



Microsoft Azureを使い始める Cloud Volumes ONTAP

NetApp
February 17, 2026

This PDF was generated from <https://docs.netapp.com/ja-jp/storage-management-cloud-volumes-ontap/concept-azure-mktplace-direct.html> on February 17, 2026. Always check docs.netapp.com for the latest.

目次

Microsoft Azureを使い始める	1
Azure でのCloud Volumes ONTAP の展開オプションについて学習します	1
NetApp Consoleで始める	2
Azure でのCloud Volumes ONTAPのクイック スタート	2
AzureでCloud Volumes ONTAPの構成を計画する	3
Cloud Volumes ONTAP用の Azure ネットワークを設定する	6
Azureで顧客管理キーを使用するようにCloud Volumes ONTAPを設定する	17
AzureでCloud Volumes ONTAPのライセンスを設定する	21
AzureでCloud Volumes ONTAPの高可用性モードを有効にする	28
Azure でCloud Volumes ONTAPの VMOrchestratorZonalMultiFD を有効にする	30
AzureでCloud Volumes ONTAPを起動する	31
Azure プラットフォーム イメージの検証	43
AzureマーケットプレイスからCloud Volumes ONTAPをデプロイする	55
デプロイメントの問題のトラブルシューティング	58
コンソールで展開されたシステムを検出する	58

Microsoft Azureを使い始める

Azure でのCloud Volumes ONTAP の展開オプションについて学習します

NetApp は、Azure にCloud Volumes ONTAP を展開するための 2 つのオプションを提供しています。Cloud Volumes ONTAP は従来、導入とオーケストレーションにNetApp Consoleに依存しています。Cloud Volumes ONTAP 9.16.1 以降では、Azure マーケットプレイスの直接展開を利用できます。これは、制限はあるものの強力なCloud Volumes ONTAP の機能とオプションのセットへのアクセスを提供する合理化されたプロセスです。

Azure マーケットプレイスからCloud Volumes ONTAP を直接デプロイする場合は、コンソール エージェントをセットアップしたり、コンソール経由でCloud Volumes ONTAP をデプロイするために必要なその他のセキュリティおよびオンボーディング基準を満たしたりする必要はありません。Azure マーケットプレイスでは、数回クリックするだけでCloud Volumes ONTAPを迅速に導入し、そのコア機能と機能を自分の環境で試すことができます。

Azure マーケットプレイスでのデプロイが完了すると、コンソールでこれらのシステムを検出できるようになります。検出後は、Cloud Volumes ONTAPシステムとして管理し、コンソールのすべての機能を利用できます。。"[コンソールで展開されたシステムを検出する](#)"。

以下は 2 つのオプションの機能比較です。Azure マーケットプレイスを通じてデプロイされたスタンドアロン インスタンスの機能は、コンソールで検出された時点で変更されることに注意してください。

	Azureマーケットプレイス	NetApp Console
オンボーディング	より短く、より簡単で、直接導入に必要な準備は最小限	コンソールエージェントのインストールを含む、オンボーディングプロセスが長くなります
サポートされている仮想マシン (VM) の種類	Eds_v5 および Ls_v3 インスタンスタイプ	あらゆる種類の VM タイプ。 https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html ["Azureでサポートされている構成"]
ライセンス	無料ライセンス	任意の容量ベースのライセンス。 "Cloud Volumes ONTAPライセンス"
* NetAppサポート*	含まれません	ライセンスの種類に応じて利用可能
容量	500 GiB以下	構成により拡張可能
展開モデル	単一のアベイラビリティゾーン (AZ) での高可用性 (HA) モードの展開	単一ノードおよび HA モード、単一および複数の AZ 展開を含む、サポートされているすべての構成
サポートされているディスクタイプ	プレミアム SSD v2 マネージド ディスク	より幅広いサポート。 "Cloud Volumes ONTAPのデフォルト設定"

	Azureマーケットプレイス	NetApp Console
書き込み速度（高速書き込みモード）	サポート対象外	構成に基づいてサポートされます。 "Cloud Volumes ONTAPの書き込み速度について" 。
オーケストレーション機能	使用不可	ライセンスの種類に応じてNetApp Consoleから利用可能
サポートされるストレージVMの数	展開ごとに1つ	構成に基づいた複数のストレージ VM。 "サポートされるストレージVMの数"
インスタンスタイプの変更	サポート対象外	サポート
* FabricPool の階層化*	サポート対象外	サポート

関連リンク

- Azure マーケットプレイスの直接展開:["AzureマーケットプレイスからCloud Volumes ONTAPをデプロイする"](#)
- コンソール経由のデプロイメント:["Azure でのCloud Volumes ONTAPのクイック スタート"](#)
- ["NetApp Consoleのドキュメント"](#)

NetApp Consoleで始める

Azure でのCloud Volumes ONTAPのクイック スタート

数ステップでCloud Volumes ONTAP for Azure を使い始めましょう。

1

コンソールエージェントを作成する

もしあなたが ["コンソールエージェント"](#) まだ作成する必要があります。 ["Azure でコンソール エージェントを作成する方法を学びます"](#)

インターネット アクセスが利用できないサブネットにCloud Volumes ONTAPを展開する場合は、コンソールエージェントを手動でインストールし、そのコンソール エージェントで実行されているNetApp Consoleにアクセスする必要があることに注意してください。 ["インターネットにアクセスできない場所にコンソールエージェントを手動でインストールする方法を学びます"](#)

2

構成を計画する

コンソールでは、ワークロード要件に一致する事前構成済みのパッケージが提供されており、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。詳細については、["AzureでCloud Volumes ONTAPの構成を計画する"](#)。

3

ネットワークを設定する

1. VNet とサブネットがコンソール エージェントとCloud Volumes ONTAP間の接続をサポートすることを確認します。

2. NetApp AutoSupportのターゲット VPC 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を展開する場合、この手順は必要ありません。

["ネットワーク要件の詳細"](#)。



Cloud Volumes ONTAPを起動する

*システムの追加*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完了します。"[ステップバイステップの説明を読む](#)"。

関連リンク

- ["コンソールからコンソールエージェントを作成する"](#)
- ["Azure Marketplace からコンソール エージェントを作成する"](#)
- ["Linuxホストにコンソールエージェントソフトウェアをインストールする"](#)
- ["コンソールが権限を使って行うこと"](#)

AzureでCloud Volumes ONTAPの構成を計画する

Azure にCloud Volumes ONTAP をデプロイする場合、ワークロード要件に一致する事前構成済みのシステムを選択することも、独自の構成を作成することもできます。独自の構成を選択する場合は、利用可能なオプションを理解する必要があります。

Cloud Volumes ONTAPライセンスを選択する

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。各オプションにより、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学ぶ"](#)
- ["ライセンスの設定方法を学ぶ"](#)

サポートされている地域を選択してください

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地域の完全なリストを見る](#)"。

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 は、選択したライセンス タイプに応じて、いくつかの VM タイプをサポートします。

["Azure でサポートされるCloud Volumes ONTAPの構成"](#)

ストレージ制限を理解する

Cloud Volumes ONTAPシステムの生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。構成を計画する際には、これらの制限に注意する必要があります。

"Azure のCloud Volumes ONTAPのストレージ制限"

Azure でシステムのサイズを決定する

Cloud Volumes ONTAPシステムのサイズを設定すると、パフォーマンスと容量の要件を満たすことができます。VM タイプ、ディスク タイプ、ディスク サイズを選択する際には、いくつかの重要なポイントに注意する必要があります。

仮想マシンの種類

サポートされている仮想マシンの種類については、"[Cloud Volumes ONTAPリリースノート](#)"次に、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 タイプは特定の数のデータ ディスクをサポートすることに注意してください。

- "[Azure ドキュメント: 汎用仮想マシンのサイズ](#)"
- "[Azure ドキュメント: メモリ最適化された仮想マシンのサイズ](#)"

単一ノード システムの Azure ディスク タイプ

Cloud Volumes ONTAPのボリュームを作成するときは、Cloud Volumes 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。

単一ノード システムでは、次の種類の Azure マネージド ディスクを使用できます：

- *Premium SSD* マネージド ディスク は、コストは高くなりますが、I/O 集中型のワークロードに高いパフォーマンスを提供します。
- *Premium SSD v2* マネージド ディスク は、Premium SSD マネージド ディスクと比較して、より低いレイテンシでより高いパフォーマンスを低コストで提供します。
- *Standard SSD Managed Disks* は、低い IOPS を必要とするワークロードに対して一貫したパフォーマンスを提供します。
- 高い IOPS を必要とせず、コストを削減したい場合は、*Standard HDD Managed Disks* が適しています。

これらのディスクの使用例の詳細については、以下を参照してください。"[Microsoft Azure ドキュメント: Azure ではどのようなディスク タイプが使用できますか?](#)"。

HA ペアを備えた Azure ディスク タイプ

HA システムでは、プレミアム SSD 共有マネージド ディスクが使用されます。どちらも、コストは高くなりますが、I/O 集中型のワークロードに対して高いパフォーマンスを提供します。9.12.1 リリースより前に作成された HA デプロイメントでは、Premium ページ BLOB が使用されます。

Azure 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。NetApp Consoleは、初期アグリゲートと、シンプル プロビジョニング オプションを使用するときに作成される追加のアグリゲートにこのディスク サイズを使用します。デフォルトとは異なるディスクサイズを使用するアグリゲートを作成するには、"[高度な割り当てオプションを使用する](#)"。



アグリゲート内のすべてのディスクは同じサイズである必要があります。

ディスク サイズを選択するときは、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

レージに支払う金額、アグリゲートで作成できるボリュームのサイズ、Cloud Volumes ONTAPで使用できる合計容量、およびストレージ パフォーマンスに影響します。

Azure Premium Storage のパフォーマンスはディスク サイズに左右されます。ディスクが大きいほど、IOPS とスループットが向上します。たとえば、1 TiB ディスクを選択すると、コストは高くなりますが、500 GiB ディスクよりも優れたパフォーマンスが得られます。

標準ストレージでは、ディスク サイズ間で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: マネージド ディスクの価格"](#)
- ["Microsoft Azure: ページ BLOB の価格"](#)

デフォルトのシステムディスクを表示する

コンソールは、ユーザー データ用のストレージに加えて、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。計画のために、Cloud Volumes ONTAP を展開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 のCloud Volumes ONTAPシステム データのデフォルト ディスクを表示する"](#)。



コンソール エージェントにはシステム ディスクも必要です。 ["コンソールエージェントのデフォルト構成の詳細を表示する"](#)。

ネットワーク情報を収集する

Azure にCloud Volumes ONTAPをデプロイする場合は、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情報	あなたの価値
リージョン	
仮想ネットワーク (VNet)	
サブネット	
ネットワーク セキュリティ グループ (独自のものを使用している場合)	

書き込み速度を選択する

コンソールでは、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、標準設定と高速設定の違い、および高速書き込み速度を使用する場合のリスクと推奨事項を理解しておく必要があります。 ["書き込み速度について詳しくはこちら"](#)。

ボリューム使用プロファイルを選択する

ONTAPには、必要なストレージの総量を削減できるいくつかのストレージ効率機能が含まれています。コンソール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。どのプロファイルを使用するかを決めるには、これらの機能について詳しく理解する必要があります。

NetAppストレージ効率機能には、次のような利点があります。

シンプロビジョニング

物理ストレージ プールに実際に存在するよりも多くの論理ストレージをホストまたはユーザーに提供します。ストレージ スペースを事前に割り当てるのではなく、データが書き込まれるときに各ボリュームにストレージ スペースが動的に割り当てられます。

重複排除

同一のデータ ブロックを見つけて、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。この手法は、同じボリューム内に存在する冗長なデータ ブロックを排除することで、ストレージ容量の要件を削減します。

圧縮

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

Cloud Volumes ONTAP用の Azure ネットワークを設定する

NetApp Consoleは、IP アドレス、ネットマスク、ルートなどのCloud Volumes ONTAPのネットワーク コンポーネントのセットアップを処理します。アウトバウンドのインターネット アクセスが利用可能であること、十分なプライベート IP アドレスが利用可能であること、適切な接続が確立されていることなどを確認する必要があります。

Cloud Volumes ONTAPの要件

Azure では次のネットワーク要件を満たす必要があります。

アウトバウンドインターネットアクセス

Cloud Volumes ONTAPシステムでは、さまざまな機能の外部エンドポイントにアクセスするために、アウトバウンド インターネット アクセスが必要です。厳格なセキュリティ要件を持つ環境でこれらのエンドポイントがブロックされている場合、Cloud Volumes ONTAP は正常に動作しません。

コンソール エージェントは、日常的な操作のために複数のエンドポイントにも接続します。エンドポイントの詳細については、以下を参照してください。 ["コンソールエージェントから接続されたエンドポイントを表示する"](#)そして ["コンソールを使用するためのネットワークの準備"](#)。

Cloud Volumes ONTAPエンドポイント

Cloud Volumes ONTAP はこれらのエンドポイントを使用してさまざまなサービスと通信します。

エンドポイント	適用対象	目的	展開モード	利用できない場合の影響
https://netapp-cloud-account.auth0.com	認証	コンソールでの認証に使用されます。	標準モードと制限モード。	ユーザー認証が失敗し、次のサービスは利用できなくなります。 • Cloud Volumes ONTAPサービス • ONTAPサービス • プロトコルとプロキシサービス
https://vault.azure.net	キーバールト	カスタマー マネージド キー (CMK) を使用するとき、Azure Key Vault からクライアント シークレット キーを取得するために使用されます。	標準、制限、プライベートのモード。	Cloud Volumes ONTAPサービスは利用できません。
https://api.blueexp.net/app.com/tenancy	賃貸借	コンソールからCloud Volumes ONTAPリソースを取得して、リソースとユーザーを承認するために使用されます。	標準モードと制限モード。	Cloud Volumes ONTAPリソースとユーザーは承認されていません。
https://mysupport.netapp.com/aods/asupmessage https://mysupport.netapp.com/asupprod/post/1.0/postAsup	AutoSupport	AutoSupportテレメトリ データをNetAppサポートに送信するために使用されます。	標準モードと制限モード。	AutoSupport情報は未配信のままです。
https://management.azure.com https://login.microsoftonline.com https://bluexpinfraprod.eastus2.data.azurecr.io https://core.windows.net	パブリックリージョン	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。

エンドポイント	適用対象	目的	展開モード	利用できない場合の影響
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	中国地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.microsoftazure.de https://login.microsoftonline.de https://blob.core.cloudapi.de https://core.cloudapi.de	ドイツ地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	政府地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	政府国防総省地域	Azure サービスとの通信。	標準、制限、プライベートのモード。	Cloud Volumes ONTAP は、Azure サービスと通信して Azure のコンソールの特定の操作を実行できません。

NetApp Console エージェントのネットワークプロキシ構成

NetApp Console エージェントのプロキシ サーバー構成を使用して、Cloud Volumes ONTAP からのアウトバウンド インターネット アクセスを有効にすることができます。コンソールは次の 2 種類のプロキシをサポートしています。

- 明示的なプロキシ: Cloud Volumes ONTAP からの送信トラフィックは、コンソール エージェントのプロキシ構成時に指定されたプロキシ サーバーの HTTP アドレスを使用します。管理者は、追加の認証のためにユーザー資格情報とルート CA 証明書を構成している場合もあります。明示的なプロキシにルート CA 証明書が利用可能な場合は、必ず同じ証明書を取得して、Cloud Volumes ONTAP システムにアップロードしてください。"[ONTAP CLI: セキュリティ証明書のインストール](#)" 指示。
- 透過プロキシ: ネットワークは、Cloud Volumes ONTAP からの送信トラフィックをコンソール エージェントのプロキシを介して自動的にルーティングするように構成されています。透過プロキシを設定する場合、管理者はプロキシ サーバーの HTTP アドレスではなく、Cloud Volumes ONTAP からの接続用のルー

ト CA 証明書のみを提供する必要があります。同じルートCA証明書を取得し、Cloud Volumes ONTAP システムにアップロードしてください。"[ONTAP CLI: セキュリティ証明書のインストール](#)"指示。

プロキシサーバーの設定方法については、"[プロキシサーバーを使用するようにコンソールエージェントを構成する](#)"。

IPアドレス

コンソールは、Azure のCloud Volumes ONTAPに必要な数のプライベート IP アドレスを自動的に割り当てます。ネットワークに十分なプライベート IP アドレスが利用可能であることを確認する必要があります。

Cloud Volumes ONTAP に割り当てられる LIF の数は、単一ノード システムを導入するか HA ペア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。SVM 管理 LIF は、SnapCenter などの管理ツールに必要です。



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、システムによって他の重要なネットワーク ワークフローに使用されます。これらの LIF は必須であり、削除しないでください。

単一ノードシステムのIPアドレス

NetApp Console は、単一ノード 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のクラスタ間 IP
- NFS/CIFS IP
- iSCSI IP



iSCSI IP は、iSCSI プロトコルを介したクライアント アクセスを提供します。これは、システムによって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、削除しないでください。

- SVM 管理 (オプション - デフォルトでは構成されていません)

HAペアのIPアドレス

コンソールは、展開中に 4 つの NIC (ノードあたり) に IP アドレスを割り当てます。

NetApp Console は HA ペア上に SVM 管理 LIF を作成しますが、Azure の単一ノード システム上には作成しないことに注意してください。

NIC0

- ノード管理IP
- クラスタ間IP
- iSCSI IP



iSCSI IP は、iSCSI プロトコルを介したクライアント アクセスを提供します。これは、システムによって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、削除しないでください。

NIC1

- クラスターネットワークIP

NIC2

- クラスタ相互接続 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 展開にのみ適用されます。

上記の IP アドレスは、フェールオーバー イベントでは移行されません。

さらに、4 つのフロントエンド IP (FIP) がフェイルオーバー イベント時に移行するように構成されています。これらのフロントエンド IP はロードバランサー内に存在します。

- 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 サービスへの安全な接続

デフォルトでは、コンソールは、Cloud Volumes ONTAPと Azure ページ BLOB ストレージ アカウント間の接続に Azure プライベート リンクを有効にします。

ほとんどの場合、何もする必要はありません。コンソールが Azure Private Link を管理します。ただし、Azure プライベート 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。Azure 内のコンソール エージェントの場所に関する要件にも注意する必要があります。

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、コンソールは代わりにサービス エンドポイントを使用するようにCloud Volumes ONTAPを構成します。

["Cloud Volumes ONTAPで Azure Private Links またはサービス エンドポイントを使用する方法の詳細"](#)。

Azure VNet 暗号化のネットワーク

Cloud Volumes ONTAPは ["Azure Virtual Network \(VNet\) 暗号化"](#)VNet内またはピアリングされたVNet間のVM間トラフィックの暗号化をサポートしています。この機能はAzure VNetレイヤーで設定され、Cloud Volumes ONTAPトポロジ（単一ノードまたはHA）から独立しています。

機能を有効にする前に、VM の NIC で高速ネットワークが有効になっていることを確認し、Azure VNet 暗号化の要件と制限事項を確認するだけで済みます。NetApp 管理対象ロードバランサオブジェクトを変更しない

てください。

["Azure ドキュメント：VNet 暗号化と Accelerated Networking"](#)。

他のONTAPシステムへの接続

Azure のCloud Volumes ONTAPシステムと他のネットワークのONTAPシステム間でデータを複製するには、Azure VNet と他のネットワーク (企業ネットワークなど) の間に VPN 接続が必要です。

手順については、["Microsoft Azure ドキュメント: Azure ポータルでサイト間接続を作成する"](#)。

HA相互接続用のポート

Cloud Volumes ONTAP HA ペアには HA 相互接続が含まれており、これにより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、もう一方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 相互接続は通信に TCP ポート 10006 を使用します。

デフォルトでは、HA 相互接続 LIF 間の通信はオープンであり、このポートにはセキュリティ グループ ルールはありません。ただし、HA 相互接続 LIF 間にファイアウォールを作成する場合は、HA ペアが適切に動作できるように、TCP トラフィックがポート 10006 に対して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 つだけあります

Azure にデプロイする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 グループでは 1 つの HA ペアのみがサポートされます。

Azure リソース グループに 2 番目のCloud Volumes ONTAP HA ペアをデプロイしようとすると、コンソールで接続の問題が発生します。

セキュリティグループルール

コンソールは、Cloud Volumes ONTAP が正常に動作するためのインバウンド ルールとアウトバウンド ルールを含む Azure セキュリティ グループを作成します。["コンソールエージェントのセキュリティグループルールを表示する"](#)。

Cloud Volumes ONTAPの Azure セキュリティ グループでは、ノード間の内部通信用に適切なポートが開いている必要があります。["ONTAPの内部ポートについて学ぶ"](#)。

定義済みのセキュリティ グループを変更したり、カスタム セキュリティ グループを使用することはお勧めしません。ただし、必要な場合は、展開プロセスでCloud Volumes ONTAPシステムが独自のサブネット内でフルアクセス権を持つ必要があることに注意してください。デプロイが完了したら、ネットワーク セキュリティ グループを変更する場合は、クラスター ポートと HA ネットワーク ポートを開いたままにしておいてください。これにより、Cloud Volumes ONTAPクラスター内でのシームレスな通信 (ノード間の any-to-any 通信) が保証されます。

単一ノードシステムの受信ルール

Cloud Volumes ONTAPシステムを追加し、定義済みのセキュリティ グループを選択すると、次のいずれかの範囲内でトラフィックを許可することを選択できます。

- 選択した **VNet** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲です。これは推奨されるオプションです。

- すべての **VNet**: 受信トラフィックのソースは、0.0.0.0/0 IP 範囲です。
- 無効: このオプションは、ストレージ アカウントへのパブリック ネットワーク アクセスを制限し、Cloud Volumes ONTAPシステムのデータ階層化を無効にします。セキュリティ規制やポリシーにより、同じ VNet 内であってもプライベート IP アドレスを公開しない場合は、このオプションが推奨されます。

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
1000 受信SSH	22 TCP	任意対任意	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 インバウンド_http	80 TCP	任意対任意	クラスタ管理LIFのIPアドレスを使用してONTAP System Manager WebコンソールにHTTPアクセスする
1002 inbound_111_tcp	111 TCP	任意対任意	NFS のリモート プロシージャ コール
1003 inbound_111_udp	111 UDP	任意対任意	NFS のリモート プロシージャ コール
1004 inbound_139	139 TCP	任意対任意	CIFSのNetBIOSサービスセッション
1005 受信_161-162_tcp	161-162 TCP	任意対任意	簡易ネットワーク管理プロトコル
1006 受信_161-162_udp	161-162 UDP	任意対任意	簡易ネットワーク管理プロトコル
1007 inbound_443	443 TCP	任意対任意	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP System Manager WebコンソールへのHTTPSアクセス
1008 inbound_445	445 TCP	任意対任意	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
1009 inbound_635_tcp	635 TCP	任意対任意	NFSマウント
1010 inbound_635_udp	635 UDP	任意対任意	NFSマウント
1011 inbound_749	749 TCP	任意対任意	Kerberos
1012 inbound_2049_tcp	2049 TCP	任意対任意	NFSサーバ デーモン
1013 inbound_2049_udp	2049 UDP	任意対任意	NFSサーバ デーモン
1014 inbound_3260	3260 TCP	任意対任意	iSCSI データ LIF を介した iSCSI アクセス
1015 受信_4045-4046_tcp	4045-4046 TCP	任意対任意	NFS ロックデーモンとネットワークステータスマニター

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
1016 受信_4045-4046_udp	4045-4046 UDP	任意対任意	NFS ロックデーモンとネットワークステータスマニター
1017 inbound_10000	10000 TCP	任意対任意	NDMPを使用したバックアップ
1018 着信_11104-11105	11104-11105 TCP	任意対任意	SnapMirrorデータ転送
3000 受信拒否 _all_tcp	任意のポート TCP	任意対任意	その他のTCP受信トラフィックをすべてブロックする
3001 受信拒否 _all_udp	任意のポートUDP	任意対任意	その他のUDP受信トラフィックをすべてブロックする
65000 VnetInBound を許可する	任意のポート 任意のプロトコル	仮想ネットワークから仮想ネットワークへ	VNet 内からの受信トラフィック
65001 Azureロードバランサーの受信を許可する	任意のポート 任意のプロトコル	AzureLoadBalancer から Any	Azure Standard Load Balancer からのデータトラフィック
65500 全受信拒否	任意のポート 任意のプロトコル	任意対任意	その他のすべての受信トラフィックをブロックする

HAシステムの受信ルール

Cloud Volumes ONTAPシステムを追加し、定義済みのセキュリティ グループを選択すると、次のいずれかの範囲内でトラフィックを許可することを選択できます。

- 選択した **VNet** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲です。これは推奨されるオプションです。
- すべての **VNet**: 受信トラフィックのソースは、0.0.0.0/0 IP 範囲です。



HA システムでは、受信データトラフィックが Azure Standard Load Balancer を経由するため、単一ノード システムよりも受信ルールが少なくなります。このため、ロードバランサーからのトラフィックは、「AllowAzureLoadBalancerInBound」ルールに示されているように、開いている必要があります。

- 無効: このオプションは、ストレージ アカウントへのパブリック ネットワーク アクセスを制限し、Cloud Volumes ONTAPシステムのデータ階層化を無効にします。セキュリティ規制やポリシーにより、同じ VNet 内であってもプライベート IP アドレスを公開しない場合は、このオプションが推奨されます。

優先順位と名前	ポートとプロトコル	送信元と送信先	説明
100 inbound_443	443 任意のプロトコル	任意対任意	コンソールエージェントとの接続と、クラスタ管理LIFのIPアドレスを使用したONTAP System Manager WebコンソールへのHTTPSアクセス
101 inbound_111_tcp	111 任意のプロトコル	任意対任意	NFS のリモート プロシージャ コール
102 inbound_2049_tcp	2049 あらゆるプロトコル	任意対任意	NFSサーバ デーモン
111 受信SSH	22 あらゆるプロトコル	任意対任意	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 あらゆるプロトコル	任意対任意	DNSとCIFS
65000 VnetInBound を許可する	任意のポート 任意のプロトコル	仮想ネットワークから仮想ネットワークへ	VNet 内からの受信トラフィック
65001 Azureロードバランサーの受信を許可する	任意のポート 任意のプロトコル	AzureLoadBalancer から Any	Azure Standard Load Balancer からのデータ トラフィック
65500 全受信拒否	任意のポート 任意のプロトコル	任意対任意	その他のすべての受信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 ONTAPの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信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の定義済みセキュリティ グループには、次の送信ルールが含まれています。

ポート	プロトコル	目的
全て	すべてTCP	すべての送信トラフィック
全て	すべてUDP	すべての送信トラフィック

高度なアウトバウンドルール

送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による送信通信に必要なポートのみを開くことができます。



ソースは、Cloud Volumes ONTAPシステム上のインターフェース (IP アドレス) です。

サービス	ポート	プロトコル	ソース	デスティネーション	目的
Active Directory	88	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V認証
	137	UDP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	138	UDP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	139	TCP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	389	TCPとUDP	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	445	TCP	ノード管理LIF	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	464	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos鍵管理
	749	TCP	ノード管理LIF	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)
	88	TCP	データ LIF (NFS、CIFS、iSCSI)	アクティブディレクトリフォレスト	Kerberos V認証
	137	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSネーム サービス
	138	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSデータグラムサービス
	139	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOSサービス セッション
	389	TCPとUDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	445	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
	464	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (SET_CHANGE)
	464	UDP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos鍵管理
	749	TCP	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	Kerberos V パスワードの変更と設定 (RPCSEC_GSS)

サービス	ポート	プロトコル	ソース	デスティネーション	目的
AutoSupport	HTTPS	443	ノード管理LIF	mysupport.netapp.com	AutoSupport（HTTPSがデフォルト）
	HTTP	80	ノード管理LIF	mysupport.netapp.com	AutoSupport（トランスポート 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	コンソールエージェント	アウトバウンドインターネット接続が利用できない場合、コンソールエージェント上のプロキシサーバーを介して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://<コンソールエージェントのIPアドレス>/occm/offboxconfig	構成のバックアップをコンソールエージェントに送信します。 "ONTAPのドキュメント" 。
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	宛先サーバー	NDMPコピー
SMTP	25	TCP	ノード管理LIF	メール サーバ	SMTPアラートはAutoSupportに使用できます
SNMP	161	TCP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	161	UDP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	162	TCP	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	162	UDP	ノード管理LIF	監視サーバー	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

コンソールエージェントの要件

コンソール エージェントをまだ作成していない場合は、コンソール エージェントのネットワーク要件も確認する必要があります。

- ["コンソールエージェントのネットワーク要件を表示する"](#)

- ["Azure のセキュリティ グループ ルール"](#)

関連トピック

- ["Cloud Volumes ONTAPのAutoSupport設定を確認する"](#)
- ["ONTAPの内部ポートについて学ぶ"](#)。

Azureで顧客管理キーを使用するようにCloud Volumes ONTAPを設定する

データは、Microsoft が管理するキーを使用した Azure Storage Service Encryption を使用して、Azure のCloud Volumes ONTAP上で自動的に暗号化されます。ただし、このページの手順に従って、代わりに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Azureで自動的に暗号化されます。 ["Azure Storage Service Encryption"](#)。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でカスタマー管理キーを使用する場合は、次の手順を完了する必要があります。

1. Azure からキー コンテナーを作成し、そのコンテナー内にキーを生成します。
2. NetApp Consoleから、API を使用して、キーを使用するCloud Volumes ONTAPシステムを作成します。

データの暗号化方法

コンソール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 BLOB ではなく管理対象ディスクで暗号化キーを管理できるようになります。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、顧客管理キーではなく、Microsoft 管理キーが使用されます。

カスタマー管理キーを使用するように設定されたCloud Volumes ONTAPシステムを作成すると、Cloud Volumes ONTAPデータは次のように暗号化されます。

Cloud Volumes ONTAP構成	キー暗号化に使用されるシステムディスク	キー暗号化に使用されるデータディスク
シングル ノード	• ブート • コア • NVRAM	• ルート • データ
Azure HA 単一可用性ゾーンとページ BLOB	• ブート • コア • NVRAM	なし
共有マネージド ディスクを備えた Azure HA 単一可用性ゾーン	• ブート • コア • NVRAM	• ルート • データ

Cloud Volumes ONTAP構成	キー暗号化に使用されるシステムディスク	キー暗号化に使用されるデータディスク
共有マネージド ディスクを使用した Azure HA 複数可用性ゾーン	• ブート • コア • NVRAM	• ルート • データ

Cloud Volumes ONTAPのすべての Azure ストレージ アカウントは、顧客管理キーを使用して暗号化されます。ストレージ アカウントの作成中に暗号化する場合は、Cloud Volumes ONTAP作成リクエストでリソースの ID を作成して提供する必要があります。これはすべてのタイプの展開に適用されます。指定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、コンソールは最初に Microsoft 管理のキー暗号化を使用してストレージ アカウントを作成し、次にカスタマー マネージド キーを使用するようにストレージ アカウントを更新します。

Cloud Volumes ONTAPでのキーローテーション

暗号化キーを構成するときは、Azure ポータルを使用して自動キー ローテーションを設定し、有効にする必要があります。新しいバージョンの暗号化キーを作成して有効にすると、Cloud Volumes ONTAP は暗号化に最新のキー バージョンを自動的に検出して使用できるようになり、手動による介入を必要とせずにデータの安全性が確保されます。

キーの構成とキーのローテーションの設定については、次の Microsoft Azure ドキュメントのトピックを参照してください。

- ["Azure Key Vault で暗号化キーの自動ローテーションを構成する"](#)
- ["Azure PowerShell - カスタマーマネージドキーを有効にする"](#)



キーを設定したら、次の項目を選択したことを確認してください。"[自動回転を有効にする](#)"これにより、Cloud Volumes ONTAP は、以前のキーの有効期限が切れたときに新しいキーを使用できるようになります。Azure ポータルでこのオプションを有効にしないと、Cloud Volumes ONTAP は新しいキーを自動的に検出できず、ストレージのプロビジョニングで問題が発生する可能性があります。

ユーザー割り当てマネージド ID を作成する

ユーザー割り当てマネージド ID と呼ばれるリソースを作成するオプションがあります。これにより、Cloud Volumes ONTAPシステムを作成するときにストレージ アカウントを暗号化できるようになります。キー コンテナー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、マネージド ID を選択します。
2. *作成*をクリックします。
3. 以下の詳細を入力してください。
 - サブスクリプション: サブスクリプションを選択します。コンソール エージェントの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: オプションで、コンソール エージェント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*をクリックします。

キーコンテナを作成し、キーを生成する

キー コンテナは、Cloud Volumes ONTAPシステムを作成する予定の Azure サブスクリプションとリージョンに存在する必要があります。

もしあなたがユーザー割り当てマネージドIDを作成したキー コンテナを作成するときに、キー コンテナのアクセス 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にキーコンテナを作成する"。

キー コンテナの次の要件に注意してください。

- キー ボールトは、Cloud Volumes ONTAPシステムと同じリージョンに存在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。
 - ソフト削除 (このオプションはデフォルトで有効になっていますが、無効にしないでください)
 - パージ保護
 - ボリューム暗号化のための **Azure Disk Encryption** (単一ノード システム、複数ゾーンの HA ペア、および HA 単一 AZ 展開の場合)



Azure カスタマー管理暗号化キーを使用するには、キー コンテナに対して Azure Disk Encryption が有効になっている必要があります。

- ユーザー割り当てマネージド 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。
 - **Vault** アクセス ポリシー

2. [コンテナ 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 コンテナのアクセス 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。

- 得る
- リスト
- 解読する
- 暗号化する
- アンラップキー
- ラップキー
- 確認カクニン

- サイン

- b. ユーザーが割り当てたマネージド 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. "キーコンテナにキーを生成する"。

キーについては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、他のサイズもサポートされています。

暗号化キーを使用するシステムを作成する

キー ボールトを作成し、暗号化キーを生成したら、そのキーを使用するように構成された新しいCloud Volumes ONTAPシステムを作成できます。これらの手順は、API を使用することでサポートされます。

必要な権限

単一ノードのCloud Volumes ONTAPシステムでカスタマー管理キーを使用する場合は、コンソール エージェントに次の権限があることを確認してください。

```
"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"
```

"最新の権限リストを表示する"

手順

1. 次の API 呼び出しを使用して、Azure サブスクリプション内のキー コンテナの一覧を取得します。

HA ペアの場合: GET /azure/ha/metadata/vaults

単一ノードの場合: GET /azure/vsa/metadata/vaults

name と **resourceGroup** をメモします。次のステップ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"。

2. 次の API 呼び出しを使用して、ボー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/metadata/keys-vault

単一ノードの場合: GET /azure/vsa/metadata/keys-vault

keyName をメモします。次の手順で、その値 (および Vault 名) を指定する必要があります。

["このAPI呼び出しの詳細"](#)。

3. 次の 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/working-environments
```

リクエスト本体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"  
}
```



含める `"userAssignedIdentity": "userAssignedIdentityId"` このリソースをストレージ アカウントの暗号化に使用するために作成した場合は、このフィールドが必要です。

["このAPI呼び出しの詳細"](#)。

b. 単一ノード システムの場合:

```
POST /azure/vsa/working-environments
```

リクエスト本体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"  
}
```



含める `"userAssignedIdentity": "userAssignedIdentityId"` このリソースをストレージ アカウントの暗号化に使用するために作成した場合は、このフィールドが必要です。

["このAPI呼び出しの詳細"](#)。

結果

データ暗号化に顧客管理キーを使用するように設定された新しいCloud Volumes ONTAPシステムがあります。

AzureでCloud Volumes ONTAPのライセンスを設定する

Cloud Volumes ONTAPで使用するライセンス オプションを決定したら、新しいシステムを作成するときにそのライセンス 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

最大 500 GiB のプロビジョニング容量でCloud Volumes ONTAP を無料で使用するには、Freemium オファリングを選択してください。"[フリーミアムプランの詳細](#)"。

手順

1. NetApp Consoleの左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、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*をクリックし、プロンプトに従って Azure Marketplace の従量課金制オファリングをサブスクライブします。

プロビジョニングされた容量が500GiBを超えない限り、マーケットプレースのサブスクリプションを通じて課金されることはありません。その時点で、システムは自動的に"[エッセンシャルパッケージ](#)"。

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. コンソールに戻ったら、課金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

▼

["AzureでCloud Volumes ONTAPを起動するための手順を見る"](#)。

容量ベースのライセンス

容量ベースのライセンスでは、容量 1 TiB ごとにCloud Volumes ONTAPの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、Essentials パッケージまたは Professional パッケージというパッケージ形式で提供されます。

Essentials および Professional パッケージは、次の消費モデルまたは購入オプションで利用できます。

- NetAppから購入したライセンス (BYOL)
- Azure Marketplace からの時間単位の従量課金制 (PAYGO) サブスクリプション
- 年間契約

["容量ベースのライセンスについて詳しく見る"](#)。

次のセクションでは、それぞれの消費モデルを開始する方法について説明します。

BYOL

NetAppからライセンス (BYOL) を購入して前払いすることで、任意のクラウド プロバイダーにCloud Volumes ONTAPシステムを導入できます。



はBYOLライセンスの購入、延長、および更新を制限しています。 ["Cloud Volumes ONTAPのBYOL ライセンスの利用制限"](#)。

手順

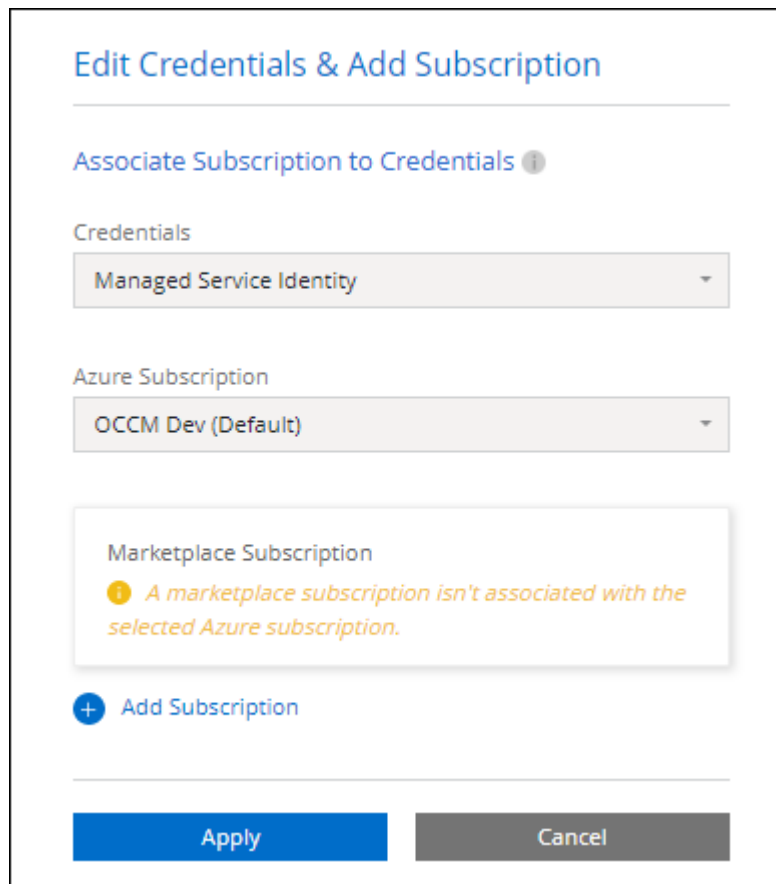
1. ["ライセンスを取得するには、NetApp の営業担当者にお問い合わせください。"](#)
2. ["NetAppサポートサイトのアカウントをコンソールに追加します"](#)

コンソールは NetApp のライセンス サービスに自動的にクエリを実行し、NetAppサポート サイト 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。エラーがない場合、コンソールはライセンスを自動的にコンソールに追加します。

Cloud Volumes ONTAPでライセンスを使用するには、コンソールからライセンスを利用する必要があります。必要であれば、"[コンソールにライセンスを手動で追加する](#)"。

3. *システム*ページで*システムの追加*をクリックし、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*をクリックし、プロンプトに従って Azure Marketplace の従量課金制オファリングをサブスクライブします。

NetAppから購入したライセンスに対しては常に最初に課金されますが、ライセンス容量を超えた場合、または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時間単位料金で課金されます。



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. コンソールに戻ったら、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

☒ Professional

By capacity

▼

☐ Essential

By capacity

▼

☐ Freemium (Up to 500 GiB)

By capacity

▼

☐ Per Node

By node

▼

"AzureでCloud Volumes ONTAPを起動するための手順を見る"。

PAYGOサブスクリプション

クラウド プロバイダーのマーケットプレイスからのオファーをサブスクライブして、時間単位で支払います。

Cloud Volumes ONTAPシステムを作成すると、コンソールに、Azure Marketplace で利用可能な契約にサブスクライブするように求めるプロンプトが表示されます。そのサブスクリプションは課金システムに関連付けられます。同じサブスクリプションを追加のシステムにも使用できます。

手順

1. 左側のナビゲーション メニューから、ストレージ > 管理 を選択します。
2. *システム*ページで*システムの追加*をクリックし、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*をクリックし、プロンプトに従って Azure Marketplace の従量課金制オファリングをサブスクライブします。

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. コンソールに戻ったら、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

☒ Professional	By capacity	▼
☐ Essential	By capacity	▼
☐ Freemium (Up to 500 GiB)	By capacity	▼
☐ Per Node	By node	▼

"AzureでCloud Volumes ONTAPを起動するための手順を見る"。



Azure アカウントに関連付けられている Azure Marketplace サブスクリプションは、[設定] > [資格情報] ページから管理できます。 ["Azure アカウントとサブスクリプションを管理する方法を学びます"](#)

年間契約

年間契約を購入して、Cloud Volumes ONTAP の料金を毎年支払います。

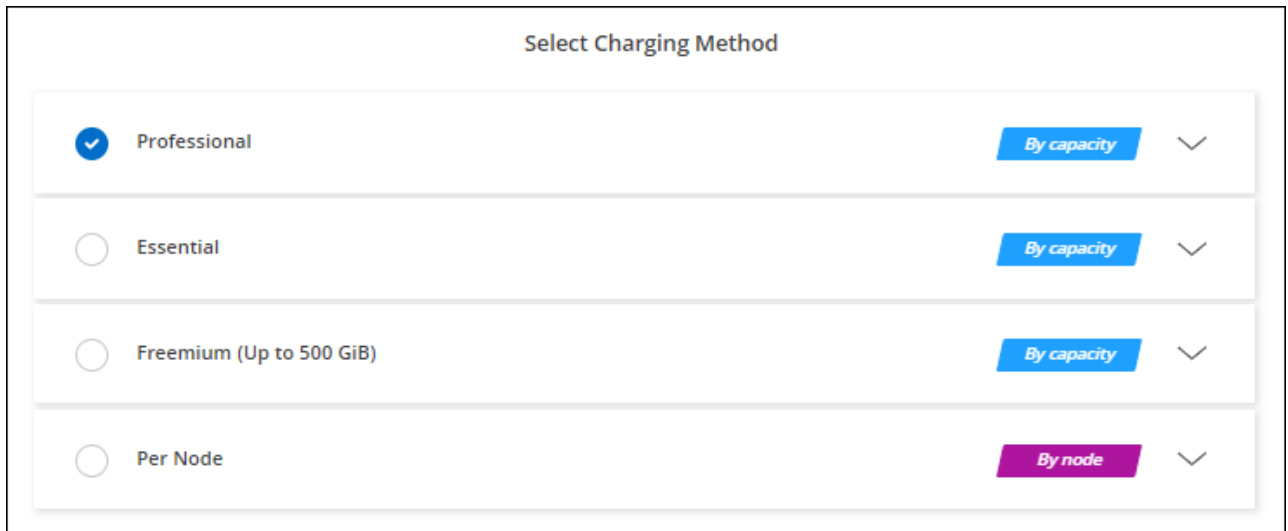
手順

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

契約は、Azure Marketplace でプライベート オファーとして利用できます。

NetApp がプライベート オファーを共有した後、システム作成中に Azure Marketplace からサブスクリブするときに年間プランを選択できます。

2. *システム*ページで*システムの追加*をクリックし、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 アカウントと共有された年間プランを選択し、[サブスクリブ] をクリックします。
 - c. コンソールに戻ったら、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	
☒ Professional	By capacity
☐ Essential	By capacity
☐ Freemium (Up to 500 GiB)	By capacity
☐ Per Node	By node

"AzureでCloud Volumes ONTAPを起動するための手順を見る"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、成長に応じて支払う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](#)"。

手順

1. まだ購読していない場合は、"[ネットアップに連絡](#)"
2. [NetAppにお問い合わせください](#) に連絡して、コンソールで 1 つ以上のKeystoneサブスクリプションを使用してユーザー アカウントを承認します。
3. NetAppがアカウントを承認すると、"[Cloud Volumes ONTAPで使用するためにサブスクリプションをリンクします](#)"。
4. *システム*ページで*システムの追加*をクリックし、手順に従います。

- a. 課金方法を選択するように求められたら、Keystoneサブスクリプションの課金方法を選択します。

Select Charging Method

☒ **Keystone** By capacity ^

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

☐ Professional By capacity v

☐ Essential By capacity v

☐ Freemium (Up to 500 GiB) By capacity v

☐ Per Node By node v

"AzureでCloud Volumes ONTAPを起動するための手順を見る"。

ノードベースのライセンス

ノードベースライセンスは、Cloud Volumes ONTAPの旧世代ライセンスです。ノードベースライセンスはNetApp（BYOL）から取得でき、特定のケースに限りライセンス更新に利用できます。詳細については、以下を参照してください。

- "ノードベースライセンスの提供終了"
- "ノードベースライセンスの提供終了"
- "ノードベースのライセンスを容量ベースのライセンスに変換する"

AzureでCloud Volumes ONTAPの高可用性モードを有効にする

予期しないフェイルオーバー時間を削減し、Cloud Volumes ONTAP の NFSv4 サポートを有効にするには、Microsoft Azure の高可用性（HA）モードを有効にする必要があります。このモードを有効にすると、Cloud Volumes ONTAP HA ノードは、CIFS および NFSv4 クライアントでの計画外のフェイルオーバー時に、低い（60 秒）復旧時間目標（RTO）を達成できます。

Cloud Volumes ONTAP 9.10.1 以降では、Microsoft Azure で実行されているCloud Volumes ONTAP HA ペア

の計画外のフェイルオーバー時間を短縮し、NFSv4 のサポートを追加しました。これらの拡張機能をCloud Volumes ONTAPで利用できるようにするには、Azure サブスクリプションで高可用性機能を有効にする必要があります。

タスク概要

NetApp Console は、Azure サブスクリプションで機能を有効にする必要がある場合、これらの詳細を表示します。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 イベントによって発生する NFS プロトコルのクライアントで観測される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 に問題は発生しません。
- Cloud Volumes ONTAP は、CIFS および NFS クライアント上のクラスターおよび SVM 管理 LIF のフェイルオーバー中に内部 Azure ロード バランサーを使用します。
- HA モードが有効になっている場合、コンソールは 12 時間ごとにシステムをスキャンして、Azure Load Balancer の内部ルールを更新します。

手順

Owner 権限を持つ Azure ユーザーは、Azure CLI からこの機能を有効にできます。

1. ["Azure ポータルから Azure Cloud Shell にアクセスする"](#)
2. 高可用性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 は次のような結果を返すはずです。

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

関連リンク

1. ["Microsoft Azure ドキュメント：高可用性ポートの概要"](#)
2. ["Microsoft Azure ドキュメント：Azure CLI の使用を開始する"](#)

Azure で Cloud Volumes ONTAP の VMOrchestratorZonalMultiFD を有効にする

ローカル冗長ストレージ (LRS) の単一アベイラビリティゾーン (AZ) に VM インスタンスを展開するには、Microsoft `Microsoft.Compute/VMOrchestratorZonalMultiFD` サブスクリプションの機能。高可用性 (HA) モードでは、この機能により、同じ可用性ゾーン内の別々の障害ドメインにノードを展開することが容易になります。

この機能を有効にしないと、ゾーン展開は行われず、以前の LRS 非ゾーン展開が有効になります。

単一のアベイラビリティゾーンでの VM の展開については、以下を参照してください。"[Azure のハイアベイラビリティ ペア](#)"。

「所有者」権限を持つユーザーとして次の手順を実行します。

手順

1. Azure ポータルから Azure Cloud Shell にアクセスします。詳細については、"[Microsoft Azure ドキュメント：Azure Cloud Shell の使用を開始する](#)"。
2. 登録する `Microsoft.Compute/VMOrchestratorZonalMultiFD` 次のコマンドを実行して機能を有効にします。

```
az account set -s <Azure サブスクリプション名または ID> az feature register --name
VMOrchestratorZonalMultiFD --namespace Microsoft.Compute
```

3. 登録ステータスと出力サンプルを確認します。


```
az feature show -n VMOrchestratorZonalMultiFD --namespace Microsoft.Compute { "id":  
"/subscriptions/<ID>/providers/Microsoft.Features/providers/Microsoft.Compute/features/VMOrchestra  
torZonalMultiFD", "name": "Microsoft.Compute/VMOrchestratorZonalMultiFD", "properties": { "state": "  
登録済み" }, "type": "Microsoft.Features/providers/features" }
```

AzureでCloud Volumes ONTAPを起動する

Azureで単一ノードシステムまたはHAペアを起動するには、NetApp ConsoleでCloud Volumes ONTAPシステムを作成します。

開始する前に

始める前に以下のものがが必要です。

- 稼働中のコンソール エージェント。
 - あなたは ["システムに関連付けられたコンソールエージェント"](#)。
 - ["コンソールエージェントを常に実行しておく必要があります"](#)。
- 使用する構成を理解すること。

構成を計画し、管理者から必要な Azure ネットワークの詳細を入手する必要があります。詳細については、["Cloud Volumes ONTAP構成の計画"](#)。

- Cloud Volumes ONTAPのライセンスを設定するために必要なことを理解していること。

["ライセンスの設定方法を学ぶ"](#)。

タスク概要

コンソールが Azure に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 オブジェクトが作成されます。ウィザードの最後にリソースの概要を確認できます。

データ損失の可能性

ベスト プラクティスは、各Cloud Volumes ONTAPシステムに新しい専用のリソース グループを使用することです。



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をデプロイすることはお勧めしません。コンソールは、デプロイメントの失敗または削除の際に共有リソース グループからCloud Volumes ONTAPリソースを削除できますが、Azure ユーザー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。

Azure でシングルノードのCloud Volumes ONTAPシステムを起動する

Azure で単一ノードの Cloud Volumes ONTAP システムを起動する場合は、コンソールで単一ノード システム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、ストレージ > 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. 場所の選択: **Microsoft Azure** と * Cloud Volumes ONTAP Single Node* を選択します。
4. プロンプトが表示されたら、["コンソールエージェントを作成する"](#)。
5. 詳細と資格情報: 必要に応じて Azure の資格情報とサブスクリプションを変更し、クラスター名を指定し、必要に応じてタグを追加して、資格情報を指定します。

次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、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。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても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、コンソールはそれらをCloud Volumes ONTAPシステムに関連付けられたリソース グループに追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、 "Microsoft Azure ドキュメント: タグを使用して Azure リソースを整理する" 。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの <i>admin</i> ユーザー名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。
資格情報の編集	このCloud Volumes ONTAPシステムで使用するために、異なる Azure 資格情報と異なる Azure サブスクリプションを選択できます。従量課金制のCloud Volumes ONTAPシステムを展開するには、Azure Marketplace サブスクリプションを選択した Azure サブスクリプションに関連付ける必要があります。 "資格情報を追加する方法を学ぶ" 。

6. サービス: Cloud Volumes ONTAPで使用する、または使用しないサービスを個別に有効または無効にします。
 - ["NetApp Data Classificationの詳細"](#)
 - ["NetApp Backup and Recoveryの詳細"](#)



WORM とデータ階層化を利用する場合は、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システムを展開する必要があります。

7. 場所: リージョン、可用性ゾーン、VNet、サブネットを選択し、チェックボックスをオンにして、コンソール エージェント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。



中国地域では、単一ノードの展開はCloud Volumes ONTAP 9.12.1 GA および 9.13.0 GA のみサポートされます。これらのバージョンは、Cloud Volumes ONTAPの以降のパッチとリリースにアップグレードできます。["Azureでサポートされています"](#)。中国地域で新しいバージョンのCloud Volumes ONTAPを展開する場合は、NetAppサポートにお問い合わせください。中国地域ではNetAppから直接購入したライセンスのみがサポートされており、マーケットプレイスのサブスクリプションは利用できません。

8. 接続: 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、定義済みのセキュリティ グループを使用するか、独自のセキュリティ グループを使用するかを選択します。

次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
Resource Group	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。ベストプラクティスは、Cloud Volumes ONTAP 専用の新しいリソースグループを使用することです。Cloud Volumes ONTAP を既存の共有リソース グループにデプロイすることは可能ですが、データ損失のリスクがあるためお勧めしません。詳細については上記の警告を参照してください。  使用しているAzureアカウントに "必要な権限"、コンソールは、デプロイメントの失敗または削除の場合に、リソース グループからCloud Volumes ONTAPリソースを削除します。
生成されたセキュリティグループ	コンソールでセキュリティ グループを生成させる場合は、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。 • 選択した VNet のみ を選択した場合、受信トラフィックのソースは、選択した VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲になります。これは推奨されるオプションです。 • すべての VNet を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のセキュリティ グループを選択する場合は、Cloud Volumes ONTAP の要件を満たしている必要があります。"デフォルトのセキュリティ グループを表示する"。

9. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、NetAppサポート サイト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学ぶ"](#)。
- ["ライセンスの設定方法を学ぶ"](#)。

10. 事前構成済みパッケージ: パッケージの 1 つを選択してCloud Volumes ONTAPシステムをすばやく展開するか、[*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構成を確認し、承認するだけです。

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、仮想マシンの種類を選択します。



選択したバージョンに対して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、BlueXP は作業環境を作成するときにシステムをそのバージョンに更新します。たとえば、Cloud Volumes ONTAP 9.16.1 P3 を選択し、9.16.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.15 から 9.16) には行われません。

12. **Azure Marketplace** からサブスクリプション: コンソールがCloud Volumes ONTAPのプログラムによるデプロイメントを有効にできなかった場合、このページが表示されます。画面に表示される手順に従ってください。"[マーケットプレイス製品のプログラムによる展開](#)"詳細についてはこちらをご覧ください。
13. 基盤となるストレージ リソース: 初期集約の設定 (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) を選択します。

次の点に注意してください。

- VNet 内でストレージ アカウントへのパブリック アクセスが無効になっている場合、Cloud Volumes ONTAPシステムでデータ階層化を有効にすることはできません。詳細については、"[セキュリティグループルール](#)"。
- ディスク タイプは初期ボリューム用です。後続のボリュームには異なるディスク タイプを選択できません。
- ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な割り当てオプションを使用して、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を選択については、以下を参照してください。"[Azure でのシステムのサイズ設定](#)"。

- 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。
- データ階層化を無効にした場合、後続の集約で有効にすることができます。

"[データ階層化の詳細](#)"。

14. 書き込み速度とWORM:

- a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

"[書き込み速度について詳しくはこちら](#)"。

- b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

このオプションは特定の VM タイプでのみ使用できます。サポートされているVMタイプを確認するには、以下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バージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。WORM と階層化を有効にした後、Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

"[WORMストレージについて詳しくはこちら](#)"。

- a. WORM ストレージを有効にする場合は、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。

"サポートされているクライアントプロトコルとバージョンについて学ぶ"。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセスレベル (アクセス制御リストまたは ACL と呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション (NFSのみ)	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、 "IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。

Volume Details & Protection

Volume Name ⓘ

Storage VM (SVM)

Volume Size ⓘ

Unit

Snapshot Policy

default policy ⓘ

16. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD Domain Services をCloud Volumes ONTAP の AD サーバーとして構成するには、このフィールドに OU=AADDC Computers または OU=AADDC Users を入力する必要があります。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure ドキュメント: Azure AD Domain Services マネージド ドメインに組織単位 (OU) を作成する"]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「 Active Directory ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント" 詳細については、NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。CIFS サーバーを作成した後は構成できません。

17. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

詳細については、["ボリューム使用プロファイルの理解"そして"データ階層化の概要"](#)。

18. 確認と承認: 選択内容を確認して確定します。

- a. 構成の詳細を確認します。
- b. 詳細情報をクリックすると、サポートとコンソールが購入する Azure リソースの詳細を確認できます。
- c. 理解しました... チェックボックスを選択します。
- d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。監査ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、["NetApp Cloud Volumes ONTAPサポート"](#)。



デプロイ プロセスが完了したら、Azure ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、ONTAP System Manager またはONTAP CLI を使用します。

クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。

AzureでCloud Volumes ONTAP HAペアを起動する

Azure でCloud Volumes ONTAP HA ペアを起動する場合は、コンソールで HA システム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、ストレージ > 管理 を選択します。
2. *システム*ページで、*システムの追加*をクリックし、指示に従います。
3. プロンプトが表示されたら、["コンソールエージェントを作成する"](#)。
4. 詳細と資格情報: 必要に応じて Azure の資格情報とサブスクリプションを変更し、クラスター名を指定し、必要に応じてタグを追加して、資格情報を指定します。

次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
システム名	コンソールは、システム名を使用して、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。このオプションを選択した場合、定義済みのセキュリティ グループのプレフィックスとしても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、コンソールはそれらをCloud Volumes ONTAPシステムに関連付けられたリソース グループに追加します。システムを作成するときに、ユーザー インターフェイスから最大 4 つのタグを追加でき、システムの作成後にさらにタグを追加できます。システムを作成するときに、API ではタグが 4 つに制限されないことに注意してください。タグの詳細については、" Microsoft Azure ドキュメント: タグを使用して Azure リソースを整理する "。
ユーザ名とパスワード	これらは、Cloud Volumes ONTAPクラスター管理者アカウントの資格情報です。これらの資格情報を使用して、ONTAP System Manager またはONTAP CLI を介してCloud Volumes ONTAPに接続できます。デフォルトの <i>admin</i> ユーザー名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。
資格情報の編集	このCloud Volumes ONTAPシステムで使用するために、異なる Azure 資格情報と異なる Azure サブスクリプションを選択できます。従量課金制のCloud Volumes ONTAPシステムを展開するには、Azure Marketplace サブスクリプションを選択した Azure サブスクリプションに関連付ける必要があります。" 資格情報を追加する方法を学ぶ "。

5. サービス: Cloud Volumes ONTAPで使用するかどうかに基づいて、個々のサービスを有効または無効にします。

- "[NetApp Data Classificationの詳細](#)"
- "[NetApp Backup and Recoveryの詳細](#)"



WORM とデータ階層化を利用する場合は、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システムを展開する必要があります。

6. HA 展開モデル:

a. *単一の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。

- 単一の可用性ゾーンの場合は、Azure リージョン、可用性ゾーン、VNet、サブネットを選択します。

Cloud Volumes ONTAP 9.15.1 以降では、Azure の単一の可用性ゾーン (AZ) に HA モードで仮想マシン (VM) インスタンスをデプロイできます。このデプロイメントをサポートするゾーンとリージョンを選択する必要があります。ゾーンまたはリージョンがゾーン展開をサポートしていない場合は、LRS の以前の非ゾーン展開モードが適用されます。共有管理ディスクのサポートされている構成については、以下を参照してください。"[共有マネージドディスクを使用した HA 単一アベイラビリティゾーン構成](#)"。

- 複数の可用性ゾーンの場合は、リージョン、VNet、サブネット、ノード 1 のゾーン、ノード 2 のゾーンを選択します。

b. ネットワーク接続を確認しました... チェックボックスを選択します。

7. 接続: 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、定義済みのセキュリティ グループを使用するか、独自のセキュリティ グループを使用するかを選択します。

次の表では、ガイダンスが必要になる可能性のあるフィールドについて説明します。

フィールド	説明
Resource Group	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。ベストプラクティスは、Cloud Volumes ONTAP 専用の新しいリソースグループを使用することです。Cloud Volumes ONTAP を既存の共有リソース グループにデプロイすることは可能ですが、データ損失のリスクがあるためお勧めしません。詳細については上記の警告を参照してください。 Azure にデプロイする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 グループでは1つの HA ペアのみがサポートされます。Azure リソース グループに2 番目のCloud Volumes ONTAP HA ペアをデプロイしようとする、コンソール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 "必要な権限"、コンソールは、デプロイメントの失敗または削除の場合に、リソース グループからCloud Volumes ONTAPリソースを削除します。
生成されたセキュリティグループ	コンソールでセキュリティ グループを生成させる場合は、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。 • 選択した VNet のみ を選択した場合、受信トラフィックのソースは、選択した VNet のサブネット範囲と、コンソール エージェントが存在する VNet のサブネット範囲になります。これは推奨されるオプションです。 • すべての VNet を選択した場合、受信トラフィックのソースは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のセキュリティ グループを選択する場合は、Cloud Volumes ONTAP の要件を満たしている必要があります。"デフォルトのセキュリティ グループを表示する"。

8. 課金方法と **NSS** アカウント: このシステムで使用する課金オプションを指定し、NetAppサポート サイト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学ぶ"](#)。
- ["ライセンスの設定方法を学ぶ"](#)。

9. 事前構成済みパッケージ: Cloud Volumes ONTAPシステムをすばやく展開するには、パッケージの1つを選択するか、[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構成を確認し、承認するだけです。

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、仮想マシンの種類を選択します。



選択したバージョンに対して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、コンソールは作成時にシステムをそのバージョンに更新します。たとえば、Cloud Volumes ONTAP 9.13.1 を選択し、9.13.1 P4 が利用可能な場合は更新が行われます。更新は、あるリリースから別のリリース (たとえば、9.13 から 9.14) には行われません。

11. **Azure Marketplace** からサブスクリプション: コンソールでCloud Volumes ONTAPのプログラムによるデプロイメントを有効にできなかった場合は、次の手順に従います。
12. 基盤となるストレージ リソース: 初期集約の設定 (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) を選択します。

次の点に注意してください。

- ディスク サイズは、初期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 オプションを使用するときにコンソールが作成する追加のアグリゲートのすべてのディスクに適用されます。高度な割り当てオプションを使用して、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、以下を参照してください。"[Azure でシステムのサイズを決定する](#)"。

- VNet 内でストレージ アカウントへのパブリック アクセスが無効になっている場合、Cloud Volumes ONTAPシステムでデータ階層化を有効にすることはできません。詳細については、"[セキュリティグループルール](#)"。
- 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。
- データ階層化を無効にした場合、後続の集約で有効にすることができます。

"[データ階層化の詳細](#)"。

- Cloud Volumes ONTAP 9.15.0P1 以降、新しい高可用性ペアの展開では Azure ページ BLOB はサポートされなくなりました。現在、既存の高可用性ペアの展開で Azure ページ BLOB を使用している場合は、Edsv4 シリーズ VM および Edsv5 シリーズ VM の新しい VM インスタンス タイプに移行できます。

"[Azureでサポートされている構成の詳細](#)"。

13. 書き込み速度と**WORM**:

- a. 必要に応じて、「通常」または「高速」の書き込み速度を選択します。

"[書き込み速度について詳しくはこちら](#)"。

- b. 必要に応じて、一度書き込み、何度も読み取り可能な (WORM) ストレージをアクティブ化します。

このオプションは特定の VM タイプでのみ使用できます。サポートされているVMタイプを確認するには、以下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バージョン 9.7 以下でデータ階層化が有効になっている場合、WORM を有効にすることはできません。WORM と階層化を有効にした後、Cloud Volumes ONTAP 9.8 への復元またはダウングレードはブロックされます。

"[WORMストレージについて詳しくはこちら](#)"。

- a. WORM ストレージを有効にする場合は、保持期間を選択します。

14. ストレージと **WORM** への安全な通信: 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、一度書き込み、複数回読み取り (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 HA ペアから Azure ページ BLOB ストレージ アカウントへ行われます。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ることに注意してください。システムを作成した後は設定を変更できません。

["WORMストレージについて詳しくはこちら"](#)。

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

["WORMストレージについて詳しくはこちら"](#)。

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。

["サポートされているクライアントプロトコルとバージョンについて学ぶ"](#)。

このページのいくつかのフィールドは説明不要です。次の表では、ガイダンスが必要になる可能性のある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な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、コンソール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、ユーザーとグループの共有へのアクセスレベル (アクセス制御リストまたは ACL と呼ばれます) を制御できます。ローカルまたはドメインの Windows ユーザーまたはグループ、あるいは UNIX ユーザーまたはグループを指定できます。ドメイン Windows ユーザー名を指定する場合は、domain\username の形式を使用してユーザーのドメインを含める必要があります。
スナップショットポリシー	スナップショット コピー ポリシーは、自動的に作成されるNetAppスナップショット コピーの頻度と数を指定します。NetAppスナップショット コピーは、パフォーマンスに影響を与えず、最小限のストレージしか必要としない、ポイントインタイム ファイル システム イメージです。デフォルトのポリシーを選択するか、ポリシーなしを選択できます。一時データの場合は none を選択できます (例: Microsoft SQL Server の場合は tempdb)。
詳細オプション (NFSのみ)	ボリュームの NFS バージョン (NFSv3 または NFSv4) を選択します。
イニシエーター 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供されます。イニシエーター グループは、iSCSI ホスト ノード名のテーブルであり、どのイニシエーターがどの 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 Ethernet ネットワーク アダプター (NIC)、ソフトウェア イニシエーターを備えた TCP オフロード エンジン (TOE) カード、統合ネットワーク アダプター (CNA)、または専用ホスト バス アダプター (HBA) を介してネットワークに接続し、iSCSI 修飾名 (IQN) によって識別されます。iSCSI ボリュームを作成すると、コンソールによって LUN が自動的に作成されます。ボリュームごとに 1 つの LUN を作成するだけで簡単になるので、管理は不要です。ボリュームを作成したら、 "IQNを使用してホストからLUNに接続します" 。

次の画像は、ボリューム作成ウィザードの最初のページを示しています。

The screenshot shows a configuration page titled "Volume Details & Protection". It contains several input fields and dropdown menus:

- Volume Name:** A text input field containing "ABDcv5689".
- Storage VM (SVM):** A dropdown menu showing "svm_c...CVO1".
- Volume Size:** A text input field containing "100".
- Unit:** A dropdown menu showing "GiB".
- Snapshot Policy:** A dropdown menu showing "default".

Below the Snapshot Policy dropdown, there is a link "default policy" with an information icon (i).

16. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバー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 サーバーの名前解決を提供する DNS サーバーの IP アドレス。これらのDNSサーバには、Active DirectoryのLDAPサーバと、CIFSサーバが参加するドメインのドメイン コントローラを見つけるために必要なサービス 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 サーバーが参加する Active Directory (AD) ドメインの FQDN。
ドメインへの参加を許可された資格情報	AD ドメイン内の指定された組織単位 (OU) にコンピューターを追加するのに十分な権限を持つ Windows アカウントの名前とパスワード。
CIFS server NetBIOS name	AD ドメイン内で一意の CIFS サーバー名。
組織単位	CIFS サーバーに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD Domain Services をCloud Volumes ONTAP の AD サーバーとして構成するには、このフィールドに OU=AADDC Computers または OU=AADDC Users を入力する必要があります。 https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou ["Azure ドキュメント: Azure AD Domain Services マネージド ドメインに組織単位 (OU) を作成する"^]
DNSドメイン	Cloud Volumes ONTAPストレージ仮想マシン (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 サーバーを構成するには、「 Active Directory ドメインを使用する」を選択します。別のアドレスを使用して NTP サーバーを構成する必要がある場合は、API を使用する必要があります。参照 "NetApp Console自動化ドキュメント" 詳細については、NTP サーバーを設定できるのは、CIFS サーバーを作成するときだけであることに注意してください。CIFS サーバーを作成した後は構成できません。

17. 使用プロファイル、ディスク タイプ、階層化ポリシー: 必要に応じて、ストレージ効率機能を有効にするかどうか、およびボリューム階層化ポリシーを変更するかどうかを選択します。

詳細については、"[ボリューム使用プロファイルを選択する](#)"、"[データ階層化の概要](#)"、そして "[KB: CVO ではどのようなインライン ストレージ効率機能がサポートされていますか?](#)"

18. 確認と承認: 選択内容を確認して確定します。

- a. 構成の詳細を確認します。
- b. 詳細情報 をクリックすると、サポートとコンソールが購入する Azure リソースの詳細を確認できます。
- c. 理解しました... チェックボックスを選択します。
- d. [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPシステムを展開します。監査ページで進捗状況を追跡できます。

Cloud Volumes ONTAPシステムのデプロイ中に問題が発生した場合は、失敗メッセージを確認してください。システムを選択して、「環境の再作成」をクリックすることもできます。

さらに詳しいヘルプについては、"[NetApp Cloud Volumes ONTAPサポート](#)"。

終了後の操作

- 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、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てください。
- ボリュームにクォータを適用する場合は、ONTAP System Manager またはONTAP CLI を使用します。

クォータを使用すると、ユーザー、グループ、または qtree が使用するディスク領域とファイル数を制限したり追跡したりできます。



デプロイ プロセスが完了したら、Azure ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しない動作やデータ損失が発生する可能性があります。

関連リンク

[**"Azure でのCloud Volumes ONTAP構成の計画" **"Azure MarketplaceからAzureにCloud Volumes ONTAPをデプロイする"](#)

Azure プラットフォーム イメージの検証

Cloud Volumes ONTAPの Azure Marketplace イメージ検証

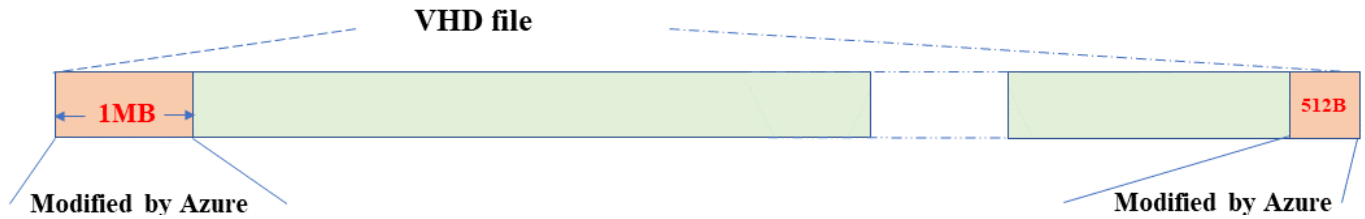
Azure イメージ検証は、強化されたNetAppセキュリティ要件に準拠しています。画像ファイルの検証は簡単なプロセスです。ただし、Azure イメージ署名の検証では、Azure マーケットプレイスで変更されるため、Azure VHD イメージ ファイルに対して特定の考慮が必要になります。



Azure イメージ検証は、Cloud Volumes ONTAP 9.15.0 以降でサポートされています。

Azure による公開 VHD ファイルの変更

VHD ファイルの先頭の 1 MB (1048576 バイト) と末尾の 512 バイトは、Azure によって変更されます。NetApp は残りの VHD ファイルに署名します。



この例では、VHD ファイルは 10 GB です。NetAppが署名した部分は緑色でマークされています (10 GB - 1 MB - 512 バイト)。

関連リンク

- ["ページフォルトブログ: OpenSSL を使った署名と検証の方法"](#)
- ["Azure Marketplace イメージを使用して、Azure Stack Edge Pro GPU 用の VM イメージを作成する | Microsoft Learn"](#)
- ["Azure CLI を使用してマネージド ディスクをストレージ アカウントにエクスポート/コピーする | Microsoft Learn"](#)
- ["Azure Cloud Shell クイックスタート - Bash | Microsoft Learn"](#)
- ["Azure CLI のインストール方法 | Microsoft Learn"](#)
- ["az storage blob コピー | Microsoft Learn"](#)
- ["Azure CLI でSign in- ログインと認証 | Microsoft Learn"](#)

Cloud Volumes ONTAP用の Azure イメージ ファイルをダウンロードします。

Azureイメージファイルは、["NetAppサポート サイト"](#)。

`tar.gz` ファイルには、イメージ署名の検証に必要なファイルが含まれています。 `tar.gz` ファイルと一緒に、イメージの `checksum` ファイルもダウンロードする必要があります。チェックサムファイルには、``md5``そして ``sha256`` `tar.gz` ファイルのチェックサム。

手順

1. に行く ["NetAppサポート サイトのCloud Volumes ONTAP製品ページ"](#)*ダウンロード*セクションから必要なソフトウェア バージョンをダウンロードします。
2. Cloud Volumes ONTAP のダウンロード ページで、Azure イメージのダウンロード可能なファイルをクリックし、`tar.gz` ファイルをダウンロードします。

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

3. Linuxでは、`md5sum AZURE-<version>_PKG.TAR.GZ`。

macOSでは、`sha256sum AZURE-<version>_PKG.TAR.GZ`。

4. 確認するには`md5sum`そして`sha256sum`値は、ダウンロードした Azure イメージの値と一致します。

5. LinuxおよびmacOSでは、`tar -xzf` 指示。

抽出された *tar.gz* ファイルには、ダイジェスト (*.sig*) ファイル、公開鍵証明書 (*.pem*) ファイル、およびチェーン証明書 (*.pem*) ファイルが含まれています。

tar.gz ファイルを抽出した後の出力例:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

Azure マーケットプレイスから Cloud Volumes ONTAP の VHD イメージをエクスポートする

VHD イメージが Azure クラウドに公開されると、NetApp によって管理されなくなります。代わりに、公開されたイメージは Azure マーケットプレイスに配置されます。イメージが Azure マーケットプレイスにステージングされ公開されると、Azure は VHD の先頭の 1 MB と末尾の 512 バイトを変更します。VHD ファイルの署名を検証するには、Azure によって変更された VHD イメージを Azure マーケットプレイスからエクス

ポートする必要があります。

開始する前に

Azure CLI がシステムにインストールされていること、または Azure ポータルから Azure Cloud Shell が利用できることを確認してください。Azure CLI のインストール方法の詳細については、["Microsoft ドキュメント: Azure CLI のインストール方法"](#)。

手順

1. `version_readme` ファイルの内容を使用して、システム上の Cloud Volumes ONTAP バージョンを Azure マーケットプレイスのイメージ バージョンにマッピングします。Cloud Volumes ONTAP のバージョンは次のように表されます。buildname Azure マーケットプレイス イメージバージョンは次のように表されます。`version` バージョン マッピングで。

次の例では、Cloud Volumes ONTAP バージョン 9.15.0P1 `Azure` マーケットプレイスのイメージバージョンにマッピングされます `9150.01000024.05090105`。この Azure マーケットプレイスのイメージバージョンは、後でイメージ URN を設定するために使用されます。

```
[
  "buildname": "9.15.0P1",
  "publisher": "netapp",
  "version": "9150.01000024.05090105"
]
```

2. VM を作成するリージョンを特定します。地域名は、`locName` マーケットプレイス イメージの URN を設定するときに使用する変数。利用可能なリージョンを一覧表示するには、次のコマンドを実行します。

```
az account list-locations -o table
```

この表では、地域名は `Name` 分野。

```
$ az account list-locations -o table
DisplayName          Name          RegionalDisplayName
-----
East US              eastus        (US) East US
East US 2            eastus2       (US) East US 2
South Central US    southcentralus (US) South Central US
...
```

3. 以下の表で、対応する Cloud Volumes ONTAP バージョンと VM 展開タイプの SKU 名を確認します。SKU 名は、`skuName` マーケットプレイス イメージの URN を設定するときに使用する変数。

たとえば、Cloud Volumes ONTAP 9.15.0 を使用したすべてのシングルノード展開では、`ontap_cloud_byol` SKU 名として。

* Cloud Volumes ONTAPバージョン*	VMの展開	SKU名
9.17.1以降	Azureマーケットプレイス	ontap_cloud_direct_gen2
9.17.1以降	NetApp Console	ontap_cloud_gen2
9.16.1	Azureマーケットプレイス	ontap_cloud_direct
9.16.1	コンソール	オンタップクラウド
9.15.1	コンソール	オンタップクラウド
9.15.0	コンソール、単一ノードの展開	ontap_cloud_byol
9.15.0	コンソール、高可用性（HA）展開	ontap_cloud_byol_ha

4. ONTAPバージョンと Azure マーケットプレイス イメージをマッピングした後、Azure Cloud Shell または Azure CLI を使用して Azure マーケットプレイスから VHD ファイルをエクスポートします。

Linux 上の **Azure Cloud Shell** を使用して **VHD** ファイルをエクスポートする

Azure Cloud Shell から、マーケットプレイス イメージを VHD ファイル (たとえば、`9150.01000024.05090105.vhd`) にエクスポートし、ローカル Linux システムにダウンロードします。Azure マーケットプレイスから VHD イメージを取得するには、次の手順を実行します。

手順

1. マーケットプレイス イメージの URN とその他のパラメータを設定します。URN形式は `<publisher>:<offer>:<sku>:<version>`。必要に応じて、NetAppマーケットプレイスのイメージを一覧表示して、正しいイメージ バージョンを確認できます。

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. 一致するイメージ バージョンを持つマーケットプレイス イメージから新しいマネージド ディスクを作成します。

```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnfl"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference $urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600 --access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas

```

3. マネージド ディスクから VHD ファイルを Azure Storage にエクスポートします。適切なアクセス レベルを持つコンテナを作成します。この例では、`vm-images`と `Container`アクセス レベル。Azure ポータルからストレージ アカウントのアクセス キーを取得します: ストレージ アカウント > **examplesaname** > アクセス キー > **key1** > **key** > 表示 > **<copy>**

```

PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext -StorageAccountName $storageAccountName -StorageAccountKey $storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS -DestContainer $containerName -DestContext $destContext -DestBlob $destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName -Context $destContext -Blob $destBlobName

```

4. 生成されたイメージを Linux システムにダウンロードします。使用 `wget`VHD ファイルをダウンロードするコマンド:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL は標準形式に従います。自動化のために、以下のように URL 文字列を導出できます。あるいは、Azure CLIを使用することもできます。 az URL を取得するコマンド。 URLの例:<https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd>

5. 管理ディスクをクリーンアップする

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName $diskName

```

Linux 上の Azure CLI を使用して VHD ファイルをエクスポートする

ローカル Linux システムから Azure CLI を使用して、マーケットプレイス イメージを VHD ファイルにエクスポートします。

手順

1. Azure CLI にログインし、マーケットプレイスのイメージを一覧表示します。

```
% az login --use-device-code
```

2. サインインするには、ウェブブラウザを使用してページを開きます <https://microsoft.com/devicelogin> 認証コードを入力します。

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...
```

3. 一致するイメージ バージョンを持つマーケットプレイス イメージから新しいマネージド ディスクを作成します。

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluelxpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluelxpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

プロセスを自動化するには、標準出力から SAS を抽出する必要があります。ガイダンスについては適切なドキュメントを参照してください。

4. 管理ディスクから VHD ファイルをエクスポートします。
 - a. 適切なアクセス レベルを持つコンテナを作成します。この例では、`vm-images`と `Container` アクセス レベルが使用されます。
 - b. Azure ポータルからストレージ アカウントのアクセス キーを取得します: ストレージ アカウント > **examplesaname** > アクセス キー > **key1** > **key** > 表示 > **<copy>**

また、`az`このステップのコマンド。

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
--container $containerName --account-name $storageAccountName --account
--key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. BLOB コピーのステータスを確認します。

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

6. 生成されたイメージを Linux サーバーにダウンロードします。

```
wget <URL of file examplesaname/Containers/vm-  
images/9150.01000024.05090105.vhd>
```

URL は標準形式に従います。自動化のために、以下のように URL 文字列を導出できます。あるいは、Azure CLIを使用することもできます。 az URL を取得するコマンド。 URL の例:https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 管理ディスクをクリーンアップする

```
az disk revoke-access --name $diskName --resource-group $diskRG  
az disk delete --name $diskName --resource-group $diskRG --yes
```

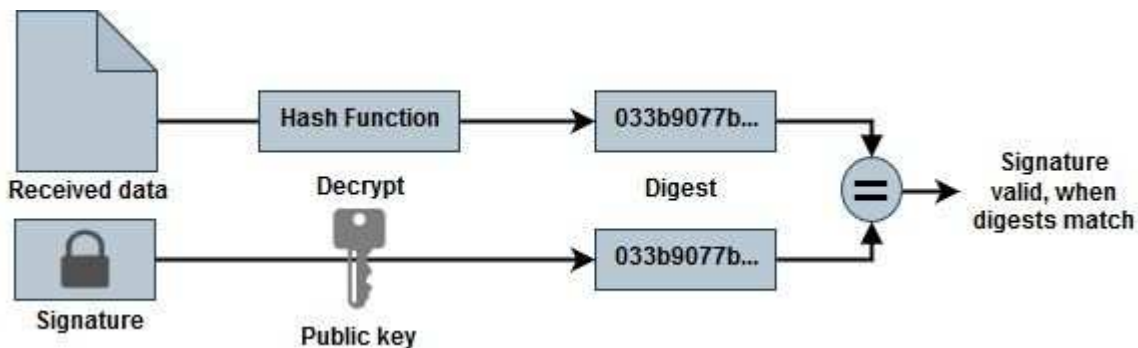
ファイルの署名を検証する

Cloud Volumes ONTAPの Azure Marketplace イメージ署名検証

Azure イメージ検証プロセスでは、先頭の 1 MB と末尾の 512 バイトを削除し、ハッシュ関数を適用して、VHD ファイルからダイジェスト ファイルを生成します。署名手順に合わせて、ハッシュには *sha256* が使用されます。

ファイル署名検証ワークフローの概要

以下は、ファイル署名検証ワークフロー プロセスの概要です。



- Azureイメージを "[NetAppサポート サイト](#)"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。参照"[Azure イメージ ダイジェスト ファイルをダウンロードする](#)"詳細についてはこちらをご覧ください。
- 信頼チェーンの検証。
- 公開鍵証明書 (.pem) から公開鍵 (.pub) を抽出します。
- 抽出された公開鍵を使用してダイジェスト ファイルを復号化します。
- 先頭の 1 MB と末尾の 512 バイトを削除した後、イメージ ファイルから作成された一時ファイルの新しく生成されたダイジェストと結果を比較します。この手順は、OpenSSL コマンドライン ツールを使用して実行されます。 OpenSSL CLI ツールは、ファイルの一致が成功または失敗した場合に適切なメッセージを表示します。


```
openssl dgst -verify <public_key> -keyform <form> <hash_function>
-signature <digest_file> -binary <temporary_file>
```

Linux 上のCloud Volumes ONTAPの Azure Marketplace イメージ署名を確認する

Linux 上でエクスポートされた VHD ファイル署名の検証には、信頼チェーンの検証、ファイルの編集、署名の検証が含まれます。

手順

1. Azureイメージファイルを以下からダウンロードします。"[NetAppサポート サイト](#)"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。

参照 "[Azure イメージ ダイジェスト ファイルをダウンロードする](#)"詳細についてはこちらをご覧ください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD ファイルの先頭の 1 MB (1,048,576 バイト) と末尾の 512 バイトを削除します。使用する場合 tail、-c +K`オプションは、ファイルの K 番目のバイトからバイトを生成します。したがって、1048577は `tail -c。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL を使用して証明書から公開キーを抽出し、署名ファイルと公開キーを使用してストリップされたファイル (sign.tmp) を検証します。

コマンド プロンプトには、検証に基づいて成功または失敗を示すメッセージが表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

macOS 上の Cloud Volumes ONTAP の Azure Marketplace イメージ署名を確認する

Linux 上でエクスポートされた VHD ファイル署名の検証には、信頼チェーンの検証、ファイルの編集、署名の検証が含まれます。

手順

1. Azure イメージファイルを以下からダウンロードします。"[NetApp サポート サイト](#)"ダイジェスト (.sig) ファイル、公開鍵証明書 (.pem) ファイル、チェーン証明書 (.pem) ファイルを抽出します。

参照 "[Azure イメージ ダイジェスト ファイルをダウンロードする](#)" 詳細についてはこちらをご覧ください。

2. 信頼チェーンを検証します。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. VHD ファイルの先頭の 1 MB (1,048,576 バイト) と末尾の 512 バイトを削除します。使用する場合 tail、-c +K オプションは、ファイルの K 番目のバイトからバイトを生成します。したがって、1048577 は `tail -c`。macOS では、tail コマンドが完了するまでに約 10 分かかる場合がありますことに注意してください。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. OpenSSL を使用して証明書から公開キーを抽出し、署名ファイルと公開キーを使用してストリップされたファイル (sign.tmp) を検証します。コマンド プロンプトには、検証に基づいて成功または失敗を示すメッセージが表示されます。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0Pl_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. ワークスペースをクリーンアップします。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

Azure マーケットプレイスから Cloud Volumes ONTAP をデプロイする

Azure マーケットプレイスの直接展開を使用すると、Cloud Volumes ONTAP を迅速かつ簡単に展開できます。Azure マーケットプレイスでは、数回クリックするだけで Cloud Volumes ONTAP を迅速に導入し、そのコア機能と機能を自分の環境で試すことができます。

このオファーの詳細については、以下を参照してください。"[NetApp Console とマーケットプレイスで Cloud Volumes ONTAP のサービスについて学ぶ](#)"。

タスク概要

Azure マーケットプレイスの直接展開を使用して展開された Cloud Volumes ONTAP システムには、次のプロパティがあります。Azure マーケットプレイスを通じてデプロイされたスタンドアロン インスタンスの機能は、NetApp Console で検出された時点で変更されることに注意してください。

- 最新の Cloud Volumes ONTAP バージョン (9.16.1 以降)。
- プロビジョニングされた容量が 500 GiB に制限された Cloud Volumes ONTAP の無料ライセンス。このライセンスには NetApp サポートは含まれず、有効期限もありません。
- 単一の可用性ゾーン (AZ) に高可用性 (HA) モードで構成され、デフォルトのシリアル番号でプロビジョニングされた 2 つのノード。ストレージ仮想マシン (ストレージ VM) は、"[柔軟なオーケストレーションモード](#)"。
- デフォルトで作成されるインスタンスの集約。

- 500 GiB のプロビジョニング容量を持つ Premium SSD v2 マネージド ディスク、ルート ディスク、およびデータ ディスク。
- NFS、CIFS、iSCSI、NVMe/TCP データ サービスが備わった 1 つのデータ ストレージ VM がデプロイされています。追加のデータ ストレージ VM を追加することはできません。
- NFS、CIFS (SMB)、iSCSI、Autonomous Ransomware Protection (ARP)、SnapLock、および SnapMirror のライセンスがインストールされています。
- "ONTAP 温度に敏感なストレージ効率 (TSSE)"、ボリューム暗号化、および外部キー管理がデフォルトで有効になっています。
- 以下の機能はサポートされていません:
 - FabricPool の階層化
 - ストレージ VM タイプの変更
 - 高速書き込みモード

開始する前に

- 有効な Azure Marketplace サブスクリプションがあることを確認します。
- ネットワーク要件を満たしていることを確認してください"[単一 AZ での HA 展開](#)"Azure で。。 "[Cloud Volumes ONTAP用の Azure ネットワークを設定する](#)"。
- Cloud Volumes ONTAPをデプロイするには、次のいずれかの Azure ロールが割り当てられている必要があります。
 - その `contributor` デフォルトの権限を持つロール。詳細については、 "[Microsoft Azure ドキュメント: Azure 組み込みロール](#)"。
 - 次の権限を持つカスタム RBAC ロール。詳細については、 "[Azure ドキュメント: Azure カスタム ロール](#)"。

```
"permissions": [ { "actions": [ "Microsoft.AAD/register/action",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Network/loadBalancers/write", "Microsoft.ClassicCompute/virtualMachines/write",
"Microsoft.Compute/capacityReservationGroups/deploy/action",
"Microsoft.ClassicCompute/virtualMachines/networkInterfaces/associatedNetworkSecurityGroups/write", "Microsoft.Network/networkInterfaces/write", "Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Network/virtualNetworks/write", "Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Compute/disks/write",
"Microsoft.Compute/virtualMachineScaleSets/write", "Microsoft.Resources/deployments/write",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write" ], "notActions": [], "dataActions": [],
"notDataActions": [] } ]
```



リソースプロバイダー「Microsoft.storage」をサブスクリプションに登録している場合は、`Microsoft.AAD/register/action` 許可。詳細については、 "[Azure ドキュメント: ストレージの Azure アクセス許可](#)"。

手順

1. Azure Marketplace サイトから、NetApp製品を検索します。
2. * NetApp Cloud Volumes ONTAP direct*を選択します。
3. 作成 をクリックして、デプロイメント ウィザードを起動します。
4. プランを選択してください。プラン リストには通常、Cloud Volumes ONTAPの最新リリースが表示されます。
5. *基本*タブで、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。デプロイメントはサブスクリプション番号にリンクされます。
 - 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。リソース グループは、ディスクやストレージ VM などのすべてのリソースをCloud Volumes ONTAP システムの単一のグループ内に割り当てて役に立ちます。
 - リージョン: 単一の AZ での Azure HA デプロイメントをサポートするリージョンを選択します。リストには利用可能なリージョンのみが表示されます。
 - サイズ: サポートされている Premium SSD v2 マネージド ディスクのストレージ VM サイズを選択します。
 - ゾーン: 選択した地域のゾーンを選択します。
 - 管理者パスワード: パスワードを設定します。デプロイメント後にシステムにログインするには、この管理者パスワードを使用します。
 - パスワードの確認: 確認のために同じパスワードをもう一度入力します。
 - ネットワーク タブで、仮想ネットワークとサブネットを追加するか、リストから選択します。



Microsoft Azure の制限に準拠するには、新しい仮想ネットワークを設定するときに新しいサブネットを作成する必要があります。同様に、既存のネットワークを選択する場合は、既存のサブネットを選択する必要があります。

- 定義済みのネットワーク セキュリティ グループを選択するには、[はい] を選択します。必要なトラフィック ルールが定義された Azure ネットワーク セキュリティ グループを割り当てるには、[いいえ] を選択します。詳細については、"[Azure のセキュリティ グループ ルール](#)"。
- *詳細*タブで、このデプロイメントに必要な 2 つの Azure 機能が設定されているかどうかを確認します。参照"[Cloud Volumes ONTAP の単一 AZ デプロイメントで Azure 機能を有効にする](#)"そして"[AzureでCloud Volumes ONTAPの高可用性モードを有効にする](#)"。
- タグ タブで、リソースまたはリソース グループの名前と値のペアを定義できます。
- 確認 + 作成 タブで詳細を確認し、デプロイを開始します。

終了後の操作

通知アイコンを選択して、デプロイメントの進行状況を表示します。Cloud Volumes ONTAPがデプロイされた後、操作用にリストされたストレージ VM を表示できます。

アクセスできるようになったら、ONTAP System Manager またはONTAP CLI を使用して、設定した管理者認証情報でストレージ VM にログインします。その後、ボリューム、LUN、または共有を作成し、Cloud Volumes ONTAPのストレージ機能を使い始めることができます。

デプロイメントの問題のトラブルシューティング

Azure マーケットプレイスを通じて直接導入されたCloud Volumes ONTAPシステムには、NetAppからのサポートは含まれません。展開中に問題が発生した場合、独自にトラブルシューティングして解決できます。

手順

1. Azure Marketplace サイトで、ブート診断 > シリアル ログ に移動します。
2. シリアルログをダウンロードして調査します。
3. トラブルシューティングについては、製品ドキュメントとナレッジベース (KB) の記事を参照してください。
 - ["Azure マーケットプレイスのドキュメント"](#)
 - ["NetAppのドキュメント"](#)
 - ["NetApp KB記事"](#)

コンソールで展開されたシステムを検出する

Azure マーケットプレイスの直接展開を使用して展開したCloud Volumes ONTAPシステムを検出し、コンソールの システム ページで管理できます。コンソール エージェントはシステムを検出し、追加して必要なライセンスを適用し、これらのシステムに対してコンソールの全機能のロックを解除します。 PSSD v2 マネージド ディスクを使用した単一の AZ 内の元の HA 構成は保持され、システムは元のデプロイメントと同じ Azure サブスクリプションとリソース グループに登録されます。

タスク概要

Azure マーケットプレイスの直接展開を使用して展開されたCloud Volumes ONTAPシステムを検出すると、コンソール エージェントは次のタスクを実行します。

- 検出されたシステムの無料ライセンスを通常の容量ベースのライセンスに置き換えます["フリーミアムライセンス"](#)。
- 展開されたシステムの既存の機能を保持し、データ保護、データ管理、セキュリティ機能などのコンソールの追加機能を追加します。
- ノードにインストールされているライセンスを、NFS、CIFS (SMB)、iSCSI、ARP、SnapLock、およびSnapMirrorの新しいONTAPライセンスに置き換えます。
- 汎用ノードのシリアル番号を一意的シリアル番号に変換します。
- 必要に応じてリソースに新しいシステム タグを割り当てます。
- インスタンスの動的 IP アドレスを静的 IP アドレスに変換します。
- 以下の機能を有効にします["FabricPool の階層化"](#)、["AutoSupport"](#)、そして["一度書き込み、何度も読み取り"](#)展開されたシステム上の (WORM) ストレージ。必要なときにコンソールからこれらの機能を有効にすることができます。
- インスタンスを検出するために使用される NSS アカウントにインスタンスに登録します。
- 容量管理機能を有効にする["自動モードと手動モード"](#)発見されたシステムについて。

開始する前に

Azure マーケットプレイスでのデプロイが完了していることを確認します。コンソール エージェントは、展開が完了し、検出可能になった場合にのみシステムを検出できます。

手順

コンソールでは、既存のシステムを検出するための標準の手順に従います。。 ["既存のCloud Volumes ONTAP システムをコンソールに追加する"](#)。



検出中に失敗メッセージが表示される場合がありますが、検出プロセスが完了するまで無視できます。検出中に、Azure Marketplace ポータルでシステムによって生成されたCloud Volumes ONTAP構成、特にシステム タグを変更しないでください。これらの構成に変更を加えると、予期しないシステム動作が発生する可能性があります。

終了後の操作

検出が完了すると、コンソールの システム ページにリストされているシステムを表示できます。次のようなさまざまな管理タスクを実行できます。["総計を拡大する"](#)、["ボリュームの追加"](#)、["追加のストレージVMのプロビジョニング"](#)、そして["インスタンスタイプの変更"](#)。

関連リンク

ストレージの作成の詳細については、ONTAP のドキュメントを参照してください。

- ["NFS用のボリュームを作成する"](#)
- ["iSCSI用のLUNを作成する"](#)
- ["CIFSの共有を作成する"](#)

著作権に関する情報

Copyright © 2026 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。