以下の手順に従ってください。
11. * 基盤となるストレージリソース * : 初期アグリゲートの設定を選択します。ディスクタイプ、各ディスクのサイズ、BLOB ストレージへのデータ階層化を有効にするかどうかを指定します。

次の点に注意してください。

- ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できません。
- ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプションを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

ディスクの種類とサイズの選択については、を参照してください ["Azure でのシステムのサイジング"](#)。

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

["データ階層化の詳細については、こちらをご覧ください。"](#)

12. * 書き込み速度と WORM * (シングルノードシステムのみ) : * Normal * または * High * 書き込み速度を

選択し、必要に応じて Write Once 、 Read Many （ WORM ） ストレージをアクティブにします。

"書き込み速度の詳細については、こちらをご覧ください。"。

Cloud Backup が有効になっている場合やデータ階層化が有効になっている場合は、 WORM を有効にすることはできません。

"WORM ストレージの詳細については、こちらをご覧ください。"。

13. * Secure Communication to Storage & WORM * （ HA のみ ） : Azure ストレージアカウントへの HTTPS 接続を有効にするかどうかを選択し、必要に応じて Write Once Read Many （ WORM ） ストレージをアクティブにします。

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

"WORM ストレージの詳細については、こちらをご覧ください。"。

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

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

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

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL と呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンスドオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。

フィールド	説明
イニシエータグループと IQN（iSCSI のみ）	iSCSI ストレージターゲットは LUN（論理ユニット）と呼ばれ、標準のブロックデバイスとしてホストに提示されます。イニシエータグループは、iSCSI ホストのノード名のテーブルであり、どのイニシエータがどの LUN にアクセスできるかを制御します。iSCSI ターゲットは、標準のイーサネットネットワークアダプタ（NIC）、ソフトウェアイニシエータを搭載した TOE カード、CNA、または専用の HBA を使用してネットワークに接続され、iSCSI Qualified Name（IQN）で識別されます。iSCSI ボリュームを作成すると、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" 。

次の図は、CIFS プロトコルの [Volume] ページの設定を示しています。

Volume Details, Protection & Protocol

Details & Protection

Volume Name:

Size (GB):

Snapshot Policy: default

Default Policy

Protocol

NFS
CIFS
iSCSI

Share name:

Permissions: Full Control

Users / Groups:

Valid users and groups separated by a semicolon

15. * CIFS セットアップ*：CIFS プロトコルを選択した場合は、CIFS サーバをセットアップします。

フィールド	説明
DNS プライマリおよびセカンダリ IP アドレス	CIFS サーバの名前解決を提供する DNS サーバの IP アドレス。リストされた DNS サーバには、CIFS サーバが参加するドメインの Active Directory LDAP サーバとドメインコントローラの検索に必要なサービスロケーションレコード（SRV）が含まれている必要があります。
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。

フィールド	説明
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。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。

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

詳細については、を参照してください ["ボリューム使用率プロファイルについて"](#) および ["データ階層化の概要"](#)。

17. * レビューと承認 *：選択内容を確認して確認します。
- 設定の詳細を確認します。
 - 詳細情報 * をクリックして、Cloud Manager で購入するサポートと Azure リソースの詳細を確認します。
 - [* I understand ... *（理解しています ... *）] チェックボックスを選択
 - [Go*] をクリックします。

Cloud Manager は Cloud Volumes ONTAP システムを導入します。タイムラインで進行状況を追跡できます。

Cloud Volumes ONTAP システムの導入で問題が発生した場合は、障害メッセージを確認してください。作業環境を選択し、* 環境の再作成 * をクリックすることもできます。

詳細については、を参照してください ["NetApp Cloud Volumes ONTAP のサポート"](#)。

完了後

- CIFS 共有をプロビジョニングした場合は、ファイルとフォルダに対する権限をユーザまたはグループに付与し、それらのユーザが共有にアクセスしてファイルを作成できることを確認します。
- ボリュームにクォータを適用する場合は、System Manager または CLI を使用します。

クォータを使用すると、ユーザ、グループ、または qtree が使用するディスク・スペースとファイル数を制限または追跡できます。

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](#)"。

ライセンスをデジタルウォレットに追加する方法

ネットアップの営業担当者からライセンスを購入されると、ネットアップからシリアル番号と追加のライセンス情報を記載したEメールが送信されます。

その間、Cloud Managerはネットアップのライセンスサービスを自動的に照会し、ネットアップサポートサイトのアカウントに関連付けられているライセンスに関する詳細を取得します。エラーがなければ、Cloud Managerはライセンスをデジタルウォレットに自動的に追加します。

Cloud Managerでライセンスを追加できない場合は、手動でDigital Walletに追加する必要があります。たとえば、インターネットにアクセスできない場所にConnectorがインストールされている場合は、ライセンスを自分で追加する必要があります。 [購入済みライセンスをアカウントに追加する方法について説明します](#)。

アカウントの容量を表示します

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

購入したライセンスがデジタルウォレットに表示されない場合は、Cloud Managerにライセンスを追加して、容量をCloud Volumes ONTAP で使用できるように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

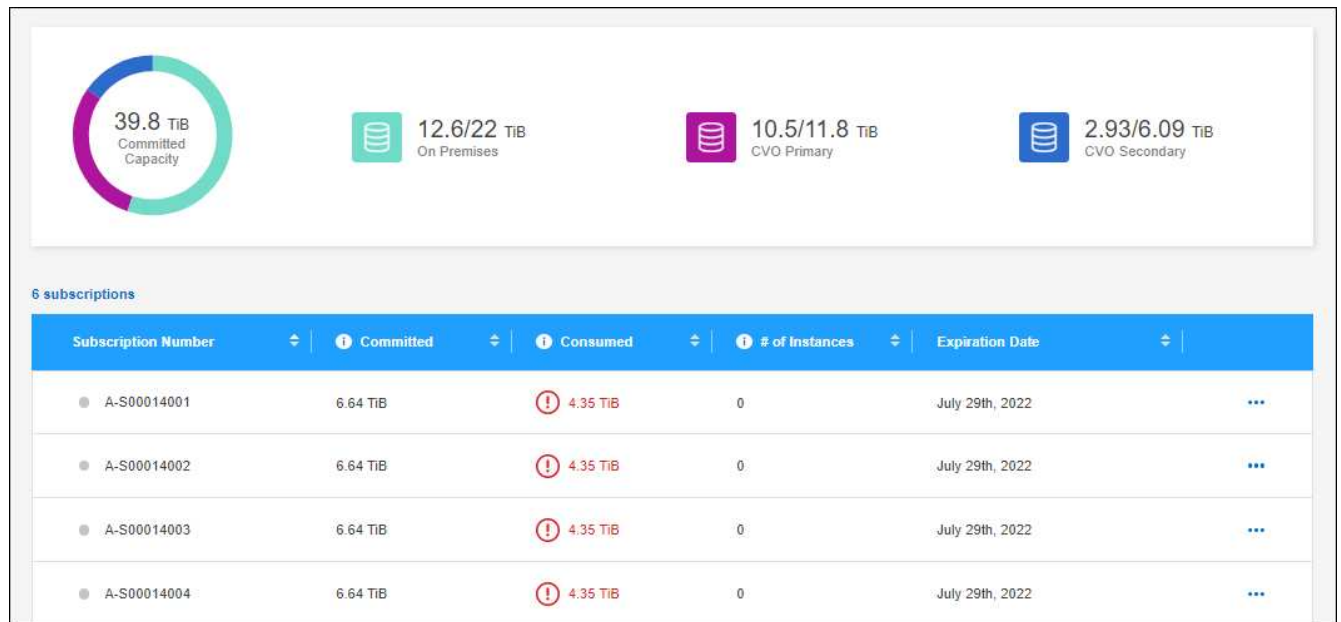
Cloud Manager で Keystone Flex Subscriptions を使用して管理する前に、ネットアップに連絡して、Keystone Flex Subscriptions で Cloud Manager ユーザアカウントを承認する必要があります。

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.

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。

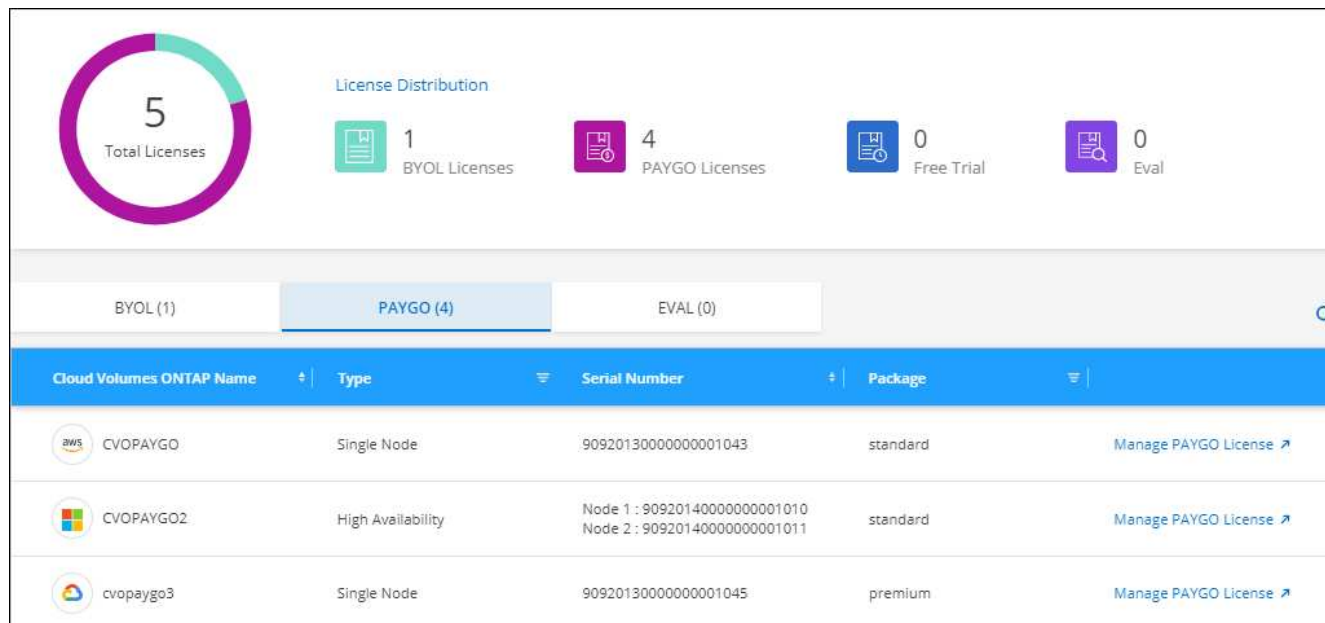
"Cloud Volumes ONTAP ライセンスの詳細については、こちらをご覧ください"。

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)		Search	Add Unassigned Licenses
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。

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。

- ° 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にのみ設定できます。CIFS サーバを作成したあとで設定することはできません。

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。

- a. * ディスクタイプ *：パフォーマンスのニーズとコストの要件に基づいて、ボリュームの基盤となるディスクタイプを選択します。

- ["Azure でのシステムのサイジング"](#)

4. * 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。

5. * 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。

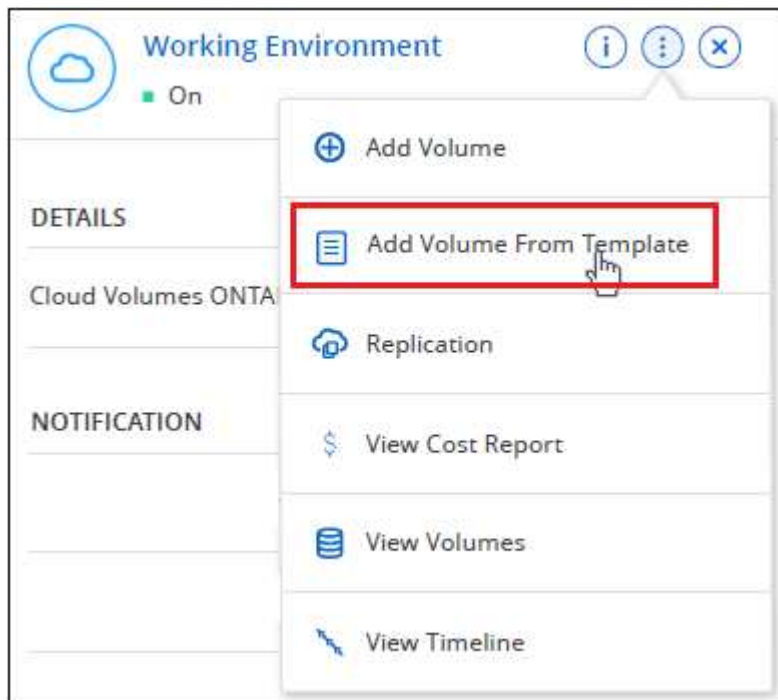
テンプレートを使用すると、ディスクタイプ、サイズ、プロトコル、スナップショットポリシー、クラウドプロバイダ、その他。パラメータがすでに事前定義されている場合は、次のボリュームパラメータに進みます。



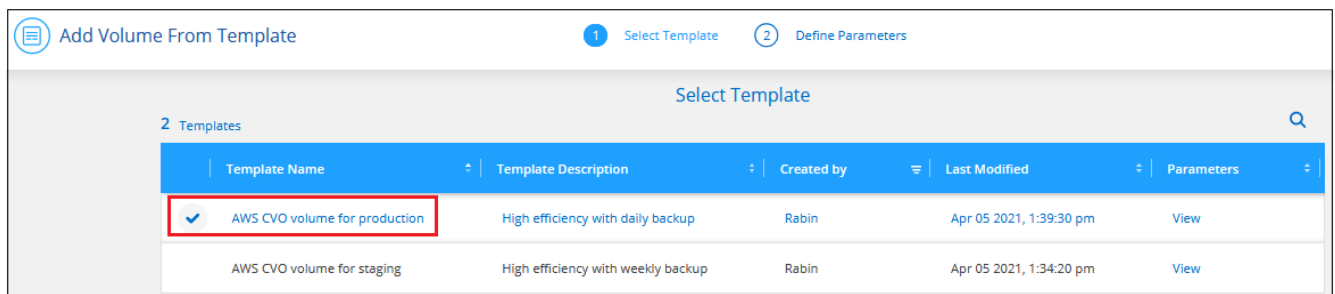
テンプレートを使用する場合にのみ、NFS ボリュームまたは CIFS ボリュームを作成できません。

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。

Define Parameters

Enter your values for the actions. Parameters that are locked by the template are not editable.

Actions

```

graph TD
    A[Create Volume in Cloud Volumes ONTAP (1)] --> B[Enable Cloud Backup (1)]
  
```

☐ Show read-only parameters

Details

Volume Name ?

Volume Name should start with "staging"

Volume Size (GB) ?

Minimum value is 160, Maximum value is 185

Protection

Snapshot Policy

Default X ▼

Usage Profile

☒ Storage Efficiency
 ☐ No Storage Efficiency

Disk Type

Disk Type

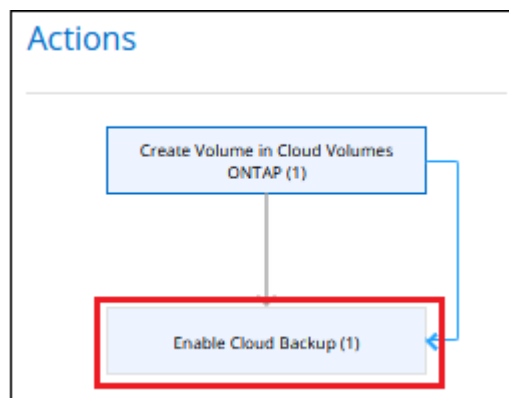
GP2 - General Purpose SSD X ▼



[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。

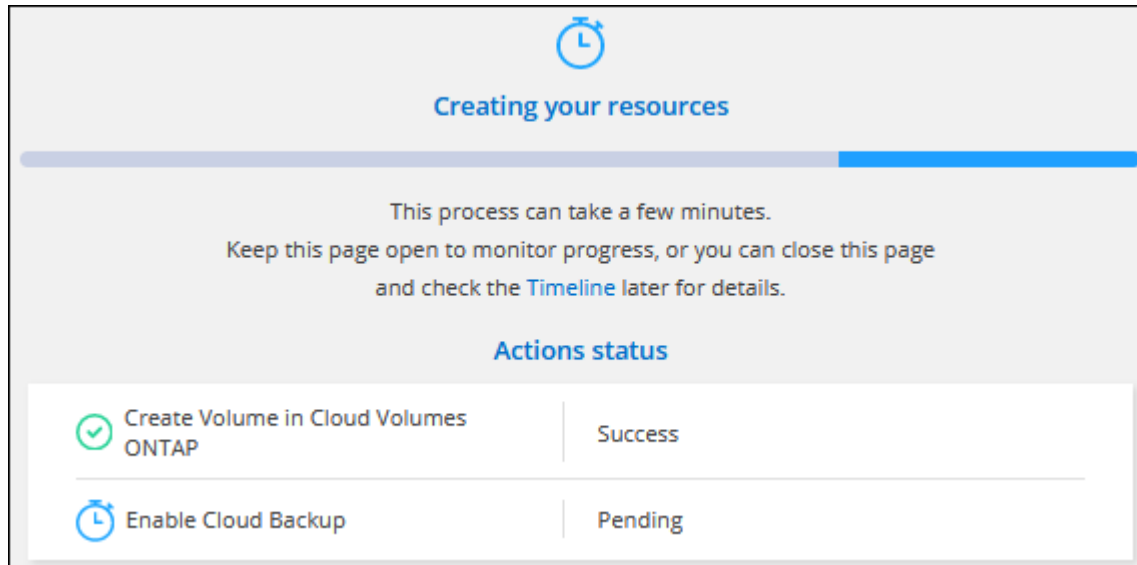
他のアクションがある場合は、左ペインのアクションをクリックして、完了する必要のあるパラメータを表示します。



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。



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。

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）	<div><div>a. ボリュームを選択し、* 編集 * をクリックします。</div><div>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></div> <div> 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。</div>
ボリュームのクローンを作成します	<div><div>a. ボリュームを選択し、* Clone * をクリックします。</div><div>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。</div></div> <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	<div><div>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。</div><div>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。</div></div>

タスク	アクション
オンデマンドで Snapshot コピーを作成します	<ol style="list-style-type: none"> ボリュームを選択し、 * Snapshot コピーの作成 * をクリックします。 必要に応じて名前を変更し、 * 作成 * をクリックします。
nfs mount コマンドを取得します	<ol style="list-style-type: none"> 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。 [* コピー (Copy)] をクリックします
iSCSI ボリュームのターゲット IQN を表示します	<ol style="list-style-type: none"> ボリュームを選択し、 * Target IQN * をクリックします。 [* コピー (Copy)] をクリックします "IQN を使用して、から LUN に接続します ホスト"。
基になるディスクタイプを変更します	<ol style="list-style-type: none"> 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。 ディスクタイプを選択し、 * Change * をクリックします。 <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>
階層化ポリシーを変更します	<ol style="list-style-type: none"> 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。 [* ポリシーの編集 *] をクリックします。 別のポリシーを選択し、 * 変更 * をクリックします。 <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	<ol style="list-style-type: none"> ボリュームを選択し、 * 削除 * をクリックします。 再度 * Delete * をクリックして確定します。

ボリュームのサイズを変更する

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

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

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

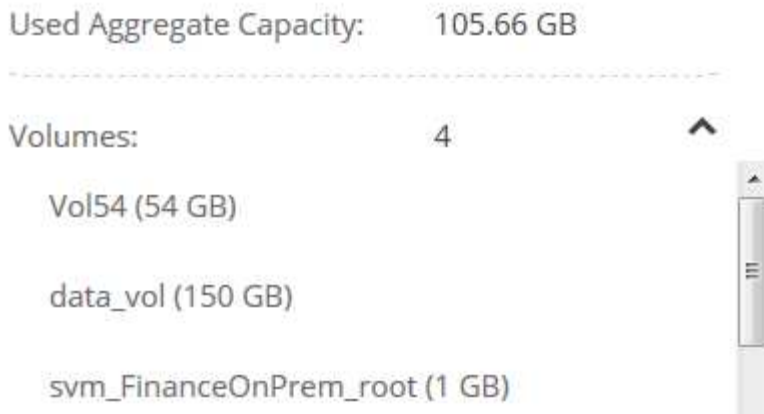
容量の問題を回避するためにボリュームの移動が必要で、Cloud Manager から推奨される処理が提示されない場合、移動が必要なボリュームと、そのボリュームを同じシステムの別のアグリゲートまたは別のシステムのどちらに移動すべきかを特定する必要があります。

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

9.4 リリース以前のアグリゲートでデータの階層化が有効になっている場合は、古い命名規則が使用されます。

- 暗号化設定がソースアグリゲートとデスティネーションアグリゲートで一致しないか、キーの変更を実行中です。
- 階層化ポリシーを変更するためにボリューム移動で `-tiering-policy _` オプションが指定されています。
- ボリューム移動で、`generate-destination-key_option` が指定されました。

使用頻度の低いデータを低コストのオブジェクトストレージに階層化

ホットデータ用の SSD または HDD の高パフォーマンス階層と、アクセス頻度の低いデータ用のオブジェクトストレージの大容量階層を組み合わせることで、Cloud Volumes ONTAP のストレージコストを削減できます。データ階層化は、FabricPool テクノロジ

によって実現されます。概要については、を参照してください ["データ階層化の概要"](#)。

データの階層化を設定するには、次の操作を実行する必要があります。

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。"](#)。

- 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。](#)

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に求められます。

- ["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。
- 大容量階層用のオブジェクトストア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

特定の構成や機能を使用する場合は、データの階層化を有効にすることができます。

Azure でのサポート

- Azureでは、次のデータ階層化がサポートされています。
 - シングルノードシステムの場合はバージョン9.4
 - HAペアではバージョン9.6
- 高パフォーマンス階層には、Premium SSD Managed Disks、Standard SSD Managed Disks、Standard HDD Managed Disksがあります。

機能の相互運用性

- 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 **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"**。

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 *

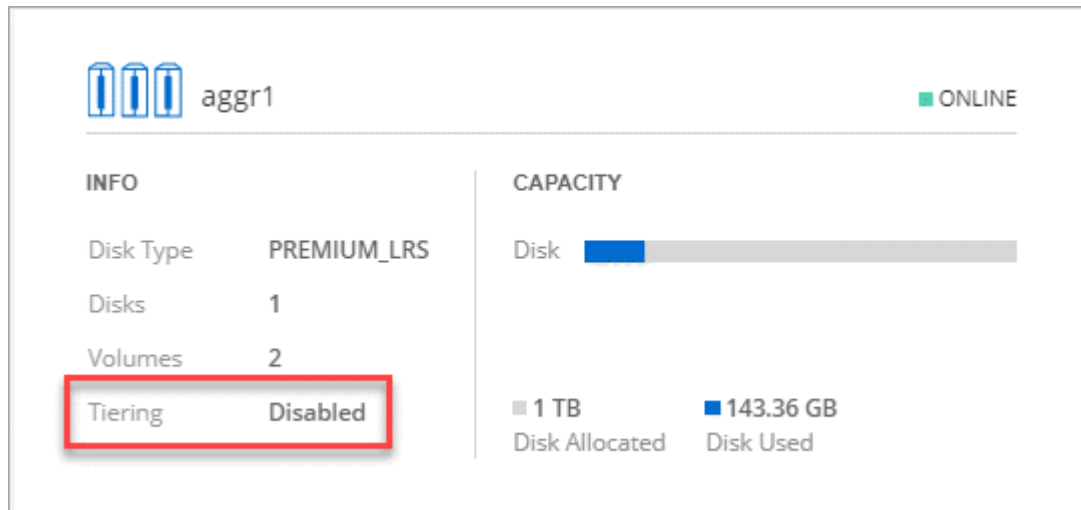
新しいボリュームでデータ階層化を有効にする場合、アグリゲートでデータ階層化を有効にする必要はありません。Cloud Manager では、階層化が有効になっている既存のアグリゲートにボリュームが作成されます。データ階層化が有効になっているアグリゲートがない場合は、ボリューム用の新しいアグリゲートが作成されます。

• * 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

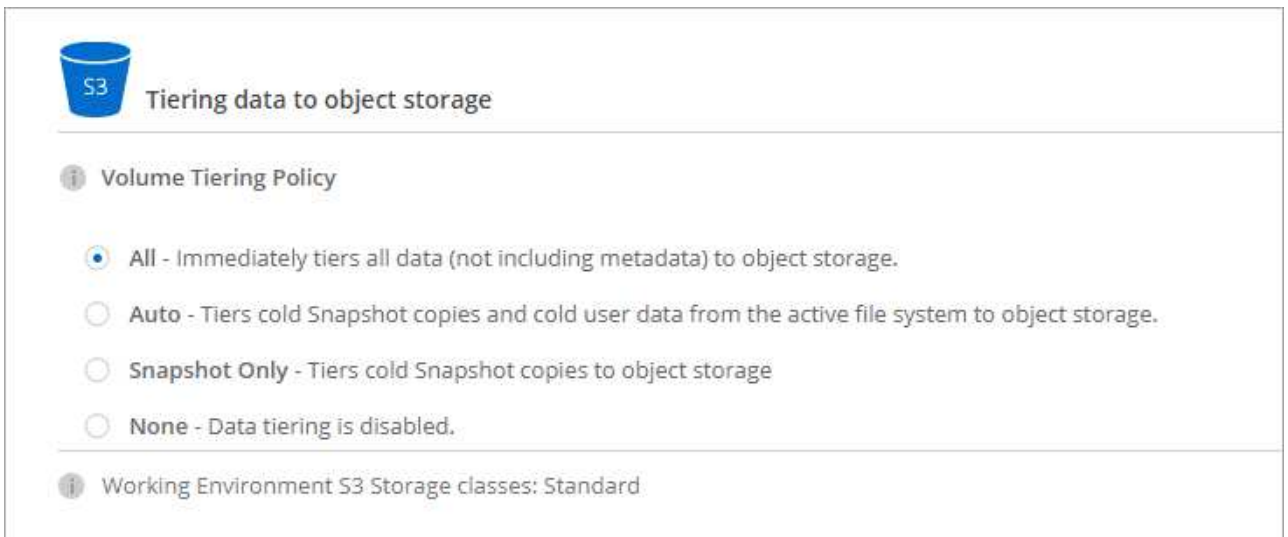
1. 作業環境で、新しいボリュームを作成するか、既存のボリュームの階層を変更します。

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。

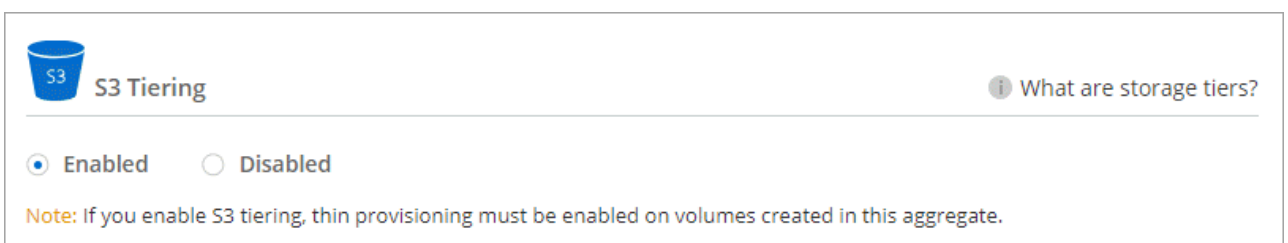
データ保護ボリュームのデータを階層化する

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

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。



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 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があります。

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、* 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><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></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

一部の構成では複数の Storage VM がサポートされます。にアクセスします ["Cloud Volumes ONTAP リリースノート"](#) 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

複数の **Storage VM** を使用できます

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) ⓘ

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:

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』"](#)

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

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

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

サポートされている **Storage VM** 数

9.9.0 リリース以降では、特定の Cloud Volumes ONTAP 構成で複数の Storage VM がサポートされます。にアクセスします ["Cloud Volumes ONTAP リリースノート"](#) 使用している Cloud Volumes ONTAP のバージョンでサポートされる Storage VM 数を確認してください。

他のすべての Cloud Volumes ONTAP 構成で、ディザスタリカバリに使用する 1 つのデータ提供用 Storage VM と 1 つのデスティネーション Storage VM がサポートされます。ソース Storage VM で停止が発生した場合は、デスティネーション Storage VM をデータアクセス用にアクティブ化できます。

Azure で IP アドレスを割り当てます

Storage VM を作成して LIF を割り当てる前に、Azure で IP アドレスを割り当てる必要があります。

シングルノードシステム

Storage VM を作成して LIF を割り当てる前に、Azure で IP アドレスを nic0 に割り当てる必要があります。必要な IP アドレスの数は、ストレージプロトコルによって異なります。

iSCSI

- iSCSI データ LIF アクセス用に 1 つの IP アドレス
- Storage VM （ SVM ） 管理 LIF のオプションの IP アドレスです

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

NFS

- NAS データ LIF へのアクセス用に 1 つの IP アドレス
- Storage VM （ SVM ） 管理 LIF のオプションの IP アドレスです

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

SMB

- NAS データ LIF へのアクセス用に 1 つの IP アドレス
- iSCSI LIF を介した DNS 通信と SMB 通信に使用する IP アドレス × 1

iSCSI LIF はフェイルオーバー時に移行されないため、この目的に使用されます。

- Storage VM （ SVM ） 管理 LIF のオプションの IP アドレスです

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

手順

1. Azure ポータルにログインし、 * 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。

- 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。

- SMB を使用している場合は、上記の手順を繰り返して、DNS 通信と SMB 通信用に追加の IP アドレスを作成します。
- SVM 管理 LIF を作成する場合は、上記の手順を繰り返して追加の IP アドレスを作成します。

作成したプライベート IP アドレスをコピーします。新しい Storage VM の LIF を作成するときに、これらの IP アドレスを指定する必要があります。

HA ペア

HA ペアに IP アドレスを割り当てる方法は、使用しているストレージプロトコルによって異なります。

iSCSI

Storage VM を作成して LIF を割り当てる前に、Azure で iSCSI IP アドレスを nic0 に割り当てる必要があります。iSCSI はフェイルオーバーに ALUA を使用するため、iSCSI の IPS はロードバランサではなく nic0 に割り当てられます。

次の IP アドレスを作成する必要があります。

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

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

手順

1. Azure ポータルにログインし、 * Virtual Machine * サービスを開きます。
2. ノード 1 の Cloud Volumes ONTAP VM の名前をクリックします。
3. [* ネットワーク] をクリックします。
4. nic0 のネットワークインターフェイスの名前をクリックします。
5. [* 設定] で、 [* IP 設定 *] をクリックします。
6. [追加 （ Add ）] をクリックします。
7. IP 設定の名前を入力し、 * Dynamic * を選択して、 * OK * をクリックします。
8. 作成した IP 設定の名前をクリックし、 * Assignment * を * Static * に変更して、 * Save * をクリックします。

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

9. ノード 2 で上記の手順を繰り返します。
10. SVM 管理 LIF を作成する場合は、ノード 1 で上記の手順を繰り返します。

NFS

NFS に使用する IP アドレスはロードバランサに割り当てられます。これにより、フェイルオーバー時に IP アドレスがもう一方のノードに移行できるようになります。

次の IP アドレスを作成する必要があります。

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

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

手順

1. Azure ポータルで、* ロードバランサ * サービスを開きます。
2. HA ペアのロードバランサの名前をクリックします。
3. データ LIF へのアクセスに使用するフロントエンド IP 設定をノード 1 から、データ LIF へのアクセスに使用するフロントエンド IP をノード 2 から、Storage VM (SVM) 管理 LIF のもう 1 つのオプションのフロントエンド IP に作成します。
 - a. [* 設定] で、[* フロントエンド IP 設定] をクリックします。
 - b. [追加 (Add)] をクリックします。
 - c. フロントエンド IP の名前を入力し、Cloud Volumes ONTAP HA ペアのサブネットを選択して、* 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。

Microsoft Azure

Search resources, services, and

[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

6. Cloud Volumes ONTAP のネットワークセキュリティグループルールで、ロードバランサが上記の手順 4 で作成したヘルスプローブの TCP プローブを送信できることを確認します。これはデフォルトで許可されています。

SMB

SMB データに使用する IP アドレスはロードバランサに割り当てられます。これにより、フェイルオーバー時に IP アドレスを別のノードに移行できるようになります。

次の IP アドレスを作成する必要があります。

- ノード 1 から NAS データ LIF にアクセスするための IP アドレス × 1
- ノード 2 からの NAS データ LIF アクセス用に 1 つの IP アドレス
- ノード 1 の iSCSI LIF の IP アドレス × 1
- ノード 2 の iSCSI LIF の IP アドレス × 1

iSCSI LIF は、DNS 通信と SMB 通信に必要です。iSCSI LIF はフェイルオーバー時に移行されないため、この目的に使用されます。

- Storage VM （SVM）管理 LIF のオプションの IP アドレスです

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

手順

1. Azure ポータルで、* ロードバランサ * サービスを開きます。
2. HA ペアのロードバランサの名前をクリックします。
3. 必要な数のフロントエンド IP 設定を作成します。
 - 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。

The screenshot shows the 'Add frontend IP address' page in the Microsoft Azure portal. The breadcrumb navigation is 'Home > Load balancers > azureha1011s3-rg-lb >'. The title is 'Add frontend IP address' with a three-dot menu icon. Below the title is the resource name 'azureha1011s3-rg-lb'. The form contains the following fields:

- Name ***: A text input field containing 'ip-for-svm2' with a green checkmark icon on the right.
- Virtual network**: A dropdown menu showing 'Default-Networking-vnet'.
- Subnet**: A dropdown menu showing 'default (172.19.2.0/24)' with a downward arrow icon on the right.
- Assignment**: Two radio buttons, 'Dynamic' (which is selected) and '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。

Microsoft Azure

Search resources, services, and

[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 ⓘ

dataAProbe (TCP:63002) ▼

Session persistence ⓘ

None ▼

Floating IP ⓘ

- 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。

作成したプライベート IP アドレスをコピーします。新しい Storage VM の LIF を作成するときに、これらの IP アドレスを指定する必要があります。

Storage VM と LIF を作成

Azure で IP アドレスを割り当てると、単一のノードシステムまたは HA ペアに新しい Storage VM を作成できます。

シングルノードシステム

シングルノードシステムで Storage VM と LIF を作成する方法は、使用しているストレージプロトコルによって異なります。

iSCSI

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a -address  
<iscsi-ip-address> -lif <lif-name> -home-node <name-of-node1> -data  
-protocol iscsi
```

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

NFS

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask  
-length <length> -home-node <name-of-node1> -status-admin up  
-failover-policy disabled -firewall-policy data -home-port e0a -auto  
-revert true -failover-group Default
```

3. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role  
data -data-protocol none -address <svm-mgmt-ip-address> -netmask  
-length <length> -home-node node1 -status-admin up -failover-policy  
system-defined -firewall-policy mgmt -home-port e0a -auto-revert  
false -failover-group Default
```

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

SMB

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. データ LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol cifs,nfs -address <nfs-ip-address> -netmask
-length <length> -home-node <name-of-node1> -status-admin up
-failover-policy disabled -firewall-policy data -home-port e0a -auto
-revert true -failover-group Default
```

3. DNS 通信と SMB 通信を提供するために必要な 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
```

4. オプション： Storage VM 管理 LIF を作成する

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node node1 -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert
false -failover-group Default
```

5. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

HA ペア

HA ペアで Storage VM と LIF を作成する方法は、使用しているストレージプロトコルによって異なります。

iSCSI

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. データ LIF を作成します。

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

```
network interface create -vserver <svm-name> -home-port e0a  
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-  
node1> -data-protocol iscsi
```

- b. 次のコマンドを使用して、ノード 2 に iSCSI LIF を作成します。

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

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

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

NFS

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. データ LIF を作成します。

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

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-ip-address>  
-netmask-length <length> -home-node <name-of-node1> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe1>
```

- b. 次のコマンドを使用して、ノード 2 に NAS LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name>  
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>  
-netmask-length <length> -home-node <name-of-node2> -status-admin  
up -failover-policy system-defined -firewall-policy data -home  
-port e0a -auto-revert true -failover-group Default -probe-port  
<port-number-for-azure-health-probe2>
```

3. 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>
```

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

4. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

SMB

新しい Storage VM と必要な LIF を作成するには、次の手順を実行します。

手順

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

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

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

2. NAS データ LIF を作成します。

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

```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs--ip-address>
-netmask-length <length> -home-node <name-of-nodel> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe1>
```

- b. 次のコマンドを使用して、ノード 2 に NAS LIF を作成します。


```
network interface create -vserver <svm-name> -lif <lif-name>
-role data -data-protocol cifs,nfs -address <nfs-cifs-ip-address>
-netmask-length <length> -home-node <name-of-node2> -status-admin
up -failover-policy system-defined -firewall-policy data -home
-port e0a -auto-revert true -failover-group Default -probe-port
<port-number-for-azure-health-probe2>
```

3. DNS 通信と SMB 通信を提供する iSCSI LIF を作成します。

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

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
node1> -data-protocol iscsi
```

- b. 次のコマンドを使用して、ノード 2 に iSCSI LIF を作成します。

```
network interface create -vserver <svm-name> -home-port e0a
-address <iscsi-ip-address> -lif <lif-name> -home-node <name-of-
node2> -data-protocol iscsi
```

4. オプション：ノード 1 に Storage VM 管理 LIF を作成します。

```
network interface create -vserver <svm-name> -lif <lif-name> -role
data -data-protocol none -address <svm-mgmt-ip-address> -netmask
-length <length> -home-node node1 -status-admin up -failover-policy
system-defined -firewall-policy mgmt -home-port e0a -auto-revert
false -failover-group Default -probe-port <port-number-for-azure-
health-probe3>
```

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

5. Storage VM に 1 つ以上のアグリゲートを割り当てます。

```
vserver add-aggregates -vserver svm_2 -aggregates aggr1,aggr2
```

この手順は、Storage VM にボリュームを作成する前に、新しい Storage VM が少なくとも 1 つのアグリゲートにアクセスする必要があるためです。

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。

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
 - "[Azure キーボールド \(AKV\)](#)"

Azure Key Vaultを使用してキーを管理します

を使用できます "[Azure キーボールド \(AKV\)](#)" Azure で導入されたアプリケーションで ONTAP 暗号化キーを保護するため。

AKV は保護に使用できます "[NetApp Volume Encryption \(NVE\) キー](#)" データ SVM の場合のみ。

AKVを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

AKVを使用する場合、デフォルトではクラウドキー管理エンドポイントとの通信にデータSVM LIFが使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス (login.microsoftonline.com) との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

前提条件

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption (VE) ライセンスがインストールされている (ネットアップサポートに登録されている各Cloud Volumes ONTAP システムにNetApp Volume Encryptionライセンスが自動的にインストールされます)。
- Multi-tenant Encryption Key Management (MTEKM) ライセンスがインストールされています
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなAzureサブスクリプション

制限

- AKVはデータSVM上でのみ設定できます

設定プロセス

AzureにCloud Volumes ONTAP 構成を登録する方法と、Azure Key Vaultとキーを作成する方法を概説しています。これらの手順をすでに完了している場合は、特に、で正しい設定を行っていることを確認してください [Azureキーバックアップを作成します](#)をクリックし、に進みます [Cloud Volumes ONTAP 構成](#)。* [Azureアプリケーション登録](#)* [Azureクライアントシークレットを作成する](#)* [Azureキーバックアップを作成します](#)* [暗号化キーを作成します](#)* [Azure Active Directoryエンドポイントの作成 \(HAのみ\)](#) * [Cloud Volumes ONTAP 構成](#)

Azureアプリケーション登録

1. Cloud Volumes ONTAP からAzure Key Vaultへのアクセスに使用するAzureサブスクリプションにアプリケーションを登録しておく必要があります。Azureポータルで、アプリケーション登録を選択します。
2. 新規登録を選択します。
3. アプリケーションの名前を指定し、サポートされているアプリケーションタイプを選択します。デフォルトの単一テナントでAzure Key Vaultの使用量が十分に設定されていること。[登録]を選択します。
4. Azureの概要ウィンドウで、登録したアプリケーションを選択します。アプリケーション (クライアント) IDおよびディレクトリ (テナント) IDを安全な場所にコピーします。これらの情報は、後で登録プロセスで必要になります。

Azureクライアントシークレットを作成する

1. Cloud Volumes ONTAP アプリケーション用のAzureポータルで、[** Certificates & secrets]ペインを選択します。
2. [新しいクライアントシークレット]クライアントシークレットに意味のある名前を入力してください。ネットアップでは24カ月の有効期限を推奨していますが、クラウドガバナンスポリシーによっては、別の設定が必要になる場合があります。
3. クライアントシークレットを保存するには、[追加]を選択します。シークレットの値**をすぐにコピーして、将来の設定のために安全な場所に保管してください。ページから移動してもシークレット値は表示されません。

Azureキーバックアップを作成します

1. 既存のAzure Key Vaultを使用している場合は、Cloud Volumes ONTAP 構成に接続できますが、アクセスポリシーをこのプロセスの設定に合わせる必要があります。
2. Azureポータルで、[** Key Vaults (キーボルト)]セクションに移動します。
3. [作成]を選択します。リソースグループ、地域、価格階層などの必要な情報を入力し、削除されたボールドを保持する日数と、ページ保護が有効かどうかを選択します。この構成ではデフォルトで十分ですが、クラウドガバナンスポリシーごとに異なる設定が必要になる場合があります。
4. アクセスポリシーを選択するには、**Next**を選択してください。
5. ボリューム暗号化オプションとして[**Azure Disk Encryption**]を選択し、権限モデルとして[Vault access policy]を選択します。
6. [アクセスポリシーの追加] を選択します。
7. [テンプレートから構成する (オプション)]フィールドの横にあるキャレットを選択します。次に、[**Key**]、[**Secret**]、[**Certification Management**]を選択します。
8. 各ドロップダウンメニュー(キー、シークレット、証明書)を選択し、メニューリストの一番上にある[**All**]を選択して、使用可能なすべてのアクセス許可を選択します。次の作業を完了しておきます
 - キー権限:19が選択されています
 - シークレット権限:8が選択されています
 - 証明書のアクセス許可:16が選択されています
9. アクセスポリシーを作成するには、[**追加]を選択します。
10. **Next**を選択して、**Networking**オプションに進みます。
11. 適切なネットワークアクセス方法を選択するか、すべてのネットワークおよびレビュー+作成を選択して、キーボルトを作成します。(ネットワークアクセス方法は、ガバナンスポリシーまたは企業のクラウドセキュリティチームによって規定されている場合があります)。
12. キーボルトURIを記録します。作成したキーボルトで、概要メニューに移動し、右側のカラムから**Vault URI** をコピーします。これは、あとの手順で必要になります。

暗号化キーを作成します

1. Cloud Volumes ONTAP 用に作成したキー・ボルトのメニューで、[**Keys** (キー**)]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。
 - 暗号化キー名
 - キータイプ:rsa
 - RSAキーのサイズ:2048
 - Enabled:はい
5. [****Create**]を選択して、暗号キーを作成します。
6. [**Keys** (キー**)]メニューに戻り、作成したキーを選択します。
7. キーのプロパティを表示するには、[**Current version** (現在のバージョン**)]でキーIDを選択します。

8. [**Key Identifier** (キー識別子**)]フィールドを探します。URIを16進数の文字列以外の値にコピーします。

Azure Active Directoryエンドポイントの作成 (HAのみ)

1. このプロセスは、HA Cloud Volumes ONTAP 作業環境用にAzure Key Vaultを設定する場合にのみ必要です。
2. Azureポータルで、**Virtual Networks**に移動します。
3. Cloud Volumes ONTAP 作業環境を展開した仮想ネットワークを選択し、ページの左側にある **Subnets** メニューを選択します。
4. Cloud Volumes ONTAP 環境のサブネット名をリストから選択します。
5. [サービスエンドポイント]見出しに移動します。ドロップダウンメニューで、リストから**Microsoft.AzureActiveDirectory** を選択します。
6. 保存を選択して、設定を取得します。

Cloud Volumes ONTAP 構成

1. 優先SSHクライアントを使用してクラスタ管理LIFに接続します。
2. ONTAP でadvanced権限モードに切り替えます。「set advanced-con off」
3. 目的のデータSVMを特定し、そのDNS設定を確認します。「vserver services name-service dns show
 - a. 目的のデータSVMのDNSエントリが存在し、そのエントリにAzure DNSのエントリが含まれている場合は、対処は必要ありません。表示されない場合は、Azure DNS、プライベートDNS、またはオンプレミスサーバを指すデータSVMのDNSサーバエントリを追加します。これは、クラスタ管理SVMのエントリと一致している必要があります。vserver services name-service dns create -vserver _svm_name -domains_domain_name-servers _ip_address _
 - b. データSVM用にDNSサービスが作成されたことを確認します。vserver services name-service dns show
4. アプリケーションの登録後に保存されたクライアントIDとテナントIDを使用してAzure Key Vaultを有効にします。「security key-manager external Azure enable -vserver svm_name _-client -id_caz_client_client_ID_tenant_ID_name_azure-name_aze_key_name_-key_key_id_azure_key_id_id_`
5. キー管理ツールの構成を確認します。「security key-manager external Azure show
6. キー管理ツールのステータスを確認します。「security key-manager external Azure check」出力は次のようになります。

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekmip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

「SERVICE_Reachability」ステータスが「OK」でない場合、SVMは必要なすべての接続および権限を使用してAzure Key Vaultサービスに到達できません。初期構成で'kms_wrapped_key_status'は'unknown'を報告します最初のボリュームが暗号化されるとステータスはOKに変わります

7. オプション：テストボリュームを作成してAKVの機能を確認します。vol create -vserver_svm_name_-volume_name_-aggregate_aggr_size_state online -policy default'

正しく設定されていれば、Cloud Volumes ONTAP でボリュームが自動的に作成され、ボリューム暗号化が有効になります。

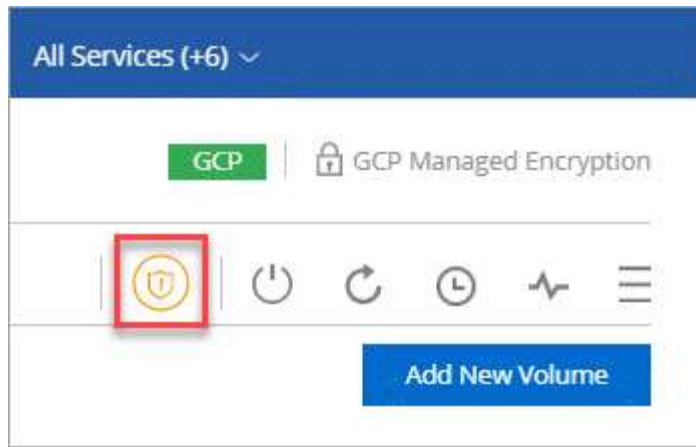
1. ボリュームが正しく作成および暗号化されたことを確認します。その場合、「-is-encrypted」パラメータは「true」と表示されます。vol show -vserver_svm_name_-fields is-cencryptedです

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に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

Azure Key Vaultを使用してキーを管理します

を使用できます **"Azure キーボールド（AKV）"** Azureで導入されたアプリケーションでONTAP 暗号化キーを保護するため。

AKVは保護に使用できます **"NetApp Volume Encryption（NVE）キー"** データSVMの場合のみ。

AKVを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にできます。

AKVを使用する場合、デフォルトではクラウドキー管理エンドポイントとの通信にデータSVM LIFが使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（login.microsoftonline.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、クラスタでキー管理サービスが適切に利用されません。

前提条件

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption（VE）ライセンスがインストールされている（ネットアップサポートに登録されている各Cloud Volumes ONTAP システムにNetApp Volume Encryptionライセンスが自動的にインストールされます）。
- Multi-tenant Encryption Key Management（MTEKM）ライセンスがインストールされています
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなAzureサブスクリプション

制限

- AKVはデータSVM上でのみ設定できます

設定プロセス

AzureにCloud Volumes ONTAP 構成を登録する方法と、Azure Key Vaultとキーを作成する方法を概説しています。これらの手順をすでに完了している場合は、特に、で正しい設定を行っていることを確認してください [Azureキーバックアップを作成します](#)をクリックし、に進みます [Cloud Volumes ONTAP 構成](#)。* [Azureアプリケーション登録](#)* [Azureクライアントシークレットを作成する](#)* [Azureキーバックアップを作成します](#)* [暗号化キーを作成します](#)* [Azure Active Directoryエンドポイントの作成（HAのみ）](#)* [Cloud Volumes ONTAP 構成](#)

Azureアプリケーション登録

1. Cloud Volumes ONTAP からAzure Key Vaultへのアクセスに使用するAzureサブスクリプションにアプリケーションを登録しておく必要があります。Azureポータルで、アプリケーション登録を選択します。
2. 新規登録を選択します。
3. アプリケーションの名前を指定し、サポートされているアプリケーションタイプを選択します。デフォルトの単一テナントでAzure Key Vaultの使用量が十分に設定されていること。[登録]を選択します。
4. Azureの概要ウィンドウで、登録したアプリケーションを選択します。アプリケーション（クライアント）IDおよびディレクトリ（テナント）IDを安全な場所にコピーします。これらの情報は、後で登録プロセスで必要になります。

Azureクライアントシークレットを作成する

1. Cloud Volumes ONTAP アプリケーション用のAzureポータルで、[** Certificates & secrets]ペインを選択します。
2. [新しいクライアントシークレット]クライアントシークレットに意味のある名前を入力してください。ネットアップでは24カ月の有効期限を推奨していますが、クラウドガバナンスポリシーによっては、別の設定が必要になる場合があります。
3. クライアントシークレットを保存するには、[追加]を選択します。シークレットの値**をすぐにコピーして、将来の設定のために安全な場所に保管してください。ページから移動してもシークレット値は表示されません。

Azureキーバックアップを作成します

1. 既存のAzure Key Vaultを使用している場合は、Cloud Volumes ONTAP 構成に接続できますが、アクセスポリシーをこのプロセスの設定に合わせる必要があります。
2. Azureポータルで、[** Key Vaults（キーボルト）]セクションに移動します。
3. [作成]を選択します。リソースグループ、地域、価格階層などの必要な情報を入力し、削除されたボールドを保持する日数と、パージ保護が有効かどうかを選択します。この構成ではデフォルトで十分ですが、クラウドガバナンスポリシーごとに異なる設定が必要になる場合があります。
4. アクセスポリシーを選択するには、**Next**を選択してください。
5. ボリューム暗号化オプションとして[Azure Disk Encryption]を選択し、権限モデルとして[Vault access policy]を選択します。
6. [アクセスポリシーの追加] を選択します。
7. [テンプレートから構成する（オプション）]フィールドの横にあるキャレットを選択します。次に、[Key]、[Secret]、[Certification Management]を選択します。
8. 各ドロップダウンメニュー(キー、シークレット、証明書)を選択し、メニューリストの一番上にある[All]を選択して、使用可能なすべてのアクセス許可を選択します。次の作業を完了しておきます
 - キー権限:19が選択されています
 - シークレット権限:8が選択されています
 - 証明書のアクセス許可:16が選択されています
9. アクセスポリシーを作成するには、[**追加]を選択します。
10. **Next**を選択して、**Networking**オプションに進みます。
11. 適切なネットワークアクセス方法を選択するか、すべてのネットワークおよびレビュー+作成を選択して、キーボルトを作成します。（ネットワークアクセス方法は、ガバナンスポリシーまたは企業のクラウドセキュリティチームによって規定されている場合があります）。

12. キーボルトURIを記録します。作成したキーボルトで、概要メニューに移動し、右側のコラムから**Vault URI** をコピーします。これは、あとの手順で必要になります。

暗号化キーを作成します

1. Cloud Volumes ONTAP 用に作成したキー・ボルトのメニューで、[**Keys** (キー**)]オプションに移動します。
2. [生成/インポート]を選択して、新しいキーを作成します。
3. デフォルトのオプションは **Generate** のままにしておきます。
4. 次の情報を入力します。
 - 暗号化キー名
 - キータイプ：rsa
 - RSAキーのサイズ：2048
 - Enabled：はい
5. [****Create**]を選択して、暗号キーを作成します。
6. [**Keys** (キー**)]メニューに戻り、作成したキーを選択します。
7. キーのプロパティを表示するには、[**Current version** (現在のバージョン**)]でキーIDを選択します。
8. [**Key Identifier** (キー識別子**)]フィールドを探します。URIを16進数の文字列以外の値にコピーします。

Azure Active Directoryエンドポイントの作成 (HAのみ)

1. このプロセスは、HA Cloud Volumes ONTAP 作業環境用にAzure Key Vaultを設定する場合にのみ必要です。
2. Azureポータルで、**Virtual Networks**に移動します。
3. Cloud Volumes ONTAP 作業環境を展開した仮想ネットワークを選択し、ページの左側にある **Subnets** メニューを選択します。
4. Cloud Volumes ONTAP 環境のサブネット名をリストから選択します。
5. [サービスエンドポイント]見出しに移動します。ドロップダウンメニューで、リストから**Microsoft.AzureActiveDirectory** を選択します。
6. 保存を選択して、設定を取得します。

Cloud Volumes ONTAP 構成

1. 優先SSHクライアントを使用してクラスタ管理LIFに接続します。
2. ONTAP でadvanced権限モードに切り替えます。「set advanced-con off」
3. 目的のデータSVMを特定し、そのDNS設定を確認します。「vserver services name-service dns show」
 - a. 目的のデータSVMのDNSエントリが存在し、そのエントリにAzure DNSのエントリが含まれている場合は、対処は必要ありません。表示されない場合は、Azure DNS、プライベートDNS、またはオンプレミスサーバを指すデータSVMのDNSサーバエントリを追加します。これは、クラスタ管理SVMのエントリと一致している必要があります。vserver services name-service dns create -vserver _svm_name -domains _domain_name-servers _ip_address _'
 - b. データSVM用にDNSサービスが作成されたことを確認します。vserver services name-service dns show

4. アプリケーションの登録後に保存されたクライアントIDとテナントIDを使用してAzure Key Vaultを有効にします。「security key-manager external Azure enable -vserver svm_name _-client-id_caz_client_client_ID_tenant_ID_name_azure-name_aze_key_name_-key_key_id_azure_key_id_id_」
5. キー管理ツールの構成を確認します。「security key-manager external Azure show」
6. キー管理ツールのステータスを確認します。「security key-manager external Azure check」 出力は次のようになります。

```
::*> security key-manager external azure check

Vserver: data_svm_name
Node: akvlab01-01

Category: service_reachability
Status: OK

Category: ekmip_server
Status: OK

Category: kms_wrapped_key_status
Status: UNKNOWN
Details: No volumes created yet for the vserver. Wrapped KEK status
will be available after creating encrypted volumes.

3 entries were displayed.
```

「SERVICE_Reachability」ステータスが「OK」でない場合、SVMは必要なすべての接続および権限を使用してAzure Key Vaultサービスに到達できません。初期構成で'kms_wrapped_key_status'は'unknown'を報告します最初のボリュームが暗号化されるとステータスはOKに変わります

7. オプション：テストボリュームを作成してAKVの機能を確認します。vol create -vserver svm_name _-volume_name_-aggregate_aggr_size_state online -policy default'

正しく設定されていれば、Cloud Volumes ONTAP でボリュームが自動的に作成され、ボリューム暗号化が有効になります。

1. ボリュームが正しく作成および暗号化されたことを確認します。その場合、「-is-encrypted」パラメータは「true」と表示されます。vol show -vserver svm_name_-fields is-cencryptedです

GoogleのCloud Key Management Serviceを使用してキーを管理します

を使用できます ["Google Cloud Platform のキー管理サービス（Cloud KMS）"](#) Google Cloud Platform導入アプリケーションでONTAP 暗号化キーを保護します。

Cloud KMSを使用したキー管理は、CLIまたはONTAP REST APIを使用して有効にすることができます。

Cloud KMSを使用する際は、デフォルトでデータSVM LIFがクラウドキー管理エンドポイントとの通信に使用されることに注意してください。ノード管理ネットワークは、クラウドプロバイダの認証サービス（oauth2.googleapis.com）との通信に使用されます。クラスタネットワークが正しく設定されていないと、

クラスタでキー管理サービスが適切に利用されません。

前提条件

- Cloud Volumes ONTAP でバージョン9.10.1以降が実行されている必要があります
- Volume Encryption （ VE ） ライセンスがインストールされている
- Multi-tenant Encryption Key Management （ MTEKM ） ライセンスがインストールされています
- クラスタ管理者またはSVMの管理者である必要があります
- アクティブなGoogle Cloud Platformサブスクリプション

制限

- クラウドKMSはデータSVMでのみ設定できます

設定

Google Cloud

1. Google Cloud環境では、["対称GCPキーリングとキーを作成します"](#)。
2. Cloud Volumes ONTAP サービスアカウント用のカスタムロールを作成します。

```
gcloud iam roles create kmsCustomRole
  --project=<project_id>
  --title=<kms_custom_role_name>
  --description=<custom_role_description>

--permissions=cloudkms.cryptoKeyVersions.get,cloudkms.cryptoKeyVersions.
list,cloudkms.cryptoKeyVersions.useToDecrypt,cloudkms.cryptoKeyVersions.
useToEncrypt,cloudkms.cryptoKeys.get,cloudkms.keyRings.get,cloudkms.loc
ations.get,cloudkms.locations.list,resourceManager.projects.get
  --stage=GA
```

3. カスタムロールをCloud KMSキーとCloud Volumes ONTAP サービスアカウントに割り当てま
す。「gcloud kms keys add -iam-policy binding_key_name_--
keyring_key_ring_name — location_key_location _ - member serviceAccount
: _service_account_Name — role project_id_id_roles/custommkskmsk`key
4. サービスアカウントのJSONキーをダウンロードします。「gcloud iam service-accounts keys create key-
file --iam-account=sa-name@project-id.iam.gserviceaccount.com

Cloud Volumes ONTAP

1. 優先SSHクライアントを使用してクラスタ管理LIFに接続します。
2. advanced権限レベルに切り替えます:'set -privilege advanced
3. データSVM用のDNSを作成'dns create -domains C.<プロジェクト>.internal -name
-servers_server_address_-vserver_svm_name _
4. CMEKエントリを作成します:'security key-manager external GCP enable -vserver_svm_name_project
-id_project_-key-ring-name_key_ring_name_-key-ring-location_key_ring_location_-key
-name_key_name_`

5. プロンプトが表示されたら、GCPアカウントのJSONキーを入力します。
6. 有効なプロセスが成功したことを確認します。「security key-manager external GCP check -vserver _svm_name _」
7. オプション：暗号化「vol create _volume_name」をテストするボリュームを作成します。-aggregate -aggregate_aggregate_aggregate—vserver vserver_name _size 10Gです

トラブルシューティングを行う

トラブルシューティングが必要な場合は、上記の最後の2つの手順でREST APIのrawログをテールできます。「set d」。「systemshell -node _node」 コマンドtail -f /mroot/etc/log/mlog/kmip2_client.log

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
9.10.1	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0

現在のバージョン	に直接アップグレードできるバージョン
9.9.0	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

また、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. 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。



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。

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. ストレージ > アグリゲートとディスク > アグリゲート * をクリックします。
 - b. アグリゲートを選択し、* その他の操作 > ステータス > オンライン * をクリックします。

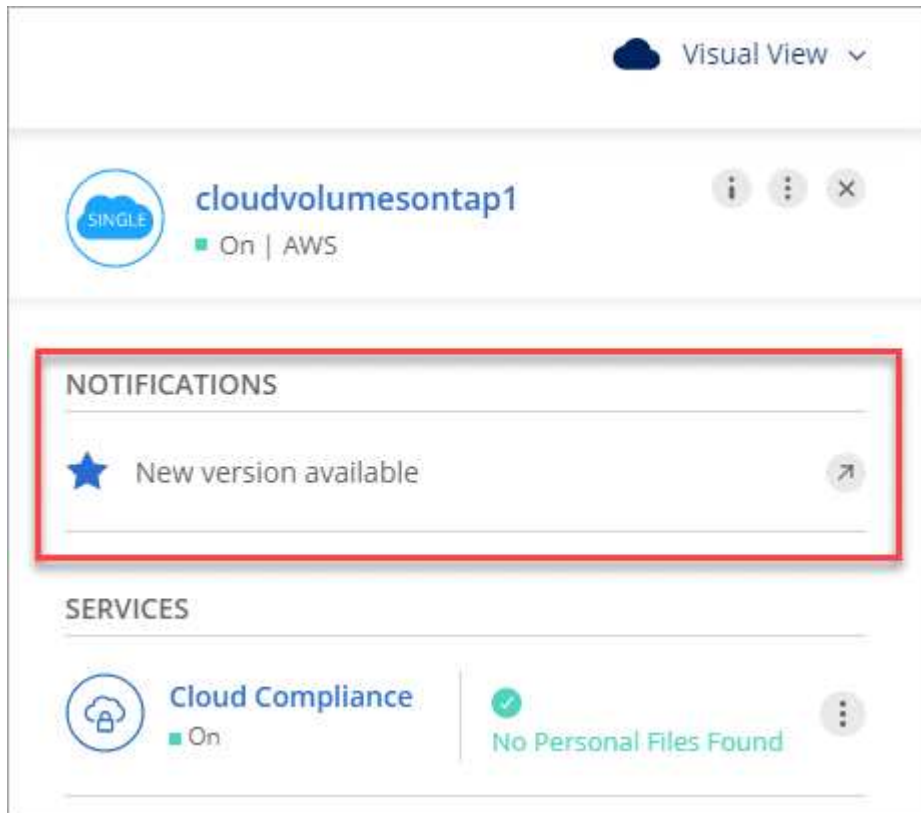
Cloud Volumes ONTAP をアップグレードします

新しいバージョンがアップグレード可能になると、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。



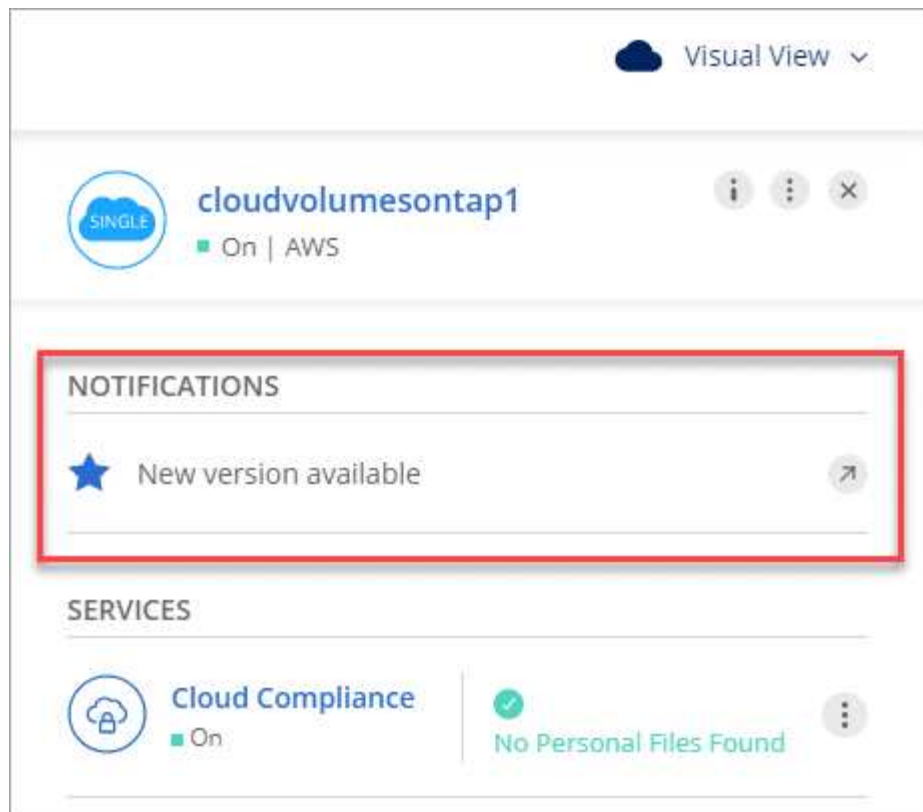
この通知からアップグレードプロセスを開始できます。アップグレードプロセスを自動化するには、S3 バケットからソフトウェアイメージを取得し、イメージをインストールしてから、システムを再起動します。

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。

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"](#)。



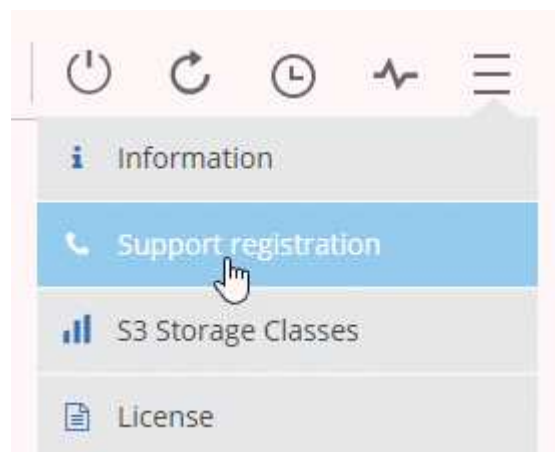
サポートに登録されていないシステムにも、新しいバージョンが利用可能になったときに Cloud Manager に表示されるソフトウェア更新通知が送信されます。ただし、ソフトウェアをアップグレードする前に、システムを登録する必要があります。

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. キャンバスページで、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

1. 作業環境で、時計アイコンをクリックします。



2. シャットダウンスケジュールを指定します。

- 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)

3. [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

- 作業環境で、* 電源オフ * アイコンをクリックします。



- 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。
- [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"](#)。

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. 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

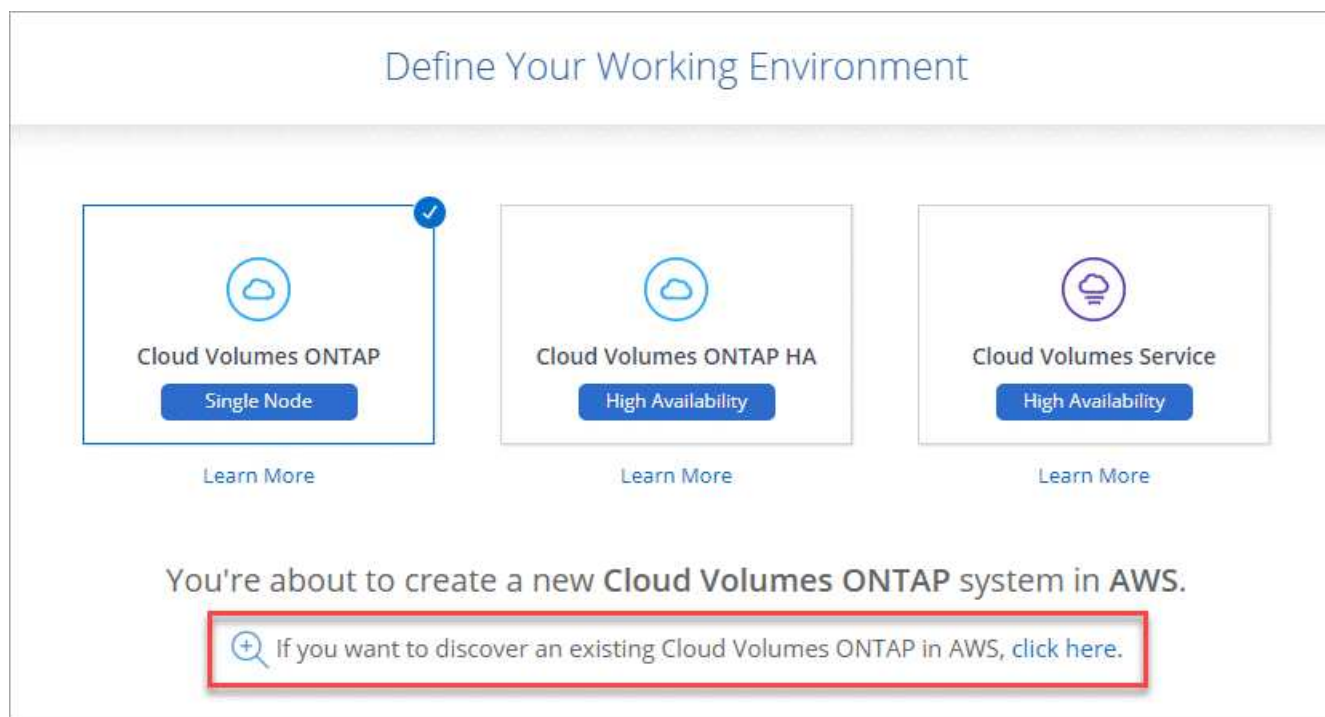
Cloud Manager に既存の **Cloud Volumes ONTAP** システムを追加

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

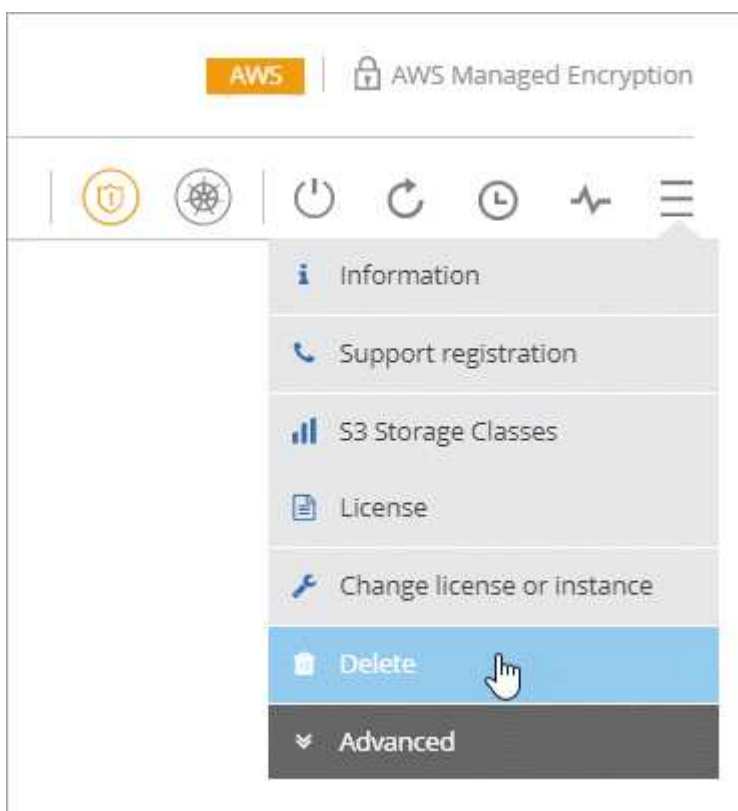
手順

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。

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。

手順

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、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。

System Manager または CLI を使用する

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。

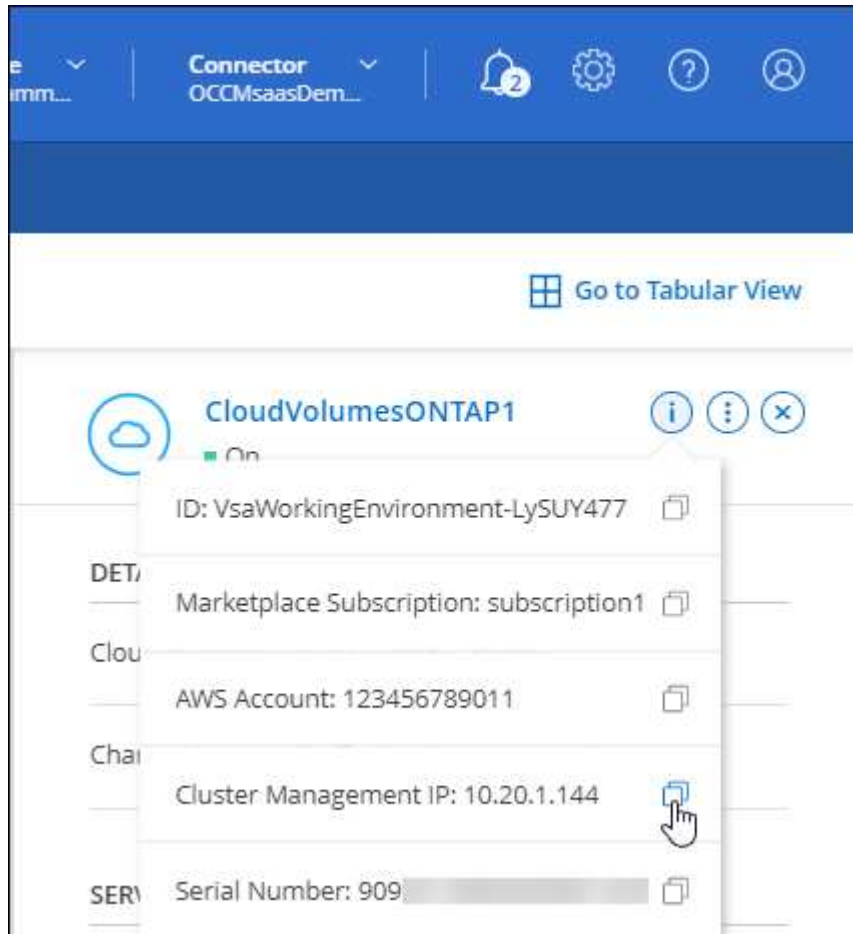
System Manager に接続しています

一部の Cloud Volumes ONTAP タスクを System Manager から実行する必要があることがあります。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。

手順

1. キャンバスから Cloud Volumes ONTAP 作業環境を選択します。
2. 右側のペインで、情報アイコンをクリックし、クラスタ管理 IP をコピーします。



3. Cloud Volumes ONTAP へのネットワーク接続が確立されたマシンで Web ブラウザを開き、IP アドレスを入力します。
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、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

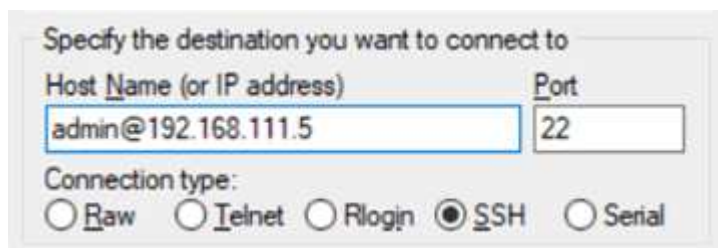
る場合などです。

手順

1. Cloud Manager で、クラスタ管理インターフェイスの IP アドレスを特定します。
 - a. 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。



Specify the destination you want to connect to

Host Name (or IP address)	Port
admin@192.168.111.5	22

Connection type:

☐ Raw ☐ Iinet ☐ Rlogin ☒ SSH ☐ Serial

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。

- ["Azure ネットワークの要件"](#)

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](#)"。

概念

Cloud Volumes ONTAP ライセンス

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

ライセンスの概要

新規のお客様は、次のライセンスオプションを利用できます。

フリーミアムのサービス

ライセンスや契約を購入することなく、プロビジョニングされた容量を最大 500GiB まで無料で利用できます。限定的なサポートが含まれます。

Essentials パッケージ

さまざまな構成で Cloud Volumes ONTAP の容量に基づいて料金が発生します。

プロフェッショナルパッケージ

Cloud Volumes ONTAP 構成の種類に関係なく、容量ごとに料金が発生Cloud Backup でバックアップを無制限に実行できます。

Keystone Flex サブスクリプション

ニーズに合わせて拡張できるサブスクリプションベースのサービス。HA ペア向けのシームレスなハイブリッドクラウドエクスペリエンスを提供します。

以前のノード単位のライセンスモデルは、ライセンスを購入済みの既存のお客様や、アクティブな Marketplace サブスクリプションを所有しているお客様には引き続き提供されます。

以降のセクションでは、これらの各オプションについて詳しく説明します。

フリーミアムのサービス

Cloud Volumes ONTAP のすべての機能をネットアップから無償で提供（クラウドプロバイダの料金がまだ適用されます）。

- ライセンスや契約は必要ありません。
- ネットアップによるサポートは含まれていません。
- Cloud Volumes ONTAP システムあたりのプロビジョニング可能な容量は 500GiB に制限されています。
- ネットアップのアカウント 1 つにつき、最大 10 台の Cloud Volumes ONTAP システムを任意のクラウドプロバイダで使用できます。
- Cloud Volumes ONTAP システム用にプロビジョニングされた容量が 500GiB を超えると、Cloud Manager はシステムを Essentials パッケージ（容量ベースのライセンス）に変換します。

プロビジョニングされた容量が 500GiB 未満の他のシステムは、Freemium（Freemium 製品を使用して導入されている場合）に残ります。

Freemium製品の導入方法をご確認ください。

- ["AzureでCloud Volumes ONTAP のライセンスをセットアップする"](#)

容量ベースのライセンスパッケージ

容量単位のライセンスでは、TiB 単位の Cloud Volumes ONTAP に対して料金を支払うことができます。このライセンスはネットアップアカウントに関連付けられており、ライセンスで十分な容量が使用可能であれば、ライセンスに対して複数のシステムを充電することができます。

たとえば、20TiB のライセンスを 1 つ購入して 4 つの Cloud Volumes ONTAP システムを導入し、各システムに 5TiB のボリュームを割り当てて合計 20TiB にするとします。そのアカウントに導入されている各 Cloud Volumes ONTAP システムのボリュームで容量を使用できます。

容量ベースのライセンスは、`a_packag_` の形式で用意されています。Cloud Volumes ONTAP システムを導入するときは、`_Essentials_package` または `_Professional_package` を選択できます。

Essentials パッケージ

- Cloud Volumes ONTAP 構成を選択します。
 - シングルノードまたは HA システム
 - ディザスタリカバリ（DR）用のファイルストレージとブロックストレージまたはセカンダリデータ
- ネットアップのクラウドデータサービスを追加コストで利用できます

プロフェッショナルパッケージ

- すべての Cloud Volumes ONTAP 構成（シングルノードまたは任意のストレージタイプの HA）にライセンスを提供
- Cloud Backup を使用したボリュームのバックアップを含みます（このライセンスを使用するボリュームのみ）
- ネットアップのクラウドデータサービスを追加コストで利用できます

消費モデル

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

- ネットアップから購入したライセンス（BYOL）。任意のクラウドプロバイダで Cloud Volumes ONTAP を導入する際に使用できます。

1 つのクラウドプロバイダに制限されることはありません。

- クラウドプロバイダの市場から 1 時間単位のサブスクリプション（PAYGO）が提供されます。
- クラウドプロバイダの市場から年間契約を獲得できます。

次の点に注意してください。

- ネットアップからライセンスを購入した場合（BYOL）は、クラウドプロバイダが提供する PAYGO のサブスクリプションも必要です。

ライセンスは常に最初に請求されますが、次の場合は、マーケットプレイスで 1 時間ごとの料金が請求さ

れます。

- ライセンス容量を超えた場合
- ライセンスの期間が終了する場合
- 市場から年間契約を結んでいる場合、導入する Cloud Volumes ONTAP システムにはその契約が適用されます。BYOL と年間市場契約を組み合わせることはできません。

価格設定

価格設定の詳細については、を参照してください ["NetApp Cloud Central"](#)。

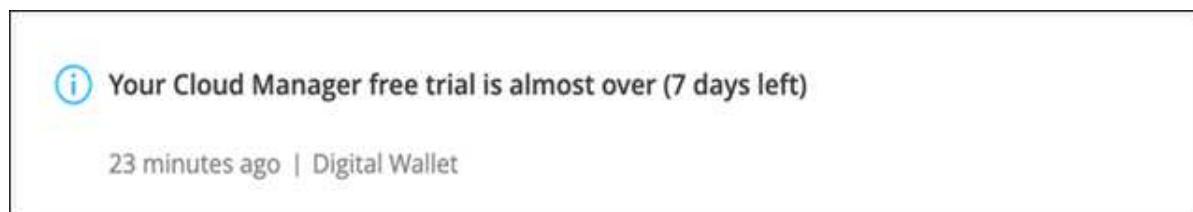
無償トライアルを利用できます

30 日間の無償トライアルをクラウドプロバイダのマーケットプレイスで従量課金制サブスクリプションで利用できます。無償トライアルには、Cloud Volumes ONTAP とクラウドバックアップが含まれています。トライアルは、市場で提供サービスに登録すると開始されます。

インスタンスや容量の制限はありません。Cloud Volumes ONTAP システムは必要な数だけ導入でき、必要な容量を30日間無償で割り当てることができます。無料トライアルは、30日後に1時間ごとの有料サブスクリプションに自動的に変換されます。

Cloud Volumes ONTAP のソフトウェアライセンス料金は1時間ごとに発生しませんが、クラウドプロバイダからインフラ料金が請求されます。

Cloud Managerには、無償トライアルが開始されたとき、7日が残ったとき、および1日が残っているときに通知が送信されます。例
:



サポートされている構成

容量ベースのライセンスパッケージは Cloud Volumes ONTAP 9.7 以降で利用できます。

容量制限

このライセンスモデルでは、個々の Cloud Volumes ONTAP システムでディスクとオブジェクトストレージへの階層化によって、最大 2 PiB の容量をサポートします。

ライセンス自体に関しては、最大容量制限はありません。

充電に関するメモ

- BYOL の容量を超えた場合やライセンスの有効期限が切れた場合は、マーケットプレイスのサブスクリプションに基づいて 1 時間あたりの料金が高すぎることを意味します。
- パッケージごとに 4TiB 以上の容量を追加容量が 4TiB 未満の Cloud Volumes ONTAP インスタンスは、

4TiB の割合で請求されます。

- データ提供用の Storage VM (SVM) を追加する場合、追加のライセンスコストは発生しませんが、データ提供用 SVM ごとの容量は 4TiB になります。
- ディザスタリカバリ用 SVM は、プロビジョニングされた容量に基づいて料金が発生します。
- HA ペアの場合、ノードのプロビジョニング済み容量に対してのみ料金が発生します。パートナーノードに同期ミラーリングされるデータには料金は発生しません。
- FlexClone ボリュームで使用される容量に対する料金は発生しません。
- ソースおよびデスティネーションの FlexCache ボリュームはプライマリデータとみなされ、プロビジョニング済みスペースに基づいて料金が発生します。

開始方法

容量単位のライセンスの取得方法については、以下をご覧ください。

- ["AzureでCloud Volumes ONTAP のライセンスをセットアップする"](#)

Keystone Flex サブスクリプション

成長に合わせて拡張できるサブスクリプションベースのサービス。運用コストの消費モデルを希望するお客様に、設備投資やリースを先行するお客様にシームレスなハイブリッドクラウドエクスペリエンスを提供します。

課金は、Keystone Flex サブスクリプションでの 1 つ以上の Cloud Volumes ONTAP HA ペアのコミット済み容量に基づいています。

各ボリュームのプロビジョニング済み容量は、Keystone Flex サブスクリプションのコミット済み容量と定期的に集計されて比較され、超過した場合は Keystone Flex サブスクリプションのバーストとして課金されます。

["Keystone Flex Subscriptions の詳細をご覧ください"](#)。

サポートされている構成

Keystone Flex Subscriptions は、HA ペアでサポートされます。現時点では、このライセンスオプションはシングルノードシステムではサポートされていません。

容量制限

個々の Cloud Volumes ONTAP システムでは、ディスクとオブジェクトストレージへの階層化によって、最大 2 PiB の容量をサポートしています。

開始方法

Keystone Flexサブスクリプションの概要については、以下をご覧ください。

- ["AzureでCloud Volumes ONTAP のライセンスをセットアップする"](#)

ノードベースのライセンス

ノードベースのライセンスは、Cloud Volumes ONTAP のライセンスをノード単位で付与することが可能になった旧世代のライセンスモデルです。このライセンスモデルは、新規のお客様にはご利用いただけません。また、無償トライアルもご利用いただけません。ノード単位の充電は、前述のキャパシティ単位の充電方法に置き換えられました。

既存のお客様は、ノードベースのライセンスを引き続き利用できます。

- アクティブなライセンスがある場合は、BYOL をライセンスの更新のみに使用できます。
- 有効なマーケットプレイスサブスクリプションをお持ちの場合は、そのサブスクリプションを通じて引き続き課金をご利用いただけます。

ライセンスの変換

既存の Cloud Volumes ONTAP システムを別のライセンス方式に変換することはできません。現在提供されている 3 つのライセンス方式は、容量ベースのライセンス、Keystone Flex Subscriptions、ノードベースのライセンスです。たとえば、システムをノードベースのライセンスから容量ベースのライセンスに変換することはできません（逆の場合も同様）。

別のライセンス方式に移行する場合は、ライセンスを購入し、そのライセンスを使用して新しい Cloud Volumes ONTAP システムを導入してから、その新しいシステムにデータをレプリケートできます。

システムの最大数

Cloud Volumes ONTAP システムの最大数は、使用しているライセンスモデルに関係なく、ネットアップアカウントあたり 20 に制限されます。

`a_system_`には、HA ペアまたはシングルノードシステムを指定します。たとえば、2 つの Cloud Volumes ONTAP HA ペアと 2 つのシングルノードシステムがある場合、合計 4 つのシステムがあり、アカウントに 16 のシステムを追加で配置できます。

ご質問がある場合は、アカウント担当者または営業チームにお問い合わせください。

["ネットアップアカウントの詳細については、こちらをご覧ください"。](#)

ストレージ

クライアントプロトコル

Cloud Volumes ONTAP は、iSCSI、NFS、SMB、S3 のクライアントプロトコルをサポートしています。

iSCSI

iSCSI は、標準のイーサネットネットワークで実行できるブロックプロトコルです。ほとんどのクライアントオペレーティングシステムには、標準のイーサネットポートで動作するソフトウェアイニシエータが搭載されています。

NFS

NFS は、UNIX および Linux システム向けの従来のファイルアクセスプロトコルです。クライアントは、NFSv3、NFSv4、および NFSv4.1 プロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。ファイルアクセスは、UNIX 形式の権限、NTFS 形式の権限、またはその両方の組み合わせを使用し、て制御できます。

クライアントは、NFS プロトコルと SMB プロトコルの両方を使用して同じファイルにアクセスできます。

SMB

SMB は、Windows システム向けの従来のファイルアクセスプロトコルです。クライアントは、SMB 2.0、SMB 2.1、SMB 3.0、および SMB 3.1.1 の各プロトコルを使用して ONTAP ボリューム内のファイルにアクセスできます。NFS と同様に、複数の形式の権限の組み合わせがサポートされています。

S3

Cloud Volumes ONTAP では、Microsoft AzureでのみS3をスケールアウトストレージのオプションとしてサポートしています。S3 プロトコルをサポートすると、SVM のバケットに格納されたオブジェクトへの S3 クライアントアクセスを設定できるようになります。

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

ディスクとアグリゲート

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



すべてのディスクとアグリゲートは、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。

概要

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



クラウドディスクにはいくつかのタイプがサポートされています。ディスクタイプはボリュームの作成時に選択し、デフォルトのディスクサイズは Cloud Volumes ONTAP の導入時に選択します。



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

Azure ストレージ

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

シングルノードシステム

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

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

管理対象の各ディスクタイプの最大ディスクサイズは 32TiB です。

管理対象ディスクと Azure BLOB ストレージをペアリングすることができます からに "使用頻度の低

いデータを低コストのオブジェクトストレージに階層化します"。

HA ペア

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

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

RAID タイプ

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

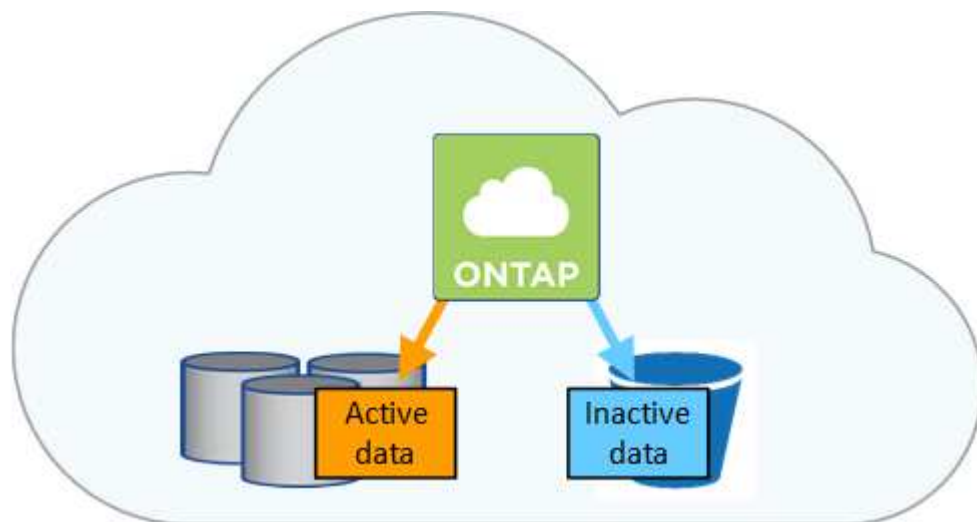
ホットスペア

RAID0 は、冗長性を確保するためにホットスペアの使用をサポートしていません。

Cloud Volumes ONTAP インスタンスに接続された未使用のディスク（ホットスペア）の作成は不要な費用であり、必要に応じて追加のスペースをプロビジョニングすることができません。そのため、お勧めしません。

データ階層化の概要

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



データ階層化は、FabricPool テクノロジーによって実現されます。



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

Azure のデータ階層化

Azure でデータ階層化を有効にすると、Cloud Volumes ONTAP は、ホットデータ用のパフォーマンス階層として Azure で管理されているディスクを、アクセス頻度の低いデータ用の大容量階層として Azure Blob Storage を使用します。

高パフォーマンス階層

高パフォーマンス階層には SSD と HDD があります。

大容量階層

Cloud Volumes ONTAP システムは、アクセス頻度の低いデータを単一の BLOB コンテナに階層化します。

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

Cloud Manager は、次の設定でストレージアカウントを作成します。

- アクセス層：ホット
- パフォーマンス：標準
- 冗長性：ローカル冗長ストレージ（LRS）
- アカウント：StorageV2（汎用v2）
- REST API 処理にはセキュアな転送が必要：有効
- ストレージアカウントキーへのアクセス：有効
- TLS の最小バージョン：バージョン 1.2
- インフラストラクチャの暗号化：無効

ストレージアクセス階層

Azure の階層化データのデフォルトのストレージアクセス階層は、_hot_tier です。ホット階層は、アクセス頻度の高いデータに最適です。

アクセス頻度の低いデータにアクセスしない場合は、_cool ストレージ階層に変更することでストレージコストを削減できます。ストレージ階層を変更すると、アクセス頻度の低いデータは最初はホットストレージ階層に配置され、アクセス日数が 30 日を超えない場合はアクセス頻度の低いストレージ階層に移行されます。

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

作業環境の作成時にストレージ階層を選択し、あとでいつでも変更できます。ストレージ階層の変更の詳細については、[を参照してください](#) "[使用頻度の低いデータを低コストのオブジェクトストレージに階層化](#)"。

データ階層化のためのストレージアクセス階層は、システム全体に適用されます。ボリューム単位ではあ

りません。

データ階層化と容量の制限

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

ボリューム階層化ポリシー

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

一部の階層化ポリシーには、最小冷却期間が関連付けられています。この期間は、データを「コールド」と見なして容量階層に移動するために、ボリューム内のユーザーデータを非アクティブのままにする必要がある時間を設定します。クーリング期間は、データがアグリゲートに書き込まれると開始されます。



最小クーリング期間とデフォルトのアグリゲートしきい値を 50% に変更できます（詳細については後述します）。"[冷却期間を変更する方法について説明します](#)" および "[しきい値を変更する方法について説明します](#)"。

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

Snapshot のみ

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

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

すべて

すべてのデータ（メタデータを除く）はすぐにコールドとしてマークされ、オブジェクトストレージにできるだけ早く階層化されます。ボリューム内の新しいブロックがコールドになるまで、48 時間待つ必要はありません。「すべて」のポリシーが設定される前のボリュームにあるブロックは、コールドになるまで 48 時間かかります。

読み取られた場合、クラウド階層のコールドデータブロックはコールドのまま、パフォーマンス階層に書き戻されません。このポリシーは ONTAP 9.6 以降で使用できます。

自動

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

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

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

なし

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

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

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

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

- 自動：31 日
- Snapshot のみ：2 日

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



Cloud Volumes ONTAP をオフにすると、システムを再起動するまで各ブロックの温度が維持されます。たとえば、システムの電源をオフにしたときにブロックの温度が 5 であっても、システムの電源をオンにしたときの温度は 5 のままです。

データ階層化の設定

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

ストレージ管理

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



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

ストレージのプロビジョニング

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

プロビジョニングの簡素化

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

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

- 十分な空きスペースがある既存のアグリゲートにボリュームを配置します。
- ボリュームを既存のアグリゲートに配置するには、そのアグリゲート用に追加のディスクを購入します。
- 新しいアグリゲートのディスクを購入し、そのアグリゲートにボリュームを配置します。

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



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

高度な割り当て

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

容量管理

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

自動容量管理

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

次の例は、このモードの動作を示しています。

- アグリゲートが容量のしきい値に達してディスクの空き容量が増えた場合、Cloud Manager はそのアグリゲート用の新しいディスクを自動的に購入し、ボリュームを継続して拡張できるようにします。

Cloud Manager は 15 分ごとに空きスペースの比率をチェックして、ディスクの追加購入が必要かどうかを判断します。

- アグリゲートが容量のしきい値に達し、かつそれ以上ディスクをサポートできない場合、Cloud Manager は、そのアグリゲートから使用可能な容量を持つアグリゲートまたは新しいアグリゲートにボリュームを自動的に移動します。

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

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

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

容量の自動管理による LUN の管理

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。

手動による容量管理

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

書き込み速度

Cloud Manager では、ほとんどの Cloud Volumes ONTAP 構成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。書き込み速度を選択する前に、高速書き込みを使用する場合の標準設定と高設定の違い、およびリスクと推奨事項を理解しておく必要があります。

通常書き込み速度

通常書き込み速度を選択した場合、データはディスクに直接書き込まれます。データをディスクに直接書き込んだ場合、計画外のシステム停止が発生した場合や、計画外のシステム停止が発生した場合のデータ損失の可能性を低減します（HA ペアのみ）。

デフォルトでは、通常書き込み速度が使用されます。

高速書き込み速度

高速書き込みを選択すると、データはディスクに書き込まれる前にメモリにバッファされるため、書き込みパフォーマンスが向上します。このキャッシュにより、計画外のシステム停止が発生した場合にデータが失われる可能性があります。

計画外のシステム停止が発生した場合に失われる可能性があるデータの量は、最後の 2 つの整合ポイントの範囲です。整合ポイントとは、バッファされたデータをディスクに書き込むことです。整合ポイントは、書き込みログがいっぱいになったとき、または 10 秒後（どちらか早い方）に発生します。ただし、クラウドプロバイダが提供するストレージのパフォーマンスが整合ポイントの処理時間に影響する可能性があります。

高速書き込みを使用する場合

高速書き込みパフォーマンスが求められるワークロードで、計画外のシステム停止が発生した場合や、計画外のシステム停止（HA ペアのみ）に伴うカスケード障害が発生した場合のデータ損失リスクに対処できる場合は、高速書き込み速度を使用することを推奨します。

高速書き込みを使用する場合の推奨事項

高速書き込み速度を有効にする場合は、アプリケーションレイヤでの書き込み保護を確保するか、またはデータ損失が発生した場合にアプリケーションで許容されるようにする必要があります。

高速書き込み速度をサポートする構成

すべての Cloud Volumes ONTAP 構成で高速書き込みがサポートされるわけではありません。デフォルトでは、これらの構成では通常書き込み速度が使用されます。

Azure

シングルノードシステムを使用する場合、Cloud Volumes ONTAP では、すべての種類の VM で高速な書き込み速度がサポートされます。

HA ペアを使用する場合、Cloud Volumes ONTAP では 9.8 リリース以降、複数の種類の VM で高速の書き込み速度がサポートされます。にアクセスします ["Cloud Volumes ONTAP リリースノート"](#) をクリックして、高速の書き込み速度をサポートする VM タイプを確認します。

書き込み速度を選択する方法

を作成するときに、書き込み速度を選択できます 新しい作業環境を構築できます ["既存のシステムの書き込み速度を変更する"](#)。

データ損失が発生した場合の予測

高速の書き込み速度を選択し、データ損失が発生した場合、システムをブートして、ユーザの手を煩わせることなくデータを提供できるはずですが、ノードでデータが失われると、2つの EMS メッセージが報告されます。1つは `waf1.root.content.changed` で、もう1つは `ERROR` 重大度レベルイベントです。もう1つは、デバッグ重大度レベルイベントを含む `nv.check.failed` です。両方のメッセージがデータ損失の兆候として存在している必要があります。

データ損失が発生した場合のデータアクセスの停止方法

データ損失について懸念がある場合、データ損失時にアプリケーションの実行を停止し、データ損失の問題に適切に対処したあとでデータアクセスを再開するには、CLI から NVFAIL オプションを使用してこの目標を達成します。

をクリックして **NVFAIL** オプションを有効にします

```
vol modify -volume <vol-name> -nvfail on`
```

をクリックして **NVFAIL** 設定を確認します

```
vol show -volume <vol-name> -fields nvfail`
```

NVFAIL オプションを無効にする場合

```
vol modify -volume <vol-name> -nvfail off`
```

データ損失が発生した場合、NVFAIL が有効になっている NFS または iSCSI ボリュームは、データ処理を停止する必要があります（ステートレスプロトコルである CIFS への影響はありません）。詳細については、を参照してください ["NFS ボリュームまたは LUN へのアクセスに対する NVFAIL の影響"](#)。

をクリックして **NVFAIL** 状態を確認します

```
vol show -fields in in-nvfailed-state`」を参照してください
```

データ損失の問題に適切に対処したら、NVFAIL 状態を解消でき、ボリュームへのデータアクセスが可能になります。

をクリックして **NVFAIL** 状態を解消します

```
vol modify -volume <vol-name> -in-nvfailed-state false
```


Flash Cache

一部のCloud Volumes ONTAP 構成にはローカルのNVMeストレージが含まれており、Cloud Volumes ONTAP はパフォーマンスを向上させるために_Flash Cache _として使用します。

Flash Cache とは

Flash Cache は、最近読み取られたユーザデータとネットアップのメタデータをリアルタイムでインテリジェントにキャッシングすることで、データへのアクセスを高速化します。データベース、Eメール、ファイルサービスなど、ランダムリードが大量に発生するワークロードに効果的です。

サポートされている構成

Flash Cacheは、特定のCloud Volumes ONTAP 構成でサポートされています。でサポートされている構成を表示します ["Cloud Volumes ONTAP リリースノート"](#)

制限

- Flash Cache のパフォーマンス向上を利用するには、すべてのボリュームで圧縮を無効にする必要があります。

Cloud Manager からボリュームを作成するときに Storage Efficiency を使用しないようにするか、ボリュームを作成してから実行するように選択します ["CLI を使用してデータ圧縮を無効にします"](#)。

- 再起動後のキャッシュの再ウォームアップは、Cloud Volumes ONTAP ではサポートされていません。

WORM ストレージ

Cloud Volumes ONTAP システム上で Write Once Read Many (WORM) ストレージをアクティブにして、指定した保存期間内にファイルを変更せずに保持できます。クラウド WORM ストレージには SnapLock テクノロジーが採用されており、WORM ファイルはファイルレベルで保護されます。

WORM ストレージの仕組み

WORM ストレージにコミットされたファイルは、保持期間が過ぎたあとも変更することはできません。改ざん防止クロックは、WORM ファイルの保持期間が経過したタイミングを決定します。

保存期間が経過すると、不要になったファイルを削除する必要があります。

充電中

WORM ストレージの充電は、合計プロビジョニング容量に基づいて 1 時間ごとに行われます。

["WORM ストレージの価格設定については、こちらをご覧ください"](#)。

WORM ストレージのアクティブ化

新しい作業環境を作成するときに、Cloud Volumes ONTAP システムで WORM ストレージをアクティブに

きます。これには、ファイルのデフォルトの保持期間の設定も含まれます。



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

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

The screenshot shows the 'Create a New Working Environment' wizard in Cloud Manager. The current step is 'WORM (write once, read many)'. On the left, under 'Write Speed', there are two options: 'Normal' (selected) and 'High'. The 'Normal' option description states: 'Data is written directly to disk, reducing the likelihood of data loss in the event of an unplanned system outage.' The 'High' option description states: 'Data is buffered in memory before it is written to disk, which provides faster write performance. Due to this caching, there is the potential for data loss in the event of an unplanned system outage.' On the right, under 'WORM', there is a description: 'You can use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes and to protect from malware attacks. WORM files are protected at the file level. [Learn More](#)'. Below this, there are two radio buttons: 'Disable WORM' and 'Activate WORM' (selected). A notice states: 'Notice: If you activate WORM storage, data tiering to object storage will be disabled on the system.' At the bottom, there is a 'Retention Period' field set to '15' years. A blue 'Continue' button is at the bottom center. The footer shows 'Cloud Manager 3.9.9 Build: 0 Jun 30, 2021 02:52:27 pm UTC Environment: staging'.

ファイルを **WORM** にコミットしています

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

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

制限

- Cloud Volumes ONTAP の WORM ストレージは、「信頼されたストレージ管理者」モデルで機能します。WORM ファイルは書き換えから保護されますが、期限切れ前の WORM データがボリュームに含まれていた場合でも、クラスタ管理者はボリュームを削除できます。
- 信頼できるストレージ管理者モデルに加えて、Cloud Volumes ONTAP の WORM ストレージも「信頼できるクラウド管理者」モデルで暗黙的に動作します。クラウド管理者は、クラウドプロバイダからクラウドストレージを直接削除するか、編集することで、有効期限が切れる前に WORM データを削除できました。
- WORM ストレージをアクティブ化すると、オブジェクトストレージへのデータ階層化を有効にできません。
- WORM ストレージを有効にするには、Cloud Backup Service を無効にする必要があります。

ハイアベイラビリティペア

Azure のハイアベイラビリティペア

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

HA コンポーネント

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



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

Azure Standard Load Balancer の略

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

可用性セット

Azure 可用性セットは、Cloud Volumes ONTAP ノードを論理的にグループ化したものです。可用性セットを使用すると、ノードが異なる障害になっていることを確認し、ドメインを更新して冗長性と可用性を確保できます。"可用性セットの詳細については、[Azure のドキュメントを参照してください](#)。"

ディスク

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

ストレージアカウント

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

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

- Azure BLOB ストレージへのデータ階層化には 1 つのストレージアカウントが必要です。
- Cloud Volumes ONTAP 9.7 以降では、Cloud Manager で HA ペア用に作成するストレージアカウントを汎用 v2 のストレージアカウントに使用できます。
- 作業環境の作成時に、Cloud Volumes ONTAP 9.7 HA ペアから Azure ストレージアカウントへの HTTPS 接続を有効にすることができます。このオプションを有効にすると、書き込みパフォーマンスに影響する可能性があります。作業環境の作成後に設定を変更することはできません。

RPO と RTO

HA 構成では、次のようにデータの高可用性が維持されます。

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

ストレージのテイクオーバーとギブバック

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

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

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



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

ストレージのテイクオーバー、再同期、ギブバックは、すべてデフォルトで自動的に実行されます。ユーザによる操作は必要ありません。

ストレージ構成

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

テイクオーバー中は操作を実行できません

HA ペアの一方向のノードが利用できない場合は、もう一方のノードがパートナーに引き続きデータを提供します。これを `_storage takeover_` と呼びます。storage giveback が完了するまで、いくつかの操作は実行できません。



HA ペアのノードが利用できない場合、Cloud Manager の作業環境の状態は `Degraded_` になります。

ストレージのテイクオーバー中は、Cloud Manager から次の操作を実行できません。

- サポート登録
- ライセンスの変更
- インスタンスまたは VM のタイプが変更された
- 書き込み速度の変更
- CIFS セットアップ
- 構成バックアップの場所を変更する
- クラスタのパスワードを設定しています
- ディスクとアグリゲートの管理（高度な割り当て）

これらの操作は、ストレージのギブバックが完了し、作業環境の状態が正常に戻ったあとで再度実行できます。

セキュリティ

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

保存データの暗号化

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

- ネットアップの暗号化ソリューション（NVE および NAE）
- Azure Storage Service Encryption の略

ネットアップの暗号化ソリューションは、クラウドプロバイダがネイティブに暗号化することでハイパーバイザーレベルでデータを暗号化します。これにより、機密性の高いデータには二重の暗号化が必要になる場合があります。暗号化されたデータにアクセスすると、暗号化されていないデータがハイパーバイザーレベルで 2 回（クラウドプロバイダのキーを使用）暗号化されてから、ネットアップの暗号化ソリューションを再度使用して（外部キー管理ツールのキーを使用）暗号化されます。

ネットアップの暗号化ソリューション（NVE および NAE）

Cloud Volumes ONTAP はをサポートします ["NetApp Volume Encryption（NVE）および NetApp Aggregate Encryption（NAE）"](#)。NVE と NAE は、（FIPS）140-2 に準拠したボリュームの保管データ暗号化を可能にするソフトウェアベースのソリューションです。NVE と NAE はいずれも AES 256 ビット暗号化を使用します。

- NVE は、一度に 1 ボリュームずつ保管データを暗号化する。各データボリュームには、一意の暗号化キーがあります。
- NAE は NVE の拡張機能です。NVE は各ボリュームのデータを暗号化し、ボリュームはアグリゲート全体でキーを共有します。NAE では、アグリゲート内のすべてのボリュームの共通ブロックも重複排除できます。

NVE と NAE はどちらも外部キー管理機能でサポートされています。

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

サポートされているキー管理ツールをセットアップするだけで済みます。セットアップ手順については、を参照してください ["ネットアップの暗号化ソリューションによるボリュームの暗号化"](#)。

Azure Storage Service Encryption の略

データは、を使用して Azure の Cloud Volumes ONTAP で自動的に暗号化されます ["Azure Storage Service Encryption の略"](#) Microsoft が管理するキーを使用する場合：

必要に応じて、独自の暗号化キーを使用できます。 ["Azure でお客様が管理するキーを使用するように Cloud Volumes ONTAP を設定する方法について説明します"](#)。

ONTAP のウィルススキャン

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

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

Vscan でサポートされるベンダー、ソフトウェア、およびバージョンについては、を参照してください ["NetApp Interoperability Matrix を参照してください"](#)。

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

ランサムウェアからの保護

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

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

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

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

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

2 Block Ransomware File Extensions

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

パフォーマンス

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

パフォーマンスに関するテクニカルレポート

- Cloud Volumes ONTAP for Microsoft Azure

["NetApp テクニカルレポート 4671 : アプリケーションワークロードを使用した Azure における Cloud Volumes ONTAP のパフォーマンス特性評価"](#)

CPU パフォーマンス

Cloud Volumes ONTAP ノードは、クラウドプロバイダの監視ツールから高い利用率（90% 超）を示します。これは、ONTAP が仮想マシンに提供されているすべての vCPU を、必要に応じて使用できるようにリザーブするためです。

["Cloud Volumes ONTAP のパフォーマンスを監視する方法について説明します"](#)をクリックしてください ["CLI を使用して ONTAP CPU 利用率を監視する方法に関するネットアップの技術情報アートを参照してください"](#)

ノードベースの BYOL のライセンス管理

ノードベース BYOL を使用する各 Cloud Volumes ONTAP システムには、アクティブなサブスクリプションを使用してシステムライセンスがインストールされている必要があります。Cloud Manager は、ライセンスを管理し、期限が切れる前に警告を表示することでプロセスを簡易化します。



ノードベースのライセンスは、Cloud Volumes ONTAP を使用するための旧世代の BYOL です。ノードベースのライセンスは、ライセンスの更新のみ可能です。

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

BYOL システムのライセンス

ノードベースのライセンスは、単一のノードまたは HA ペアに対して最大 368 TiB の容量を提供します。

Cloud Volumes ONTAP BYOL システムでは、複数のライセンスを購入して、368 TiB を超える容量を割り当てることができます。たとえば、2 つのライセンスを購入して、Cloud Volumes ONTAP に最大 736 TiB の容量を割り当てることができます。また、4 つのライセンスを購入して、最大 1.4 PiB までライセンスを取得することもできます。

シングルノードシステムまたは HA ペアに対して購入できるライセンスの数に制限はありません。



購入した一部のオンプレミス ONTAP ストレージシステムには、Cloud Volumes ONTAP のライセンスが無償で付属している場合があります。ライセンスを使用して新しい Cloud Volumes ONTAP システムを作成するか、または既存の Cloud Volumes ONTAP システムにライセンスを適用して容量を拡張できます。"使用できるライセンスがあるかどうかを確認します"。

ディスク制限によって、ディスクだけを使用することで容量制限に達することがないことに注意してください。を使用すると、ディスク制限を超えることができます "使用頻度の低いデータをオブジェクトストレージに階層化します"。ディスクの制限については、を参照してください "ストレージの制限については、『Cloud Volumes ONTAP リリースノート』を参照してください"。

新しいシステムのライセンス管理

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

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

Cloud Manager がセキュアなインターネット接続を介してライセンスファイルにアクセスできない場合は、を実行できます ["ファイルを自分で取得し、Cloud Manager に手動でアップロードする"](#)。

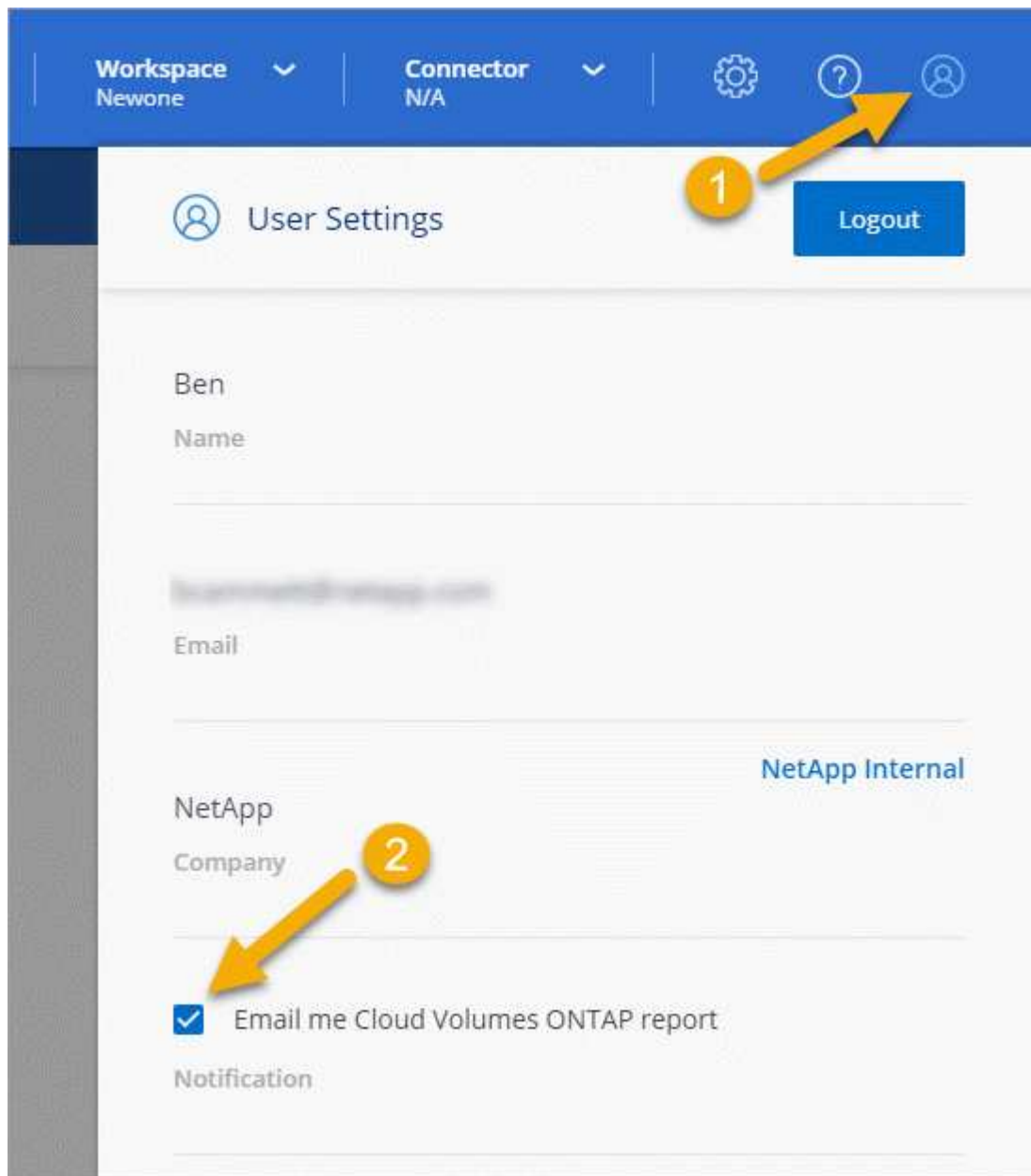
ライセンスの有効期限

Cloud Manager では、ノードベースのライセンスの期限が切れる 30 日前とライセンスの期限が切れる 30 日後に警告が表示されます。次の図は、ユーザインターフェイスに表示される 30 日間の有効期限に関する警告を示しています。



メッセージを確認する作業環境を選択できます。

アカウント管理者がオプションを有効にしている場合、Cloud Manager は Cloud Volumes ONTAP レポートにライセンス有効期限の警告を E メールで送信します。



E メールで送信されたレポートには、2 週間ごとにライセンスの有効期限に関する警告が記載され

期限までにライセンスを更新しない場合は、Cloud Volumes ONTAP システムがシャットダウンされます。再起動すると、自動的にシャットダウンされます。

ライセンスの更新

ネットアップの担当者に連絡してノードベースの BYOL サブスクリプションを更新すると、Cloud Manager は NetApp から新しいライセンスを自動的に取得して 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を介してライセンスファイルにアクセスできない場合は、を実行できます **"ファイルを自分で取得し、Cloud Manager に手動でアップロードする"**。

新しいシステムへのライセンスの移動

既存のシステムを削除してから、同じライセンスを使用して新しいシステムを作成する場合、ノードベースの BYOL ライセンスを Cloud Volumes ONTAP システム間で移動できます。

たとえば、既存のライセンスが有効なシステムを削除してから、別の VPC / VNet またはクラウドプロバイダ内の新しい BYOL システムでライセンスを使用できます。どのクラウドプロバイダでも使用できるのは、クラウドに依存しないシリアル番号 `_` のみです。クラウドに依存しないシリアル番号は、`_908xxxx_prefix` で始まります。

BYOL ライセンスは、お客様の会社およびネットアップサポートサイトの特定のクレデンシャルセットに関連付けられていることに注意してください。

AutoSupport と Active IQ デジタルアドバイザー

ONTAP の AutoSupport コンポーネントはテレメトリを収集し、分析用に送信します。Active IQ デジタルアドバイザーは AutoSupport からデータを分析し、プロアクティブなサポートと最適化を提供します。Active IQ は、人工知能を使用して潜在的な問題を特定し、ビジネスに影響が及ぶ前に解決を支援します。

Active IQ では、クラウドベースのポータルとモバイルアプリを通じて、実用的な予測分析とプロアクティブなサポートを提供することで、グローバルハイブリッドクラウド全体でデータインフラを最適化できます。SupportEdge との契約が締結されているネットアップのすべてのお客様は、Active IQ が提供するデータ主体の分析情報と推奨事項を利用できます（機能は製品やサポートレベルによって異なります）。

Active IQ でできることは次のとおりです。

- アップグレードを計画する。

Active IQ では、ONTAP の新しいバージョンにアップグレードすることで解決可能な問題が環境内で特定されます。また、アップグレードを計画する際に役立つ Upgrade Advisor コンポーネントも用意されています。

- システムの健全性を表示します。

Active IQ ダッシュボードで、健全性に関する問題が報告されるため、それらの問題の解決に役立ちます。システム容量を監視して、ストレージスペースが不足しないようにします。システムのサポートケースを表示します。

- パフォーマンスを管理

Active IQ には、ONTAP System Manager に表示されるよりも長期間にわたるシステムパフォーマンスが

表示されます。パフォーマンスに影響を与えている構成やシステムの問題を特定します。効率性の最大化 Storage Efficiency 指標を表示し、より多くのデータをより少ないスペースに格納する方法を特定します。

- インベントリと構成を表示します。

Active IQ は、インベントリおよびソフトウェアとハードウェアの構成に関するすべての情報を表示します。サービス契約がいつ期限切れになるかを確認し、サービス契約を更新してサポートを継続するかを確認します。

関連情報

- ["ネットアップのマニュアル：Active IQ Digital Advisor"](#)
- ["Active IQ を起動します"](#)
- ["SupportEdge サービス"](#)

Cloud Volumes ONTAP のデフォルト設定

Cloud Volumes ONTAP がデフォルトでどのように設定されているかを理解すると、システムのセットアップと管理に役立ちます。特に、ONTAP に精通している場合は、Cloud Volumes ONTAP のデフォルト設定は ONTAP とは異なるためです。

デフォルトのセットアップ

- Cloud Manager は、Cloud Volumes ONTAP の導入時にデータを提供する Storage VM を 1 つ作成します。追加の Storage VM をサポートする構成もあります。 ["Storage VM の管理に関する詳細情報"](#)。

Cloud Manager 3.9.5 リリース以降では、最初の Storage VM で論理スペースのレポートが有効になります。スペースが論理的に報告されると、ONTAP は、Storage Efficiency 機能で削減されたすべての物理スペースが使用済みと報告するようにボリュームスペースを報告します。

- Cloud Manager は、次の ONTAP 機能ライセンスを Cloud Volumes ONTAP に自動的にインストールします。
 - CIFS
 - FlexCache
 - FlexClone
 - iSCSI
 - NetApp Volume Encryption （ライセンス使用システムまたは登録従量課金制システムの場合のみ）
 - NFS
 - SnapMirror
 - SnapRestore
 - SnapVault
- デフォルトでは、いくつかのネットワークインターフェイスが作成されます。
 - クラスタ管理 LIF
 - クラスタ間 LIF

- AzureのHAシステム上のSVM管理LIF
- ノード管理 LIF
- iSCSI データ LIF
- CIFS および NFS データ LIF



クラウドプロバイダの要件により、Cloud Volumes ONTAP のLIFフェイルオーバーはデフォルトで無効になっています。LIF を別のポートに移行すると、インスタンス上の IP アドレスとネットワークインターフェイス間の外部マッピングが解除され、LIF にアクセスできなくなります。

- Cloud Volumes ONTAP は、HTTPS を使用してコネクタに構成バックアップを送信します。

バックアップにはからアクセスできます <https://ipaddress/occm/offboxconfig/> ここで、*ipaddress* はコネクタホストの IP アドレスです。

- Cloud Manager は、他の管理ツール（System Manager や CLI など）とは異なるボリューム属性をいくつか設定します。

次の表に、Cloud Manager がデフォルトとは異なる設定にしたボリューム属性を示します。

属性	Cloud Manager によって設定される値
オートサイズモード	成長
最大オートサイズ	1,000 パーセント  アカウント管理者は、[設定] ページからこの値を変更できます。
セキュリティ形式	CIFS ボリューム UNIX の場合は NTFS 、 NFS ボリュームの場合は NTFS
スペースギャランティスタイル	なし
UNIX 権限（NFS のみ）	777

+
これらの属性の詳細については、`_volume create` のマニュアルページを参照してください。

システムデータ用の内蔵ディスク

ユーザデータ用のストレージに加えて、Cloud Manager はシステムデータ用のクラウドストレージも購入します。

Azure（シングルノード）

- Premium SSD ディスク × 3 :

- ブートデータ用に 10 GiB のディスクを 1 台
- ルートデータ用に 140GiB のディスクが 1 つ
- NVRAM 用に 512GiB ディスクが 1 本必要です

Cloud Volumes ONTAP 用に選択した仮想マシンでウルトラ SSD がサポートされている場合、システムは Premium SSD ではなく 32GiB Ultra SSD を NVRAM に使用します。

- コアを節約するために 1024 GiB の標準 HDD ディスクを 1 台
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot
- ブートディスクとルートディスクはデフォルトで暗号化されています。

Azure （HA ペア）

- ブートボリューム用の 10GiB Premium SSD ディスク × 2 （ノードごとに 1 つ）
- ルート用の 140 GiB Premium Storage ページプロブ 2 つ ボリューム（ノードごとに 1 つ）
- コアを節約するために 1024 GiB の標準 HDD ディスク 2 台（ノードごとに 1 つ）
- NVRAM 用 512GiB Premium SSD ディスク × 2 （各ノードに 1 つ）
- 各ブートディスクとルートディスクに 1 つの Azure Snapshot
- ブートディスクとルートディスクはデフォルトで暗号化されています。

ディスクが存在する場所

Cloud Manager は次のようにストレージを配置します。

- ブートデータは、インスタンスまたは仮想マシンに接続されたディスクにあります。
このディスクにはブートイメージが含まれており、Cloud Volumes ONTAP では使用できません。
- システム構成とログを含むルートデータは、aggr0 にあります。
- Storage Virtual Machine （SVM）ルートボリュームは aggr1 にあります。
- データボリュームも aggr1 にあります。

知識とサポート

サポートに登録します

ネットアップテクニカルサポートでサポートケースをオープンするには、事前に 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、サポートに登録しておく必要があります。

NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

手順

1. ネットアップサポートサイトのアカウントがない場合は、**"1 名で登録します"**。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、*** Support *** を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

3. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、**[* Continue (続行)]** をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E メールアドレスとパスワードを入力して認証プロセスを実行します。

Cloud Manager で NSS アカウントを使用することができます。

注：お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。

アカウントを登録してサポートを受けてください

サポートの登録は、Cloud Manager のサポートダッシュボードで実行できます。

手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、* Support * を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [* リソース] タブで、[* サポートに登録 *] をクリックします。
3. 登録する NSS 資格情報を選択し、* 登録 * をクリックします。

ヘルプを表示します

ネットアップでは、Cloud Manager とその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

セルフサポート

次のオプションは、1 日 24 時間、週 7 日間無料でご利用いただけます。

- ["ナレッジベース"](#)

Cloud Manager のナレッジベースで問題のトラブルシューティングに役立つ記事を検索してください。

- ["コミュニティ"](#)

Cloud Manager コミュニティに参加して、進行中のディスカッションに参加したり、新しいコミュニティを作成したりできます。

- [ドキュメント](#)

現在表示している Cloud Manager のドキュメント。

- mailto : ng-cloudmanager-feedback@netapp.com [フィードバックメール]

お客様のご意見をお考えください。Cloud Manager の改善に役立つフィードバックを送信します。

ネットアップサポート

上記のセルフサポートオプションに加え、サポートを有効にしたあとに問題が発生した場合は、ネットアップサポートエンジニアと協力して解決できます。

手順

1. Cloud Manager で、 * Help > Support * の順にクリックします。
2. テクニカルサポートで利用可能なオプションのいずれかを選択します。
 - a. [* お問い合わせ *] をクリックして、ネットアップ・テクニカル・サポートの電話番号を検索してください。
 - b. [* 問題 を開く *] をクリックし、いずれかのオプションを選択して、[* 送信 *] をクリックします。

ネットアップの担当者がケースを確認し、すぐに対応を開始します。

法的通知

著作権に関する声明、商標、特許などにアクセスできます。

著作権

<http://www.netapp.com/us/legal/copyright.aspx>

商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/us/media/patents-page.pdf>

プライバシーポリシー

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

["Cloud Manager 3.9 に関する注意事項"](#)

著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

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、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、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

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、またはその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り特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> 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。