はじめに
Cloud Volumes ONTAP

NetApp
June 07, 2022

目次

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。

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

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。"。

<img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png" Alt="3"> 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"。

プライベートリンク

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モニタ
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モニタ
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 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

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://cloudmanagerinfraprod.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、キーヴォールトを作成し、そのヴォールトでキーを生成します
2. 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。

キーボールトを作成し、キーを生成します

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

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. "キーボールトでキーを生成します"。

   キーに関する次の要件に注意してください。

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

暗号化キーを使用する作業環境を作成します

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

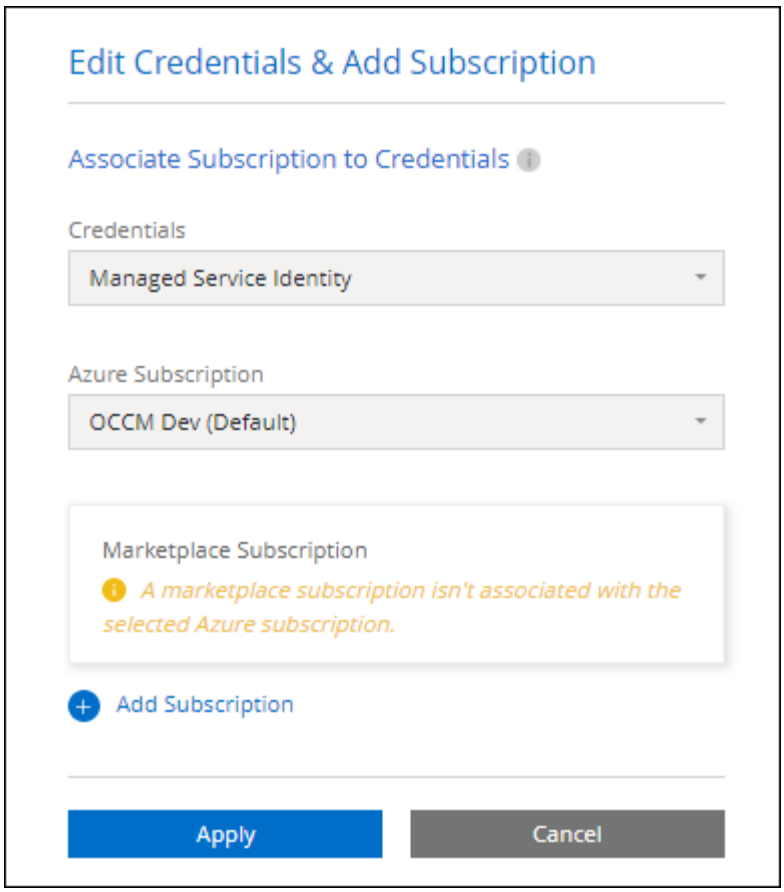
プロビジョニングされた容量が最大500GiBのCloud Volumes ONTAP を無料で使用するには、Freemium製品を選択してください。 "Freemium 製品の詳細をご覧ください"。

手順

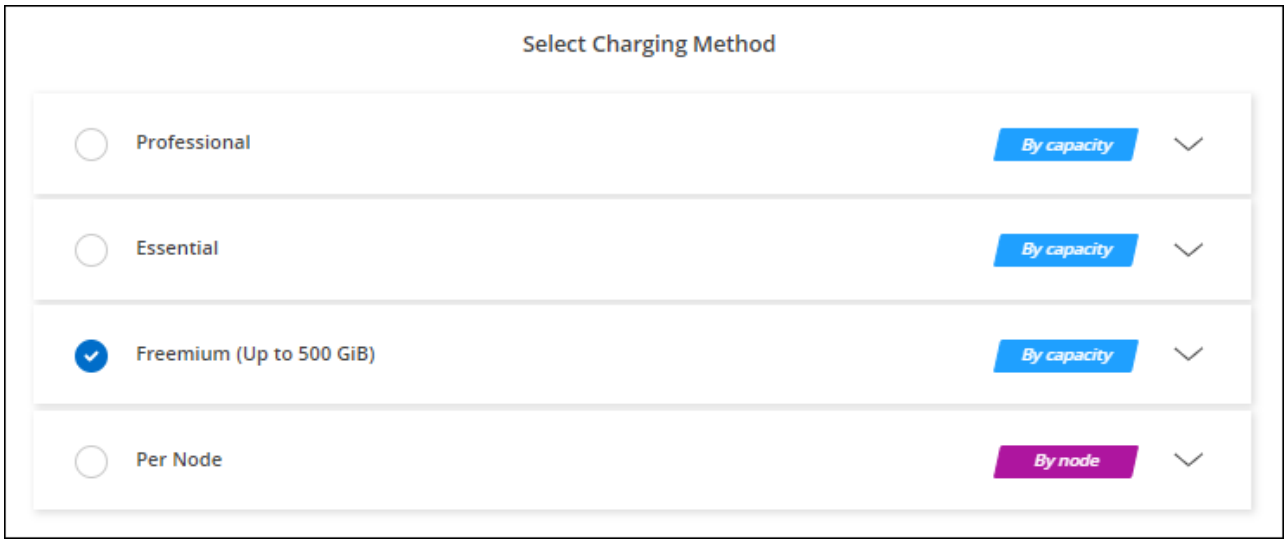
1. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。

   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、システムはに自動的に変換されないかぎり、マーケットプレイスのサブスクリプションを通じて料金が請求されることはありません "Essentials パッケージ"。



a. 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。



"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"

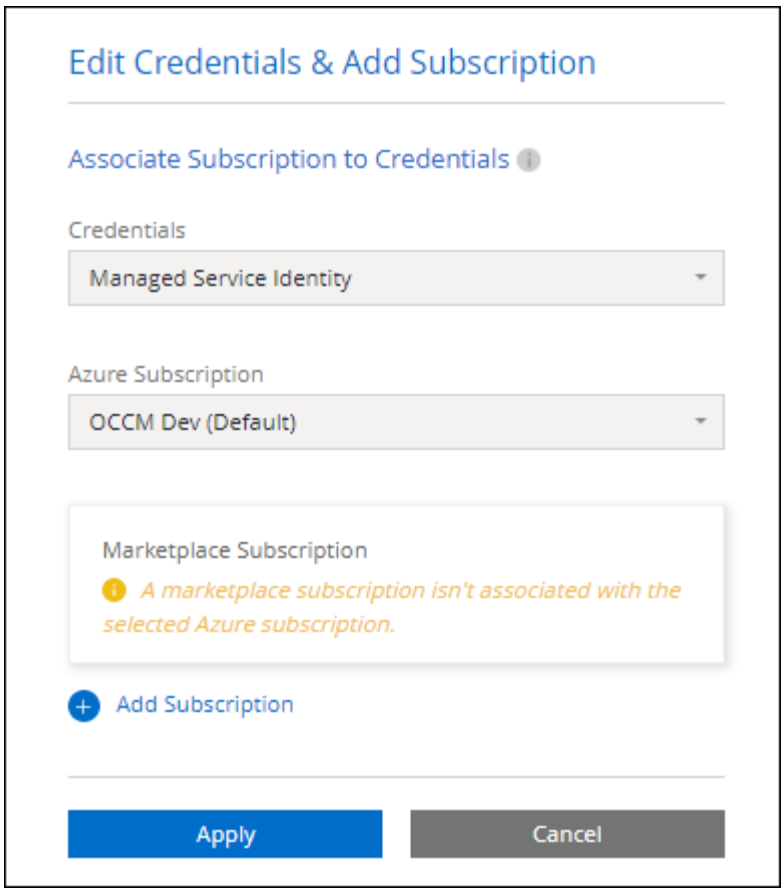
   Cloud Managerは、ネットアップのライセンスサービスを自動的に照会して、ネットアップサポートサイトのアカウントに関連付けられているライセンスに関する詳細を取得します。エラーがなければ、Cloud Managerはライセンスをデジタルウォレットに自動的に追加します。

   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"。

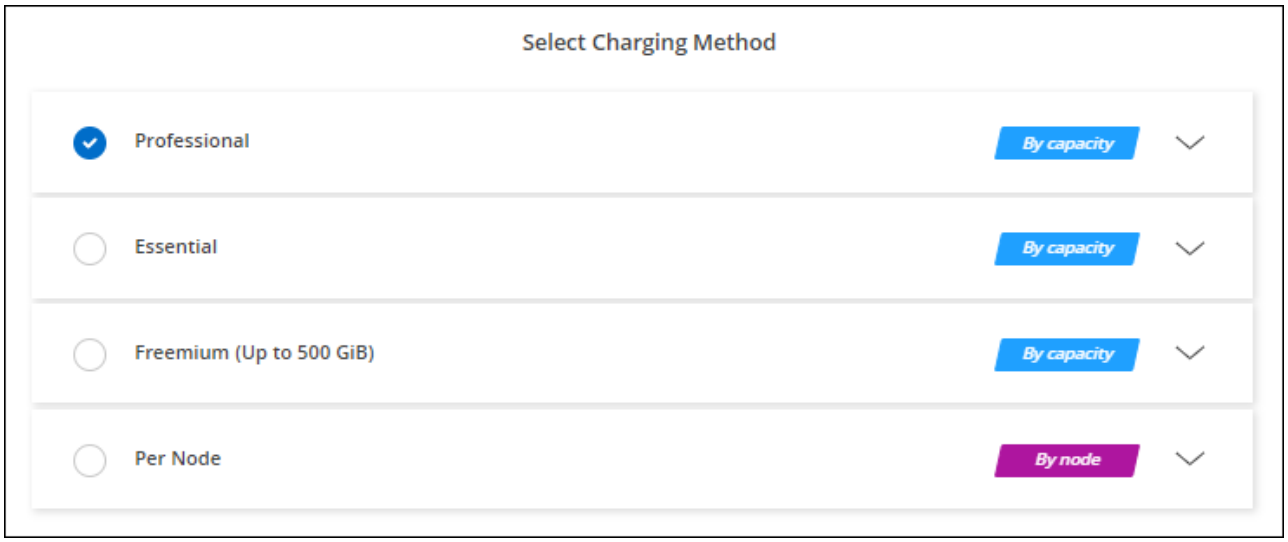
3. キャンバスページで、*作業環境の追加*をクリックし、Cloud Managerの手順に従います。

   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。



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。



"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

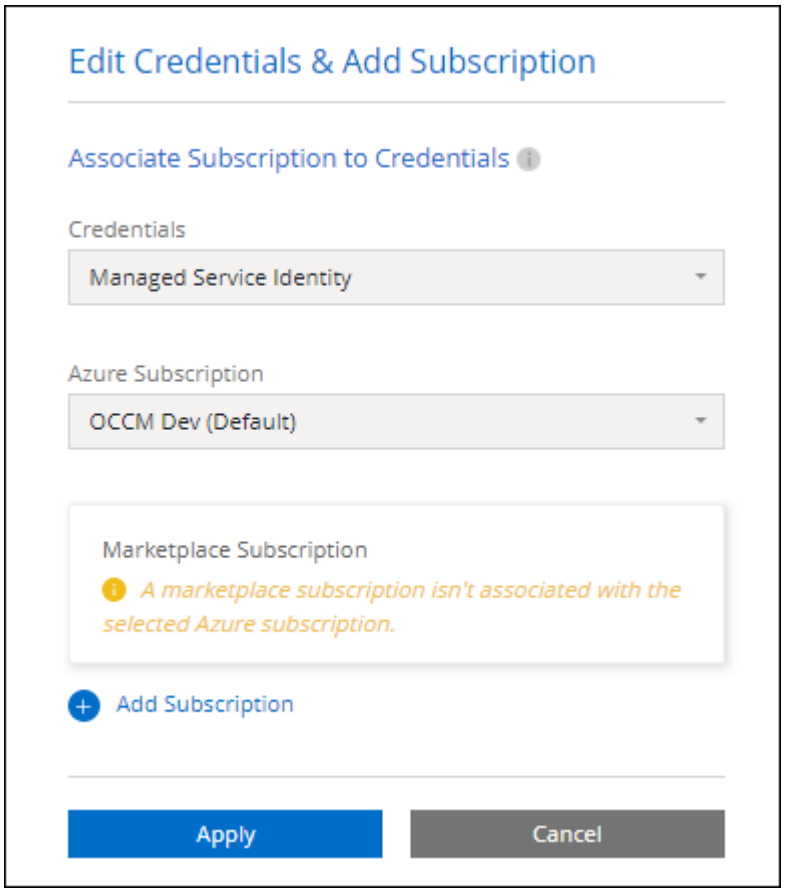
クラウドプロバイダのマーケットプレイスから提供されたサービスに登録すると、1時間ごとに料金が発生します。

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

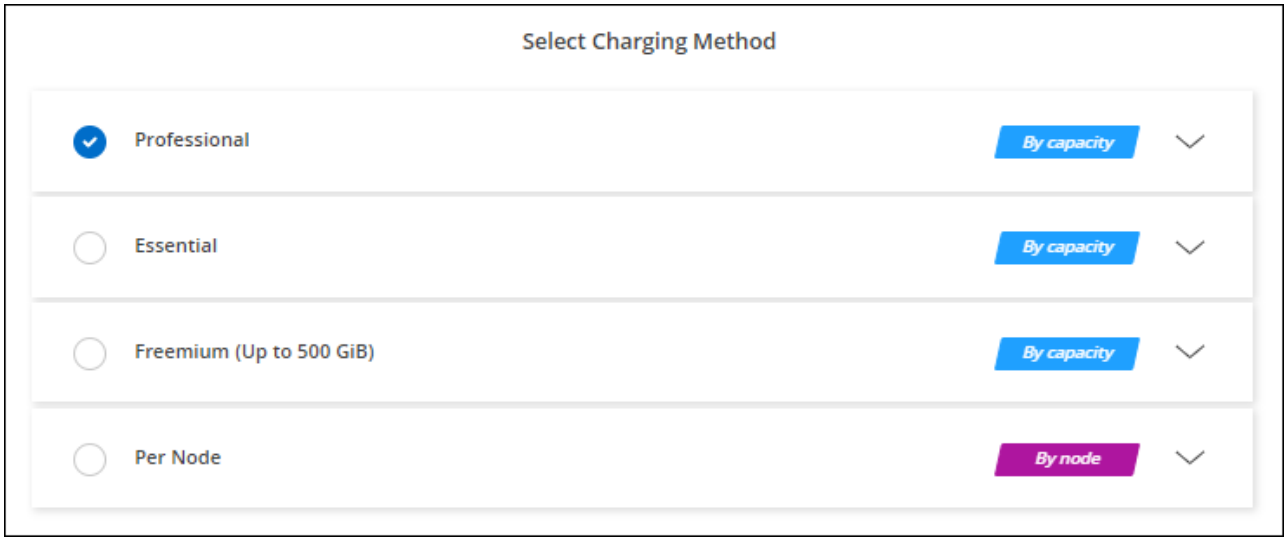
られます。このサブスクリプションは、充電のための作業環境に関連付けられます。同じサブスクリプションを追加の作業環境に使用できます。

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。



   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。



"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。

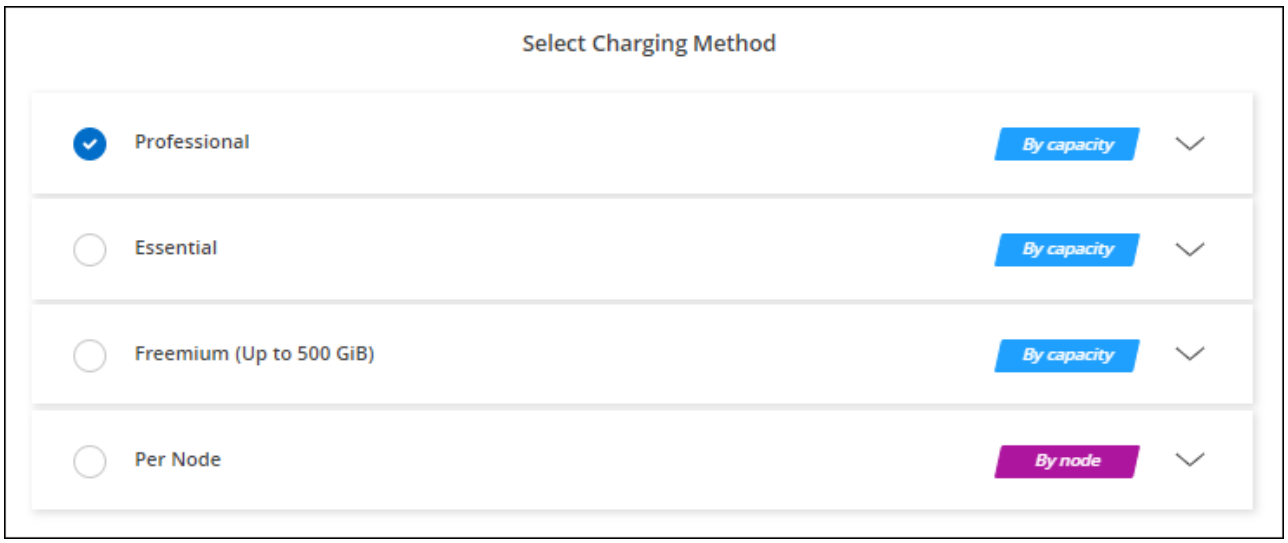
手順

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。



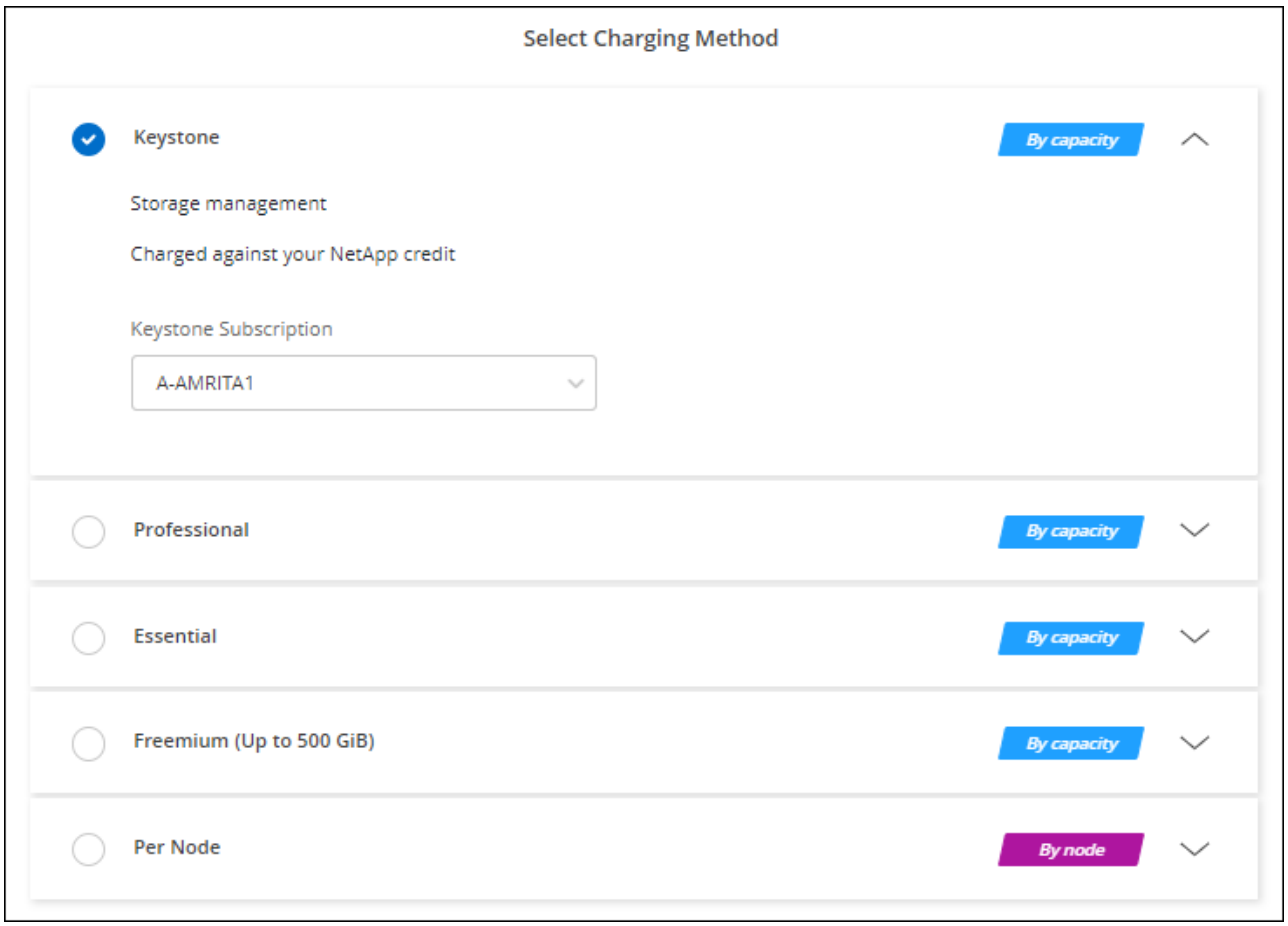
"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

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。



"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-

ontap//media/video_subscribing_azure.mp4 *(video)*

5. * サービス *: サービスを有効にしておくか、 Cloud Volumes ONTAP で使用しない個々のサービスを無効にします。
   - "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。

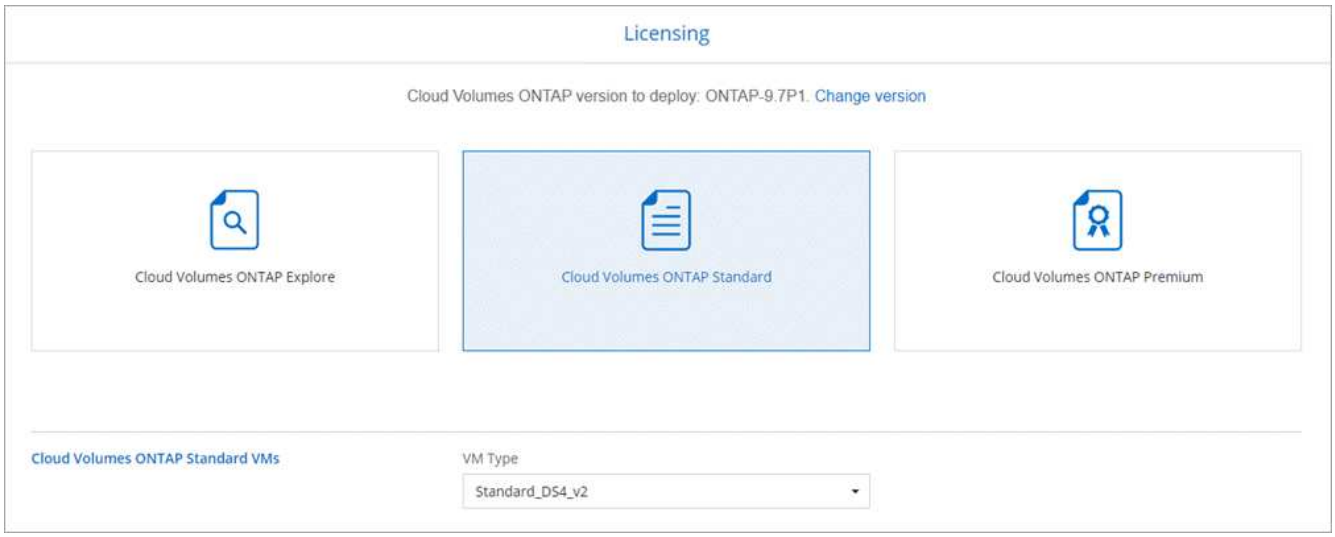
   次の表では、ガイダンスが必要なフィールドについて説明します。

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

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 からサブスクライブ * ： 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す。
    - 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。

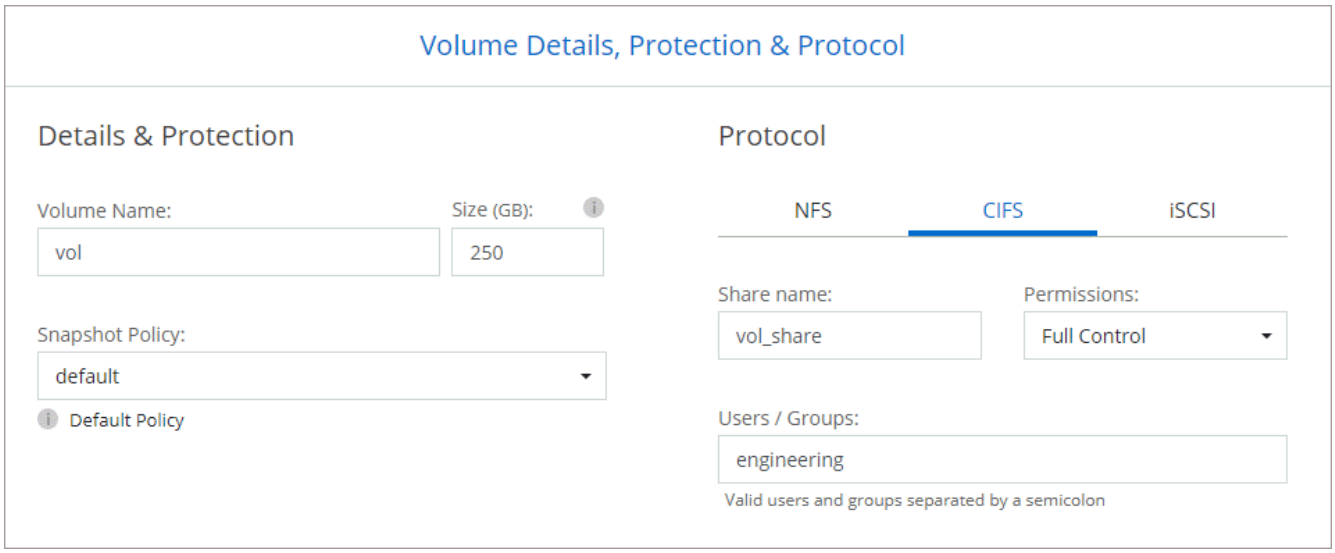
    "サポートされるクライアントプロトコルおよびバージョンについて説明します"。

    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 とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。
スナップショットポリシー	Snapshot コピーポリシーは、自動的に作成される NetApp Snapshot コピーの頻度と数を指定します。NetApp Snapshot コピーは、パフォーマンスに影響を与えず、ストレージを最小限に抑えるポイントインタイムファイルシステムイメージです。デフォルトポリシーを選択することも、なしを選択することもできます。一時データには、 Microsoft SQL Server の tempdb など、 none を選択することもできます。
アドバンストオプション（ NFS のみ）	ボリュームの NFS バージョンを NFSv3 または NFSv4 のいずれかで選択してください。

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



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 サーバを参加させる Active Directory （ AD ）ドメインの FQDN 。
ドメインへの参加を許可されたクレデンシャル	AD ドメイン内の指定した組織単位（ OU ）にコンピュータを追加するための十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。

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

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

    詳細については、を参照してください "ボリューム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。
    a. 設定の詳細を確認します。
    b. 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。
    c. [* I understand … * （理解しています … * ）] チェックボックスを選択
    d. [Go*] をクリックします。

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。

著作権情報

商標情報