



# Microsoft Azure で利用を開始しましょう

## Cloud Volumes ONTAP

NetApp  
May 28, 2024

# 目次

Microsoft Azure で利用を開始しましょう .....	1
Azure での Cloud Volumes ONTAP のクイックスタート .....	1
AzureでCloud Volumes ONTAP 構成を計画 .....	2
Azure の Cloud Volumes ONTAP のネットワーク要件 .....	5
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 .....	14
AzureでCloud Volumes ONTAP のライセンスをセットアップする .....	18
Azureでハイアベイラビリティモードを有効にします .....	25
Azure で Cloud Volumes ONTAP を起動します .....	26

# 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。

1

コネクタを作成します

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"](#)

インターネットアクセスを使用できないサブネットに Cloud Volumes ONTAP を導入する場合は、コネクタを手動でインストールし、そのコネクタで実行されている BlueXP ユーザーインターフェイスにアクセスする必要があります。 ["インターネットにアクセスできない場所にコネクタを手動でインストールする方法について説明します"](#)

2

構成を計画

BlueXP では、ワークロード要件に合わせて事前設定されたパッケージを提供しています。また、独自の構成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。"](#)

3

ネットワークをセットアップします

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 VPC からのアウトバウンドのインターネットアクセスを NetApp AutoSupport で有効にします。

インターネットにアクセスできない場所に Cloud Volumes ONTAP を導入する場合は、この手順は必要ありません。

["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"](#)。

4

BlueXP を使用して Cloud Volumes ONTAP を起動します

[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

- ["BlueXP からコネクタを作成しています"](#)
- ["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"](#)
- ["BlueXP が権限を持って実行できること"](#)

# 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」"](#)

## シングルノードシステムのAzure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。

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。)

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HAペア構成のディスクタイプ

HAシステムでは、Premium SSD Shared Managed Disksを使用して、I/O負荷の高いワークロードのパフォーマンスを高コストで実現します。9.12.1リリースより前に作成されたHA配置では、Premiumページブロブが使用されます。

## 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。BlueXPでは、このディスクサイズを最初のアグリゲート、およびシンプルなプロビジョニングオプションを使用したときに作成される追加のアグリゲートに使用します。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、BlueXP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

BlueXPでは、Cloud Volumes ONTAP の書き込み速度設定を選択できます。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。BlueXPでボリュームを作成するときに、これらの機能を有効にするプロファイル、または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。

## 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 ノードには、NetApp AutoSupport へのアウトバウンドインターネットアクセスが必要です。ネットアップは、システムの健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。

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

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

AutoSupport メッセージの送信にアウトバウンドのインターネット接続が使用できない場合、Cloud Volumes ONTAP システムは自動的にコネクタをプロキシサーバとして使用するよう設定されます。唯一の要件は、コネクタのセキュリティグループがポート3128で\_inbound\_connectionsを許可することです。コネクタを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAP に厳密なアウトバウンドルールを定義した場合は、Cloud Volumes ONTAP セキュリティグループがポート3128で\_OUTBOUND接続を許可する必要があります。

アウトバウンドのインターネットアクセスが使用可能であることを確認したら、AutoSupport をテストしてメッセージを送信できることを確認します。手順については、を参照してください ["ONTAP のドキュメント：「AutoSupport のセットアップ」](#)。

AutoSupport メッセージを送信できないことがBlueXPから通知された場合は、["AutoSupport 構成のトラブルシューティングを行います"](#)。

### IP アドレス

BlueXPは、必要な数のプライベートIPアドレスを自動的にAzureのCloud Volumes ONTAP に割り当てます。ネットワークに利用可能な十分な数のプライベートIPアドレスがあることを確認する必要があります。

Cloud Volumes ONTAP 用に割り当てられるLIFの数は、シングルノードシステムとHAペアのどちらを導入するかによって異なります。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。



iSCSI LIFは、iSCSIプロトコルを介したクライアントアクセスを提供し、システムがその他の重要なネットワークワークフローに使用します。これらのLIFは必須であり、削除しないでください。

## シングルノードシステムの IP アドレス

BlueXPは1つのノードシステムに5つまたは6つのIPアドレスを割り当てます

- クラスタ管理IP
- ノード管理IP
- SnapMirror用のクラスタ間IP
- NFS / CIFS IP
- iSCSI IP



iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- SVMの管理（オプション-デフォルトでは設定されていません）

## HA ペアの IP アドレス

BlueXPでは、導入時に1ノードあたり4 NICにIPアドレスが割り当てられています。

BlueXPでは、HAペアに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には作成されません。

- NIC0 \*
- ノード管理IP
- クラスタ間IP
- iSCSI IP



iSCSI IPは、iSCSIプロトコルを使用したクライアントアクセスを提供します。システムでは、その他の重要なネットワークワークフローにも使用されます。このLIFは必須であり、削除することはできません。

- NIC1 \*
- クラスタネットワークIP
- NIC2 \*
- クラスタインターコネクトIP (HA IC)

## NIC3

- Pageblob NIC IP (ディスクアクセス)



NIC3は、ページBLOBストレージを使用するHA環境にのみ適用できます。

上記のIPアドレスは、フェイルオーバーイベントの際に移行されません。

また、4つのフロントエンドIP (FIPS) がフェイルオーバーイベント時に移行するように設定されています。これらのフロントエンドIPはロードバランサに存在します。



- クラスタ管理IP
- nodeAデータIP (NFS / CIFS)
- nodeBデータIP (NFS / CIFS)
- SVM管理IP

## Azure サービスへのセキュアな接続

BlueXPでは、Cloud Volumes ONTAP とAzureページBLOBストレージアカウント間の接続用にAzure Private Linkがデフォルトで有効になっています。

ほとんどの場合、必要な操作は何もありません。BlueXP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。また、Azureのコネクタの場所に関する要件も把握しておく必要があります。

ビジネスニーズに応じて、プライベートリンク接続を無効にすることもできます。リンクを無効にすると、Cloud Volumes ONTAP はサービスエンドポイントを使用するように設定されます。

"[AzureプライベートリンクまたはサービスエンドポイントでCloud Volumes ONTAP を使用方法の詳細については、こちらをご覧ください](#)".

## 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、接続の問題が発生します。

## セキュリティグループのルール

BlueXPでは、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を含むAzureセキュリティグループが作成されます。テスト目的または独自のセキュリティグループを使用す

る場合は、ポートを参照してください。

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。



コネクタに関する情報をお探しですか？ ["コネクタのセキュリティグループルールを表示します"](#)

#### シングルノードシステムのインバウンドルール

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択したVNetのみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- \*すべてのVNet\*：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。

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	コネクタへの接続と、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

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
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
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 を任意のみに設定します	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

作業環境を作成し、事前定義されたセキュリティグループを選択する場合、次のいずれかの範囲内でトラフィックを許可するように選択できます。

- 選択した**VNet**のみ：インバウンドトラフィックのソースは、Cloud Volumes ONTAP システムのVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。
- \*すべてのVNet\*：インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲です。



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	コネクタへの接続と、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
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 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

#### 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)
	TCP	3128	ノード管理 LIF	コネクタ	アウトバウンドのインターネット接続が使用できない場合に、コネクタのプロキシサーバを介して AutoSupport メッセージを送信する
構成のバックアップ	HTTP	80	ノード管理 LIF	http://<connector-IP-address>/occm/offboxconfig	構成バックアップをコネクタに送信します。" <a href="#">構成バックアップファイルについて説明します</a> "。
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

コネクタをまだ作成していない場合は、コネクタのネットワーク要件も確認してください。

- "[コネクタのネットワーク要件を確認します](#)"
- "[Azureのセキュリティグループルール](#)"

# 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. BlueXP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

BlueXPではディスク暗号化セットを使用します。これにより、ページブロブではなく管理対象ディスクを使用して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。下位バージョンでは、顧客管理キーの代わりにMicrosoft管理キーが使用されます。

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。

Cloud Volumes ONTAP 構成	キーの暗号化に使用されるシステムディスク	キーの暗号化に使用されるデータディスク
シングルノード	<ul style="list-style-type: none"><li>• ブート</li><li>• コア</li><li>• NVRAM</li></ul>	<ul style="list-style-type: none"><li>• root</li><li>• データ</li></ul>
ページBLOBを含むAzure HA単一 アベイラビリティゾーン	<ul style="list-style-type: none"><li>• ブート</li><li>• コア</li><li>• NVRAM</li></ul>	なし



Cloud Volumes ONTAP 構成	キーの暗号化に使用されるシステムディスク	キーの暗号化に使用されるデータディスク
共有管理対象ディスクを使用する Azure HA 単一アベイラビリティゾーン	<ul style="list-style-type: none"> <li>• ブート</li> <li>• コア</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• root</li> <li>• データ</li> </ul>
Azure HA：共有管理対象ディスクを使用する複数のアベイラビリティゾーン	<ul style="list-style-type: none"> <li>• ブート</li> <li>• コア</li> <li>• NVRAM</li> </ul>	<ul style="list-style-type: none"> <li>• root</li> <li>• データ</li> </ul>

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。作成時にストレージアカウントを暗号化する場合は、CVO作成要求でリソースのIDを作成して指定する必要があります。これは、すべてのタイプの導入に当てはまります。提供しない場合でもストレージアカウントは暗号化されますが、BlueXPはまずMicrosoftが管理するキー暗号化を使用してストレージアカウントを作成し、次にストレージアカウントを更新してお客様が管理するキーを使用するようにします。

## ユーザーが割り当てた管理IDを作成します

ユーザーが割り当てた管理IDと呼ばれるリソースを作成することもできます。これにより、Cloud Volumes ONTAP作業環境の作成時にストレージアカウントを暗号化できます。キーボールドを作成してキーを生成する前に、このリソースを作成することをお勧めします。

リソースのIDは次のとおりです。 `userassignedidentity`。

### 手順

1. Azureで、Azureサービスに移動し、\* Managed Identities \*を選択します。
2. [作成 (Create)] をクリックします。
3. 次の詳細を入力します。
  - サブスクリプション: サブスクリプションを選択します。コネクタサブスクリプションと同じサブスクリプションを選択することをお勧めします。
  - リソースグループ: 既存のリソースグループを使用するか、新しいリソースグループを作成します。
  - リージョン: 必要に応じて、コネクタと同じリージョンを選択します。
  - 名前: リソースの名前を入力します。
4. 必要に応じて、タグを追加します。
5. [作成 (Create)] をクリックします。

## キーボールドを作成し、キーを生成します

キーボールドは、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。

あなたの場合 **ユーザーが割り当てた管理IDを作成しました**、キーボールドの作成時に、キーボールドのアクセスポリシーも作成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 \* (シングルノードシステムの場合、または複数のゾーンのHAペアの場合)
- ユーザーが割り当てた管理IDを作成した場合は、次のオプションを有効にする必要があります。
  - バックアップアクセスポリシー

### 2. バックアップアクセスポリシーを選択した場合は、[作成]をクリックしてキーバックアップのアクセスポリシーを作成します。そうでない場合は、手順3に進みます。

#### a. 次の権限を選択します。

- 取得
- リスト
- 復号化します
- 暗号化
- キーのラップを解除します
- ラップキー
- 検証
- サインだ

#### b. ユーザーが割り当てた管理ID (リソース) をプリンシパルとして選択します。

#### c. アクセスポリシーを確認して作成します。

### 3. "キーヴォ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、BlueXP APIを使用してサポートされています。

### 必要な権限

シングルノードのCloud Volumes ONTAP システムで顧客管理キーを使用する場合は、BlueXP Connectorに次

の権限があることを確認します。

```
"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",  
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
```

"権限の最新のリストを表示します"

手順

1. 次のBlueXP 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ボルト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-vs-a/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BlueXP API呼び出しを使用して、ボルト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-vs-a/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BlueXP 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"  
}
```



を含めます "userAssignedIdentity": " userAssignedIdentityId" フィールド: ストレージアカウントの暗号化に使用するリソースを作成した場合。

"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"  
}
```



を含めます "userAssignedIdentity": " userAssignedIdentityId" フィールド: ストレージアカウントの暗号化に使用するリソースを作成した場合。

"この API 呼び出しの詳細を確認してください"。

結果

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. 左側のナビゲーションメニューから、\* Storage > Canvas \*を選択します。
2. キャンバスページで、\*Add Working Environment\*をクリックし、BlueXP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、マーケットプレー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](#)"

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. BlueXPに戻ったら、充電方法のページにアクセスして「\* 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. ["NetApp Support Site アカウントをBlueXPに追加します"](#)

BlueXP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、NetApp Support Site アカウントに関連付けられているライセンスの詳細を取得します。エラーがなければ、BlueXPは自動的にライセンスをデジタルウォレットに追加します。

Cloud Volumes ONTAP でライセンスを使用するには、事前にBlueXPデジタルウォレットからライセンスを入手しておく必要があります。必要に応じて、を実行できます ["ライセンスをBlueXPデジタルウォレットに手動で追加します"](#)。

3. キャンバスページで、\*Add Working Environment\*をクリックし、BlueXP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

Azure Subscription

Marketplace Subscription

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

+ Add Subscription

a. BlueXPに戻ったら、[課金方法]ページにアクセスして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	<input type="button" value="By capacity"/>	▼
<input type="radio"/>	Essential	<input type="button" value="By capacity"/>	▼
<input type="radio"/>	Freemium (Up to 500 GiB)	<input type="button" value="By capacity"/>	▼
<input type="radio"/>	Per Node	<input type="button" value="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. 左側のナビゲーションメニューから、\* Storage > Canvas \*を選択します。
2. キャンバスページで、\*Add Working Environment\*をクリックし、BlueXP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。

**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

- b. BlueXPに戻ったら、[課金方法]ページにアクセスして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 <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Essential	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Freemium (Up to 500 GiB)	By capacity <span style="font-size: 0.8em;">▼</span>
<input type="radio"/>	Per Node	By node <span style="font-size: 0.8em;">▼</span>

"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、\*Add Working Environment\*をクリックし、BlueXP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. BlueXPに戻ったら、[課金方法]ページにアクセスして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	▼

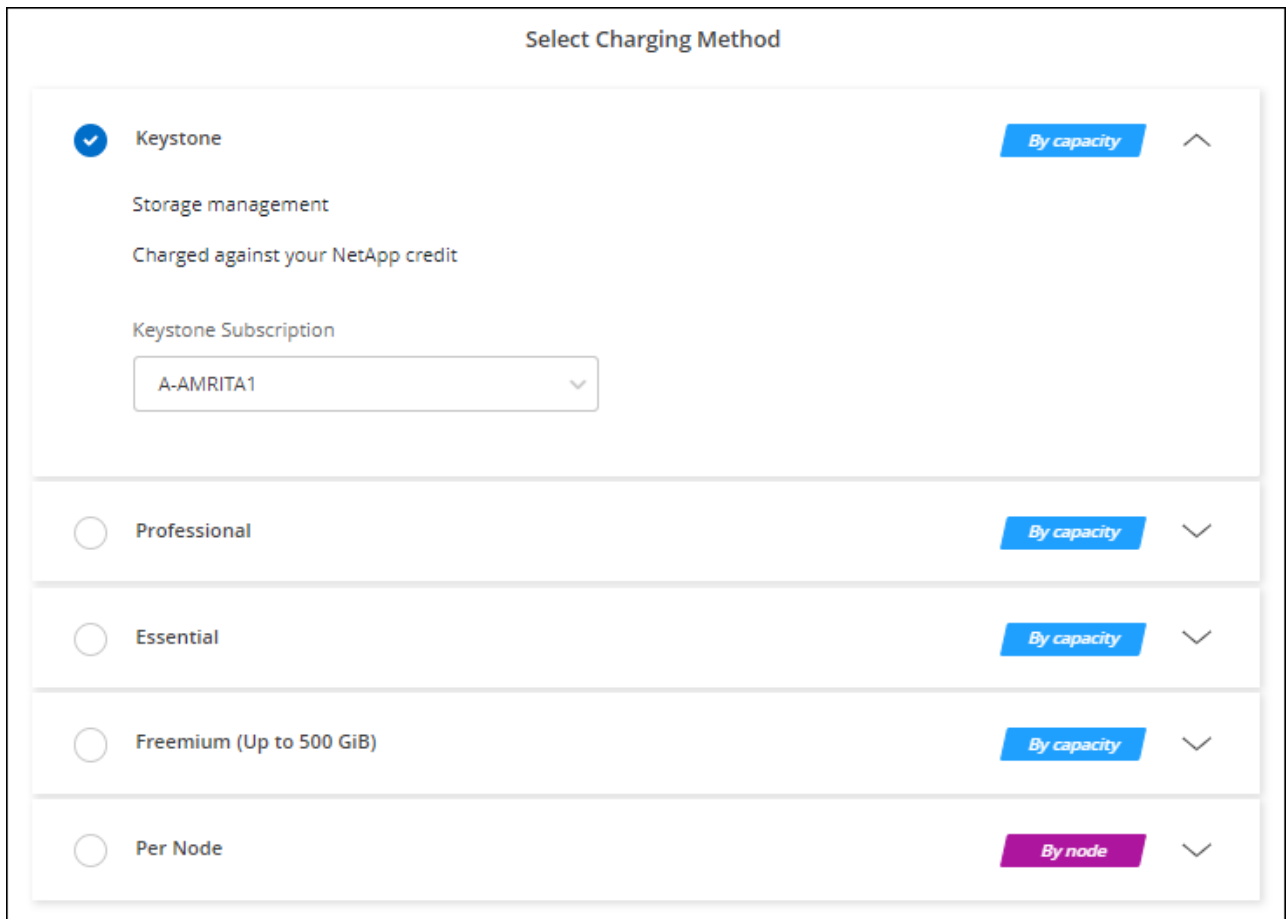
"ステップバイステップの手順を参照して、AzureでCloud Volumes ONTAP を起動してください"。

## Keystoneサブスクリプション

Keystoneサブスクリプションは、ビジネスの成長に応じたサブスクリプションベースのサービスです。  
"NetApp Keystone サブスクリプションの詳細については、こちらをご覧ください"。

### 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サブスクリプションでBlueXPユーザアカウントを承認する場合。
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、\*Add Working Environment\*をクリックし、BlueXPの手順に従います。
  - a. 課金方法を選択するよう求められたら、Keystoneサブスクリプションの課金方法を選択します。



オプションのスクリーンショット。"]

"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でハイアベイラビリティモードを有効にします

Microsoft Azureの高可用性モードを有効にして、計画外のフェイルオーバー時間を短縮し、NFSv4でCloud Volumes ONTAP がサポートされるようにする必要があります。

Cloud Volumes ONTAP 9.10.1リリースから、Microsoft Azureで実行されるCloud Volumes ONTAP HAペアの計画外フェイルオーバー時間が短縮され、NFSv4がサポートされるようになりました。これらの機能拡張をCloud Volumes ONTAP で使用できるようにするには、Azureサブスクリプションでハイアベイラビリティ機能を有効にする必要があります。

Azureサブスクリプションでこの機能を有効にする必要がある場合、「Action Required」メッセージにこれらの詳細が表示されます。

次の点に注意してください。

- Cloud Volumes ONTAP HA ペアの高可用性に問題はありません。この Azure 機能は、ONTAP と連携して動作し、計画外のフェイルオーバーによって発生する NFS プロトコルのアプリケーション停止時間を短縮します。
- この機能を有効にしても、Cloud Volumes ONTAP HA ペアの処理は中断されません。
- Azure サブスクリプションでこの機能を有効にしても、他の VM で原因の問題は発生しません。

「Owner」権限があるAzureユーザは、Azure CLIからこの機能を有効にできます。

手順

1. "Azure PortalからAzure Cloud Shellにアクセスします"
2. ハイアベイラビリティモード機能を登録します。

```
az account set -s AZURE_SUBSCRIPTION_NAME_OR_ID
az feature register --name EnableHighAvailabilityMode --namespace
Microsoft.Network
az provider register -n Microsoft.Network
```

3. 必要に応じて、機能が登録されたことを確認します。

```
az feature show --name EnableHighAvailabilityMode --namespace
Microsoft.Network
```

Azure CLIから次のような結果が返されることを確認します。

```
{
  "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/providers/Microsoft.Features/providers/Microsoft.Network/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

## Azure で Cloud Volumes ONTAP を起動します

BlueXPでCloud Volumes ONTAP 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。

必要なもの

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](#)"。

このタスクについて

BlueXPは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いくつかのAzureオブジェクトを作成します。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。導入に失敗したり削除したりした場合に、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 リソースを削除する可能性があります。

## AzureでのシングルノードCloud Volumes ONTAP システムの起動

AzureでシングルノードのCloud Volumes ONTAP システムを起動する場合は、BlueXPでシングルノードの作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、\* Storage > Canvas \*を選択します。
2. [[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。
3. 場所を選択：「\* Microsoft Azure 」および「 Cloud Volumes ONTAP シングルノード\*」を選択します。
4. プロンプトが表示されたら、"[コネクタを作成します](#)"。
5. \* 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、クラスター名を指定し、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	BlueXPでは、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が付けられます。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。

フィールド	説明
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、ユーザー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 " <a href="#">Microsoft Azure のドキュメント：「Using tags to organize your Azure resources」</a> "。
ユーザ名とパスワード	Cloud Volumes ONTAP クラスター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。 " <a href="#">クレデンシャルを追加する方法について説明します</a> "。

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합니다。

#### Azure MarketplaceでBlueXPにサブスクライブ

- \* 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。
  - "BlueXPの分類の詳細については、[こちらをご覧ください](#)"
  - "BlueXPのバックアップとリカバリの詳細については、[こちらをご覧ください](#)"



WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバ리를無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

- 場所：リージョン、アベイラビリティゾーン、VNet、およびサブネットを選択し、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。

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、BlueXPによってそのAZが選択されます。

- 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

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
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> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <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 "<a href="#">必要な権限</a>"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。</p> </div>
セキュリティグループが生成されました	<p>BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。</p> <ul style="list-style-type: none"> <li>• 「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。</li> <li>• 「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。</li> </ul>
既存のを使用します	<p>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。 "<a href="#">デフォルトのセキュリティグループを表示します</a>"。</p>

9. \* 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](#)".

10. \* 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。

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



選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1 と 9.10.1 P4 が利用可能になっていれば、更新が実行されます。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。

12. \* Azure Marketplace からサブスクリプション \* : BlueXP 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、このページが表示されます。画面に表示される手順に従います。を参照してください "[Marketplace 製品のプログラムによる導入](#)" を参照してください。

13. \* 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。
- シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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。"](#)

14. \* 書き込み速度とWORM \* :

- a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

["書き込み速度の詳細については、こちらをご覧ください。"](#)

- b. 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。

このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください ["HAペアのライセンスでサポートされる構成"](#)。

Cloud Volumes ONTAP 9.7以前のバージョンで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。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

["WORM ストレージの詳細については、こちらをご覧ください。"](#)

- a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

15. \* 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。



フィールド	説明
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、BlueXPはサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
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。
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、BlueXPによって自動的にLUNが作成されます。ボリュームごとに1つのLUNだけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、"IQN を使用して、から LUN に接続します ホスト"。

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:

i Default Policy

#### Protocol

NFS   
 CIFS   
 iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

16. \* 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。
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 <a href="#">"BlueXP自動化ドキュメント"</a> 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。

17. \* 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"](#)。

18. \* 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、BlueXPが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。

## 結果

BlueXPがCloud Volumes ONTAP システムを導入しました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。

## AzureでのCloud Volumes ONTAP HAペアの起動

AzureでCloud Volumes ONTAP HAペアを起動するには、BlueXPでHA作業環境を作成する必要があります。

手順

1. 左側のナビゲーションメニューから、\* Storage > Canvas \*を選択します。
2. [[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。
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	BlueXPでは、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が付けられます。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 " <a href="#">Microsoft Azure のドキュメント：「Using tags to organize your Azure resources」</a> "。
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。 " <a href="#">クレデンシャルを追加する方法について説明します</a> "。

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합니다。

[Azure MarketplaceでBlueXPにサブスクリライブ](#)


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。
- "BlueXPの分類の詳細については、こちらをご覧ください"
  - "BlueXPのバックアップとリカバリの詳細については、こちらをご覧ください"



WORMとデータ階層化を活用する場合は、BlueXPのバックアップとリカバリを無効にし、バージョン9.8以降のCloud Volumes ONTAP 作業環境を導入する必要があります。

6. \* HA導入モデル\* :
- a. 単一アベイラビリティゾーン\*または\*複数のアベイラビリティゾーン\*を選択します。
  - b. 場所と接続 (単一AZ) および\*地域と接続\* (複数のAZ)
    - 単一のAZの場合は、リージョン、VNet、およびサブネットを選択します。
    - 複数のAZについて、リージョン、VNet、サブネット、ノード1のゾーン、およびノード2のゾーンを選択します。
  - c. [ネットワーク接続を検証しました...]\*]チェックボックスを選択します。
7. 接続性:新しいリソースグループまたは既存のリソースグループを選択し、事前定義されたセキュリティグループを使用するか、独自のリソースグループを使用するかを選択します。

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
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、接続の問題が発生します。</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <p>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 "<a href="#">必要な権限</a>"では、展開に失敗したり削除されたりした場合、Cloud Volumes ONTAP リソースがリソースグループから削除されます。</p> </div>

フィールド	説明
セキュリティグループが生成されました	<p>BlueXPがセキュリティグループを生成するようにした場合は、トラフィックを許可する方法を選択する必要があります。</p> <ul style="list-style-type: none"> <li>「選択したVNetのみ」を選択した場合のインバウンドトラフィックのソースは、選択したVNetのサブネット範囲およびコネクタが存在するVNetのサブネット範囲です。これが推奨されるオプションです。</li> <li>「すべてのVNet *」を選択した場合、インバウンドトラフィックの送信元は0.0.0.0/0のIP範囲になります。</li> </ul>
既存のを使用します	<p>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。 <a href="#">"デフォルトのセキュリティグループを表示します"</a>。</p>

8. \* 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"](#)。

9. 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、\* 構成の変更\*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。

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



選択したバージョンで新しいリリース候補、一般提供、またはパッチリリースが利用可能な場合、作業環境の作成時に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 9.10.1と9.10.1 P4が利用可能になっていれば、更新が実行されます。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。

11. \* Azure Marketplaceからサブスクリプト\* : BlueXP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。

12. \* 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。

- シンプルなプロビジョニングオプションを使用した場合、ディスクサイズは、初期アグリゲートのすべてのディスクと、BlueXPで作成される追加のアグリゲートのサイズです。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・サイズの選択については、を参照してください ["Azureでシステムのサイズを設定します"](#)。

- 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。"

13. \*書き込み速度とWORM\* :

- a. 必要に応じて、「標準」または「高速」の書き込み速度を選択します。

"書き込み速度の詳細については、こちらをご覧ください。"

- b. 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。

このオプションは、特定のVMタイプに対してのみ使用できます。サポートされるVMタイプについては、を参照してください "[HAペアのライセンスでサポートされる構成](#)".

Cloud Volumes ONTAP 9.7以前のバージョンで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。Cloud Volumes ONTAP 9.8へのリバートまたはダウングレードは、WORMと階層化を有効にしたあとはブロックされます。

"WORM ストレージの詳細については、こちらをご覧ください。"

- a. WORMストレージをアクティブ化する場合は、保持期間を選択します。

14. ストレージと**WORM**へのセキュアな通信：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化します。

HTTPS接続は、Cloud Volumes ONTAP 9.7のHAペアからAzureページBLOBストレージアカウントに確立されます。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。

"WORM ストレージの詳細については、こちらをご覧ください。"

データの階層化が有効になっていると、WORM を有効にできません。

"WORM ストレージの詳細については、こちらをご覧ください。"

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

フィールド	説明
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。
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、BlueXPによって自動的にLUNが作成されます。ボリュームごとに1つのLUNだけを作成することでシンプルになり、管理は不要になります。ボリュームを作成したら、 <b>"IQN を使用して、から LUN に接続します ホスト"</b> 。

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 Policy

#### Protocol

NFS   
 CIFS   
 iSCSI

Share name:  Permissions:

Users / Groups:

Valid users and groups separated by a semicolon

16. \* 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。
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。 <a href="https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou">https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou</a> ["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 <a href="#">"BlueXP自動化ドキュメント"</a> 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。

17. \* 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 ["ボリュームの使用プロファイルを選択してください"](#) および ["データ階層化の概要"](#)。

18. \* 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、BlueXPが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。

## 結果

BlueXPがCloud Volumes ONTAP システムを導入しました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。

## 著作権に関する情報

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

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

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

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

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

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

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

## 商標に関する情報

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