Azure で始めましょう

Cloud Manager

NetApp
June 05, 2021

目次

Azure で始めましょう

Cloud Volumes ONTAP for Azure での作業の開始

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

コネクタを作成します

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

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

構成を計画

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

ネットワークを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 VNet からのアウトバウンドインターネットアクセスを有効にして、コネクタと Cloud Volumes ONTAP が複数のエンドポイントに接続できるようにします。

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

"ネットワーク要件の詳細については、こちらをご覧ください"。

Cloud Manager 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

- "評価中"
- "Cloud Manager からコネクタを作成します"
- "Azure Marketplace からコネクタを作成する"
- "Linux ホストへの Connector ソフトウェアのインストール"
- "クラウドマネージャーが Azure の権限で行うこと"

Azure での Cloud Volumes ONTAP 構成の計画

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。

ライセンスタイプの選択

Cloud Volumes ONTAP には、従量課金制とお客様所有のライセンスを使用（ BYOL ）の 2 種類の料金プランがあります。従量課金制の場合は、 Explore 、 Standard 、 Premium の 3 つのライセンスから選択できます。ライセンスごとに容量とコンピューティングのオプションが異なります。

"Azure で Cloud Volumes ONTAP 9.9.1 がサポートされる構成"

サポートされている **VM** タイプ

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 9.9.1 がサポートされる構成"

ストレージの制限を理解する

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 9.9.1 のストレージの制限"

Azure でのシステムのサイジング

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

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

Azure のディスクタイプ

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

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

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

Azure のディスクサイズ

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 TB のディスクを選択すると、 500 GB 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"

Flash Cache をサポートする構成を選択しています

Azure の Cloud Volumes ONTAP 構成にはローカルの NVMe ストレージが含まれており、 Cloud Volumes ONTAP はパフォーマンスを向上させるために _Flash Cache _ として使用します。 "Flash Cache の詳細については、こちらをご覧ください"。

Azure ネットワーク情報ワークシート

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）	

書き込み速度の選択

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

ボリューム使用プロファイルの選択

ONTAP には、必要なストレージの合計容量を削減できるストレージ効率化機能がいくつか搭載されています。Cloud Manager でボリュームを作成する場合は、これらの機能を有効にするプロファイルを選択する

か、無効にするプロファイルを選択できます。これらの機能の詳細については、使用するプロファイルを決定する際に役立ちます。

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

シンプロビジョニング

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

重複排除

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

圧縮

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

Azure の Cloud Volumes ONTAP のネットワーク要件

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

Cloud Volumes ONTAP の要件

Azure では、次のネットワーク要件を満たしている必要があります。

Cloud Volumes ONTAP 用のアウトバウンドインターネットアクセス

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

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

  "AutoSupport の設定方法について説明します"。

セキュリティグループ

Cloud Manager ではセキュリティグループを作成する必要がないため、セキュリティグループを作成する必要はありません。独自のルールを使用する必要がある場合は、以下のセキュリティグループルールを参照してください。

IP アドレスの数

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

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

ム上には作成されません。

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

クラウドボリューム **ONTAP** から **Azure BLOB** ストレージへの接続により、データ階層化を実現します

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

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

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

他のネットワーク内の **ONTAP** システムへの接続

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"。

コネクタの要件

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

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

ターゲットネットワークへの接続

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

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

アウトバウンドインターネットアクセス

Connector では、パブリッククラウド環境内のリソースとプロセスを管理するためにアウトバウンドインターネットアクセスが必要です。コネクタは、 Azure でリソースを管理する際に次のエンドポイントに接続します。

エンドポイント	目的
https://management.azure.com https://login.microsoftonline.com	Cloud Manager では、ほとんどの Azure リージョンに Cloud Volumes ONTAP を導入して管理できます。
https://management.microSoftazure.de https://login.microsoftonline.de	Cloud Manager は、 Azure Germany リージョンに Cloud Volumes ONTAP を導入して管理できます。

エンドポイント	目的
https://management.usgovcloudapi.net/ https://login.microsoftonline.com	Cloud Manager は、 Azure US GOV リージョンに Cloud Volumes ONTAP を導入して管理できます。
\ https://api.services.cloud.netapp.com:443	NetApp Cloud Central への API 要求。
\ https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	ソフトウェアイメージ、マニフェスト、およびテンプレートにアクセスできます。
¥ https://cognito-idp.us-east-1.amazonaws.com ¥ https://cognito-identity.us-east-1.amazonaws.com ¥ https://sts.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	コネクタがマニフェスト、テンプレート、および Cloud Volumes ONTAP アップグレードイメージにアクセスしてダウンロードできるようにします。
\ https://cloudmanagerinfraprod.azurecr.io	Docker を実行しているインフラのコンテナコンポーネントのソフトウェアイメージにアクセスでき、 Cloud Manager とのサービス統合のためのソリューションを提供します。
\ https://kinesis.us-east-1.amazonaws.com	ネットアップが監査レコードからデータをストリーミングできるようにします。
\ https://cloudmanager.cloud.netapp.com	Cloud Central アカウントを含む Cloud Manager サービスとの通信。
https://netapp-cloud-account.auth0.com	NetApp Cloud Central との通信により、ユーザ認証を一元的に行うことができます。
support.netapp.com:443 https://mysupport.netapp.com	ネットアップ AutoSupport との通信：コネクタは support.netapp.com:443 と通信し、 https://mysupport.netapp.com にリダイレクトされます。
¥ https://support.netapp.com/svcgw ¥ https://support.netapp.com/ServiceGW/entitlement ¥ https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	システムライセンスとサポート登録を行うためのネットアップとの通信
¥ https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com ¥ https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com ¥ https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	ネットアップがサポートの問題のトラブルシューティングに必要な情報を収集できるようにします。
\ https://ipa-signer.cloudmanager.netapp.com	Cloud Manager でライセンスを生成できます（ Cloud Volumes ONTAP 用の FlexCache ライセンスなど）。
* .blob.core.windows.net	プロキシを使用する場合は HA ペアに必要です。

エンドポイント	目的
次のようなさまざまなサードパーティの場所があります。 • https://repo1.maven.org/maven2 です • https://oss.sonType.org/content/repository を参照してください • \ https://repo.typesafe.com サードパーティの所在地は変更される可能性があります。	アップグレード時に、 Cloud Manager はサードパーティの依存関係に対応する最新のパッケージをダウンロードします。

SaaS ユーザインターフェイスからほとんどのタスクを実行する必要がありますが、ローカルユーザインターフェイスは引き続きコネクタで使用できます。Web ブラウザを実行するマシンは、次のエンドポイントに接続する必要があります。

エンドポイント	目的
コネクタホスト	Cloud Manager コンソールをロードするには、 Web ブラウザでホストの IP アドレスを入力する必要があります。 クラウドプロバイダへの接続に応じて、ホストに割り当てられたプライベート IP またはパブリック IP を使用できます。 • プライベート IP は、 VPN とがある場合に機能します 仮想ネットワークへの直接アクセス • パブリック IP は、あらゆるネットワークシナリオで機能します いずれの場合も、セキュリティグループのルールで許可された IP またはサブネットからのアクセスのみを許可することで、ネットワークアクセスを保護する必要があります。
¥ https://auth0.com ¥ https://cdn.auth0.com ¥ https://netapp-cloud-account.auth0.com ¥ https://services.cloud.netapp.com	Web ブラウザはこれらのエンドポイントに接続し、 NetApp Cloud Central を介してユーザ認証を一元化します。
\ https://widget.intercom.io	製品内でのチャットにより、ネットアップのクラウドエキスパートと会話できます。

Cloud Volumes ONTAP のセキュリティグループのルール

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

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

シングルノードシステムのインバウンドルール

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

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
1000 inbound_ssh	22 TCP	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
1001 INBOUND _http	80 TCP	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTP アクセス
1002 INBOUND _111_TCP	111 TCP	Any から Any	NFS のリモートプロシージャコール
1003 INBONED_111_UDP	111 UDP	Any から Any	NFS のリモートプロシージャコール
1004 INBOUND _139	139 TCP	Any から Any	CIFS の NetBIOS サービスセッション
1005 inbound_161-162_TCP	161-162 TCP	Any から Any	簡易ネットワーク管理プロトコル
1006 INBOUND _161-162_UDP	UDP 161-162	Any から Any	簡易ネットワーク管理プロトコル
1007 INBOUND _443	443 tcp	Any から Any	クラスタ管理 LIF の IP アドレスを使用した System Manager Web コンソールへの HTTPS アクセス
1008 INBOUND _445	445 TCP	Any から Any	NetBIOS フレーム同期を使用した Microsoft SMB over TCP
1009 INBOUND _635_TCP	635 TCP	Any から Any	NFS マウント
1010 INBOUND _635_UDP	635 UDP	Any から Any	NFS マウント
1011 INBOUND _749	749 TCP	Any から Any	Kerberos
1012 INBOUND _2049 _TCP	2049 TCP	Any から Any	NFS サーバデーモン
1013 INBOUND _2049 _UDP	2049 UDP	Any から Any	NFS サーバデーモン
1014 インバウンド _3260	3260 TCP	Any から Any	iSCSI データ LIF を介した iSCSI アクセス

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

HA システムのインバウンドルール

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

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

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

優先順位と名前	ポートおよびプロトコル	ソースとデスティネーションの **2** つです	説明
102 インバウンド _2049 _TCP	2049 任意のプロトコル	Any から Any	NFS サーバデーモン
111 inbound_ssh	22 すべてのプロトコル	Any から Any	クラスタ管理 LIF またはノード管理 LIF の IP アドレスへの SSH アクセス
121 INBOUND _53	53 任意のプロトコル	Any から Any	DNS と CIFS
65000 AllowVnetInBound	任意のポート任意のプロトコル	VirtualNetwork	VNet 内からのインバウンドトラフィック
65001 AllowAzureLoad BalancerInBound の略	任意のポート任意のプロトコル	AzureLoadBalancer を任意のに設定します	Azure Standard Load Balancer からのデータトラフィック
65500 DenyAllInBound	任意のポート任意のプロトコル	Any から Any	他のすべてのインバウンドトラフィックをブロックする

アウトバウンドルール

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

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

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

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

サービス	ポート	プロトコル	ソース	宛先	目的
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

コネクタのセキュリティグループルール

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

インバウンドルール

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

アウトバウンドルール

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

ルールを使用します。

基本的なアウトバウンドルール

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

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

高度なアウトバウンドルール

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

送信元 IP アドレスは、コネクタホストです。

サービス	ポート	プロトコル	宛先	目的
Active Directory	88	TCP	Active Directory フォレスト	Kerberos V 認証
	139	TCP	Active Directory フォレスト	NetBIOS サービスセッション
	389	TCP	Active Directory フォレスト	LDAP
	445	TCP	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	Active Directory フォレスト	Kerberos V パスワードの変更と設定（SET_CHANGE ）
	749	TCP	Active Directory フォレスト	Active Directory Kerberos v の変更とパスワードの設定（RPCSEC_GSS ）
	137	UDP	Active Directory フォレスト	NetBIOS ネームサービス
	138	UDP	Active Directory フォレスト	NetBIOS データグラムサービス
	464	UDP	Active Directory フォレスト	Kerberos キー管理

サービス	ポート	プロトコル	宛先	目的
API コールと AutoSupport	443	HTTPS	アウトバウンドインターネットおよび ONTAP クラスタ管理 LIF	AWS および ONTAP への API コール、およびネットアップへの AutoSupport メッセージの送信
API コール	3000	TCP	ONTAP クラスタ管理 LIF	ONTAP への API コール
DNS	53	UDP	DNS	Cloud Manager による DNS 解決に使用されます

Azure で Cloud Volumes ONTAP を起動します

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

作業を開始する前に

- 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"。

コネクタを作成するには、アカウント管理者である必要があります。最初の Cloud Volumes ONTAP 作業環境を作成する際、まだコネクタがない場合はコネクタの作成を求めるメッセージが表示されます。

- "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"。
- 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"。
- BYOL システムを導入するには、ノードごとに 20 桁のシリアル番号（ライセンスキー）が必要です。

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

データ損失の可能性があります

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。API を使用して既存のリソースグループに導入する場合、ロールバックは現在デフォルトで無効になっていますが、 Cloud Volumes ONTAP を削除すると、その共有グループから他のリソースが削除される可能性があります。

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。これはデフォルトであり、 Cloud Manager から Azure に Cloud Volumes ONTAP を導入する場合にのみ推奨されるオプションです。

手順

1. Canvas ページで、 * Add Working Environment * をクリックし、画面の指示に従います。
2. * 場所を選択 * ：「 * Microsoft * Azure * 」および「 * Cloud Volumes ONTAP シングルノード * 」また

は「 * Cloud Volumes ONTAP 高可用性 * 」を選択します。

3. * 詳細とクレデンシャル * ：必要に応じて Azure クレデンシャルとサブスクリプションを変更し、クラスタ名とリソースグループ名を指定し、必要に応じてタグを追加してから、クレデンシャルを指定します。

   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
作業環境名	Cloud Manager は、作業環境名を使用して、 Cloud Volumes ONTAP システムと Azure 仮想マシンの両方に名前を付けます。また、このオプションを選択した場合は、事前定義されたセキュリティグループのプレフィックスとして名前が使用されます。
リソースグループ名	新しいリソースグループのデフォルト名をそのまま使用するか、 [デフォルトを使用する *] をオフにして、新しいリソースグループの独自の名前を入力します。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。API を使用して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。
タグ	タグは、 Azure リソースのメタデータです。このフィールドにタグを入力すると、 Cloud Volumes ONTAP システムに関連付けられているリソースグループにタグが追加されます。作業環境を作成するときに、ユーザインターフェイスから最大 4 つのタグを追加し、作成後にさらに追加できます。API では、作業環境の作成時にタグを 4 つに制限することはありません。タグの詳細については、を参照してください "Microsoft Azure のドキュメント：「 Using tags to organize your Azure resources"。
ユーザ名とパスワード	これらは、 Cloud Volumes ONTAP クラスタ管理アカウントのクレデンシャルです。これらのクレデンシャルを使用して、 OnCommand System Manager またはその CLI を使用して Cloud Volumes ONTAP に接続できます。
資格情報を編集します	この Cloud Volumes ONTAP システムで使用する別の Azure クレデンシャルと別の Azure サブスクリプションを選択できます。従量課金制 Cloud Volumes ONTAP システムを導入するには、選択した Azure サブスクリプションに Azure Marketplace サブスクリプションを関連付ける必要があります。 "クレデンシャルを追加する方法について説明します"。

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

   ▶ https://docs.netapp.com/ja-jp/occm//media/video_subscribing_azure.mp4 *(video)*

4. * 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。
   - "Cloud Compliance の詳細はこちらをご覧ください"。
   - "Cloud Backup の詳細については、こちらをご覧ください"。
   - "監視サービスの詳細については、こちらをご覧ください"。
5. * 場所と接続性 * ：場所とセキュリティグループを選択し、チェックボックスをオンにして、コネクタとターゲットの場所の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、 Cloud Manager によってその AZ が選択されます。

6. * ライセンスとサポートサイトのアカウント * ：従量課金制または BYOL のどちらを使用するかを指定し、 NetApp Support Site のアカウントを指定します。

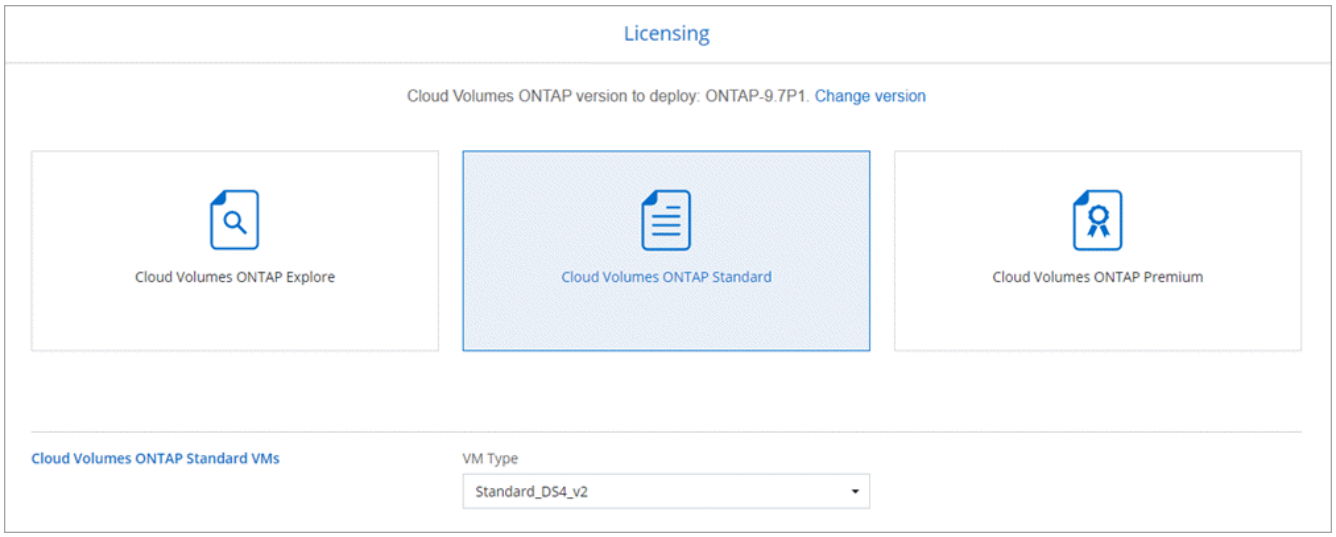
   ライセンスの仕組みについては、を参照してください "ライセンス"。

   NetApp Support Site のアカウントは、従量課金制の場合は任意ですが、 BYOL システムの場合は必須です。 "ネットアップサポートサイトのアカウントを追加する方法について説明します"。

7. * 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。

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



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

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

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

    次の点に注意してください。

    - ディスクタイプは初期ボリューム用です。以降のボリュームでは、別のディスクタイプを選択できます。
    - ディスクサイズは、最初のアグリゲート内のすべてのディスクと、シンプルプロビジョニングオプシ

ョンを使用したときに Cloud Manager によって作成される追加のアグリゲートに適用されます。Advanced Allocation オプションを使用すると、異なるディスクサイズを使用するアグリゲートを作成できます。

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

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

"データ階層化の詳細については、こちらをご覧ください。"。

11. * 書き込み速度と WORM *（シングルノードシステムのみ）： * Normal * または * High * 書き込み速度を選択し、必要に応じて Write Once 、 Read Many （ WORM ）ストレージをアクティブにします。

"書き込み速度の詳細については、こちらをご覧ください。"。

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。"。

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

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

"WORM ストレージの詳細については、こちらをご覧ください。"。

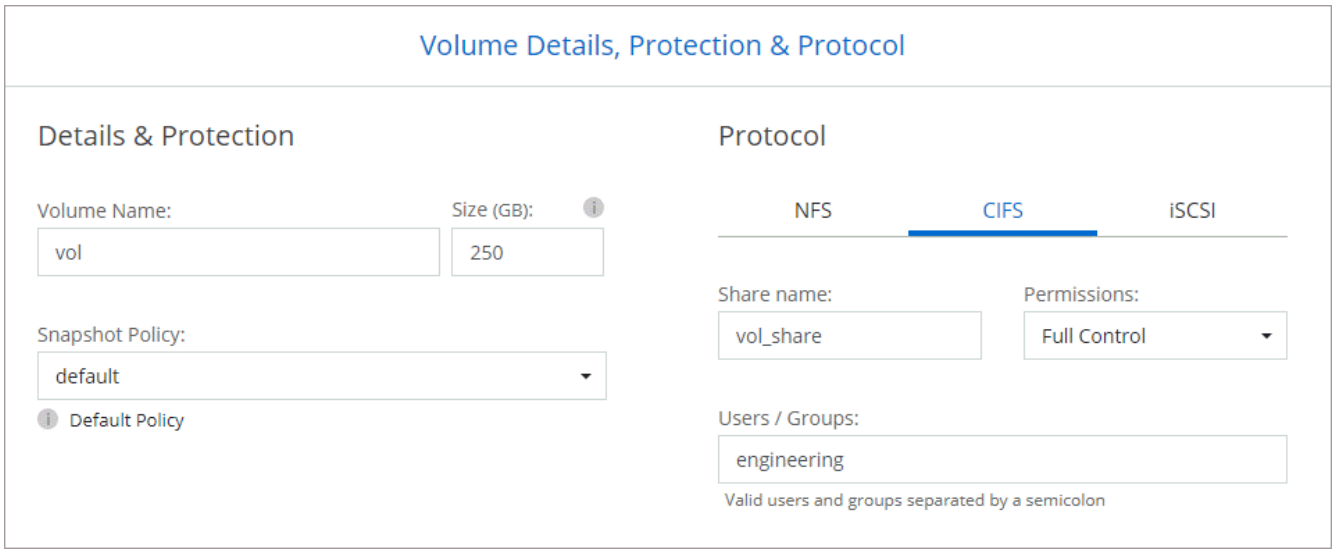
13. * ボリュームの作成 * ：新しいボリュームの詳細を入力するか、 * スキップ * をクリックします。

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

フィールド	説明
サイズ	入力できる最大サイズは、シンプロビジョニングを有効にするかどうかによって大きく異なります。シンプロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きいボリュームを作成できます。
アクセス制御（ NFS のみ）	エクスポートポリシーは、ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、 Cloud Manager はサブネット内のすべてのインスタンスへのアクセスを提供する値を入力します。
権限とユーザー / グループ（ CIFS のみ）	これらのフィールドを使用すると、ユーザおよびグループ（アクセスコントロールリストまたは ACL とも呼ばれる）の共有へのアクセスレベルを制御できます。ローカルまたはドメインの Windows ユーザまたはグループ、 UNIX ユーザまたはグループを指定できます。ドメインの Windows ユーザ名を指定する場合は、 domain\username 形式でユーザのドメインを指定する必要があります。

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

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



14. * 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。

フィールド	説明
CIFS サーバの NetBIOS 名	AD ドメイン内で一意の CIFS サーバ名。
組織単位	CIFS サーバに関連付ける AD ドメイン内の組織単位。デフォルトは CN=Computers です。Azure AD ドメインサービスを Cloud Volumes ONTAP の AD サーバとして設定するには、このフィールドに「 * OU=AADDC computers* 」または「 * OU=AADDC Users* 」と入力します。https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Azure のドキュメント：「 Create an Organizational Unit （ OU ；組織単位） in an Azure AD Domain Services managed domain"^]
DNS ドメイン	Cloud Volumes ONTAP Storage Virtual Machine （ SVM ）の DNS ドメイン。ほとんどの場合、ドメインは AD ドメインと同じです。
NTP サーバ	Active Directory DNS を使用して NTP サーバを設定するには、「 Active Directory ドメインを使用」を選択します。別のアドレスを使用して NTP サーバを設定する必要がある場合は、 API を使用してください。を参照してください "Cloud Manager API 開発者ガイド" を参照してください。

15. * 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"。

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

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

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

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

完了後

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

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