



Cloud Volumes ONTAP ドキュメント

Cloud Volumes ONTAP

NetApp
October 06, 2025

目次

Cloud Volumes ONTAPドキュメント	1
リリース ノート	2
Cloud Volumes ONTAPの新機能	2
2025年10月6日	2
2025年9月4日	2
2025年8月11日	2
2025年7月14日	3
2025年6月25日	3
2025年5月29日	4
2025年5月12日	4
2025年4月16日	4
2025年4月14日	4
2025年4月3日	4
2025年3月28日	5
2025年3月12日	5
2025年3月10日	5
2025年3月6日	5
2025年3月3日	6
2025年2月18日	6
2025年2月10日	6
2024年12月9日	7
2024年11月11日	7
2024年10月25日	8
2024年10月7日	9
2024年9月9日	9
2024年8月23日	9
2024年8月22日	9
2024年8月8日	10
2024年6月10日	10
2024年5月17日	10
2024年4月23日	11
2024年3月8日	11
2024年3月5日	11
2024年2月2日	12
2024年1月16日	12
2024年1月8日	12
2023年12月6日	12
2023年12月5日	13
2023年11月10日	13

2023年11月8日	14
2023年11月1日	14
2023年10月23日	14
2023年10月6日	14
2023年9月10日	15
2023年7月30日	15
2023年7月26日	16
2023年7月2日	16
2023年6月26日	16
2023年6月4日	16
2023年5月7日	17
2023年4月4日	18
2023年4月3日	18
2023年3月13日	20
2023年3月5日	20
2023年2月5日	21
2023年1月1日	22
2022年12月15日	22
2022年12月8日	22
2022年12月4日	23
2022年11月15日	23
2022年11月6日	23
2022年9月18日	24
2022年7月31日	25
2022年7月18日	26
2022年7月3日	27
2022年6月7日	28
2022年5月2日	29
2022年4月3日	31
2022年2月27日	32
2022年2月9日	32
2022年2月6日	32
2022年1月30日	33
2022年1月2日	33
2021年11月28日	35
2021年10月4日	36
2021年9月2日	36
2021年7月7日	36
2021年5月30日	39
2021年5月24日	40
2021年4月11日	40

2021年3月8日	40
2021年1月4日	41
2020年11月3日	43
既知の制限事項	43
コンソールはFlexGroupボリュームの作成をサポートしていません	43
コンソールはCloud Volumes ONTAPを使用したS3をサポートしていません	43
コンソールはストレージVMの災害復旧をサポートしていません	44
Cloud Volumes ONTAPリリースノート	44
始めましょう	45
Cloud Volumes ONTAPについて学ぶ	45
Cloud Volumes ONTAPデプロイメントでサポートされているONTAPバージョン	46
AWS	46
Azure	47
Google Cloud	48
Amazon Web Servicesを始める	49
AWS でのCloud Volumes ONTAPのクイックスタート	49
AWS でCloud Volumes ONTAP構成を計画する	50
ネットワークを設定する	54
AWS で顧客管理キーを使用するようにCloud Volumes ONTAP を設定する	79
Cloud Volumes ONTAPノードのAWS IAMロールを設定する	82
AWSでCloud Volumes ONTAPのライセンスを設定する	91
クイックデプロイメントを使用してAWSにCloud Volumes ONTAPをデプロイする	98
AWS でCloud Volumes ONTAP を起動	102
AWS Secret Cloud または AWS Top Secret Cloud にCloud Volumes ONTAP を導入する	115
Microsoft Azureを使い始める	132
Azure でのCloud Volumes ONTAP の展開オプションについて学習します	132
NetAppコンソールで始める	134
AzureマーケットプレイスからCloud Volumes ONTAPをデプロイする	186
Google Cloud を使い始める	190
Google Cloud でのCloud Volumes ONTAPのクイック スタート	190
Google Cloud でCloud Volumes ONTAP構成を計画する	191
Cloud Volumes ONTAP用に Google Cloud ネットワークを設定する	195
VPC Service Controls を設定して、Google Cloud にCloud Volumes ONTAP をデプロイする	207
Cloud Volumes ONTAP用の Google Cloud サービス アカウントを作成する	209
Cloud Volumes ONTAPで顧客管理の暗号化キーを使用する	212
Google Cloud でCloud Volumes ONTAPのライセンスを設定する	213
Google Cloud でCloud Volumes ONTAPを起動する	218
Google Cloud Platform イメージ検証	231
Cloud Volumes ONTAPを使用する	243
ライセンス管理	243
Cloud Volumes ONTAPの容量ベースのライセンスを管理する	243

NetAppコンソールからCloud Volumes ONTAPのKeystoneサブスクリプションを管理する	248
Cloud Volumes ONTAPのノードベースのライセンスを管理する	252
ボリュームとLUNの管理	257
Cloud Volumes ONTAPシステムにFlexVol volumeを作成する	258
Cloud Volumes ONTAPシステム上のボリュームを管理する	264
非アクティブなCloud Volumes ONTAPデータを低コストのオブジェクトストレージに階層化します	274
ホストシステムからCloud Volumes ONTAP上のLUNに接続する	283
Cloud Volumes ONTAPシステム上のFlexCacheボリュームを使用してデータ アクセスを高速化します	283
集計管理	285
Cloud Volumes ONTAPシステムのアグリゲートを作成する	285
Cloud Volumes ONTAPクラスターのアグリゲートを管理する	287
コンソールエージェントでCloud Volumes ONTAPアグリゲート容量を管理する	288
ストレージVM管理	290
Cloud Volumes ONTAPのストレージVMを管理する	290
AWS でCloud Volumes ONTAPのデータサービス ストレージ VM を管理する	291
Azure でCloud Volumes ONTAPのデータサービス ストレージ VM を管理する	299
Google Cloud でCloud Volumes ONTAPのデータ提供ストレージ VM を管理する	302
Cloud Volumes ONTAPのストレージ VM 災害復旧を設定する	305
セキュリティとデータ暗号化	305
NetApp暗号化ソリューションを使用してCloud Volumes ONTAP上のボリュームを暗号化する	305
AWS Key Management Service を使用してCloud Volumes ONTAP暗号化キーを管理する	306
Azure Key Vault を使用してCloud Volumes ONTAP暗号化キーを管理する	307
Google Cloud KMS でCloud Volumes ONTAP の暗号化キーを管理する	314
Cloud Volumes ONTAPでNetAppランサムウェア保護ソリューションを有効にする	316
Cloud Volumes ONTAPで WORM ファイルの改ざん防止スナップショット コピーを作成します	319
システム管理	320
Cloud Volumes ONTAPソフトウェアのアップグレード	320
Cloud Volumes ONTAP従量課金制システムを登録する	329
Cloud Volumes ONTAP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	331
Cloud Volumes ONTAPシステムの起動と停止	333
NTPサーバーを使用してCloud Volumes ONTAPのシステム時間を同期する	336
システムの書き込み速度を変更する	336
Cloud Volumes ONTAPクラスタ管理者のパスワードを変更する	337
システムの追加、削除、または削除	338
AWS管理	340
Azure管理	343
Google Cloud 管理	355
System Manager を使用してCloud Volumes ONTAPを管理する	357
CLIからCloud Volumes ONTAPを管理する	359
システムの健全性とイベント	360

Cloud Volumes ONTAPのAutoSupport設定を確認する	360
Cloud Volumes ONTAPシステム用の EMS を構成する	364
概念	365
ライセンス	365
Cloud Volumes ONTAPのライセンス	365
Cloud Volumes ONTAPの容量ベースのライセンスの詳細	369
ストレージ	374
Cloud Volumes ONTAPでサポートされているクライアント プロトコル	374
Cloud Volumes ONTAPクラスターに使用されるディスクとアグリゲート	374
Cloud Volumes ONTAPによる AWS Elastic Volumes のサポートについて学ぶ	377
AWS、Azure、Google Cloud でのCloud Volumes ONTAPによるデータ階層化について学習します	383
Cloud Volumes ONTAPストレージ管理	388
書き込み速度	390
Flash Cache	393
Cloud Volumes ONTAPの WORM ストレージについて学ぶ	394
ハイアベイラビリティ ペア	396
AWS のCloud Volumes ONTAP HA ペアについて学ぶ	396
Azure のCloud Volumes ONTAP HA ペアについて学ぶ	403
Google Cloud のCloud Volumes ONTAP HA ペアについて学ぶ	409
Cloud Volumes ONTAP HAペアのノードがオフラインの場合、操作は利用できません	414
Cloud Volumes ONTAP のデータ暗号化とランサムウェア保護について学ぶ	415
保存中のデータを暗号化	415
ONTAPウイルススキャン	417
ランサムウェア対策	417
Cloud Volumes ONTAPワークロードのパフォーマンス監視について学ぶ	418
パフォーマンス技術レポート	418
CPUパフォーマンス	418
ノードベースBYOLのライセンス管理	419
BYOLシステムライセンス	419
新しいシステムのライセンス管理	419
ライセンスの有効期限	419
ライセンスの更新	420
新しいシステムへのライセンスの移行	420
Cloud Volumes ONTAPでAutoSupportとDigital Advisor がどのように使用されるかを学びます	420
Cloud Volumes ONTAPでサポートされているデフォルト構成	421
デフォルト設定	421
システムデータ用の内部ディスク	423
知識とサポート	427
サポートに登録する	427
サポート登録の概要	427
NetAppサポートのためにBlueXPに登録する	427

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける	430
ヘルプを受ける	431
クラウドプロバイダーのファイルサービスのサポートを受ける	431
セルフサポートオプションを使用する	432
NetAppサポートでケースを作成する	432
サポートケースを管理する（プレビュー）	434
法律上の表示	437
著作権	437
商標	437
特許	437
プライバシー ポリシー	437
オープンソース	437

Cloud Volumes ONTAP ドキュメント

リリース ノート

Cloud Volumes ONTAPの新機能

NetAppコンソールのCloud Volumes ONTAP管理の新機能について説明します。

このページで説明する機能強化は、コンソールを介したCloud Volumes ONTAP の管理に特有のものです。Cloud Volumes ONTAPソフトウェア自体の新機能については、"[Cloud Volumes ONTAPリリースノートをご覧ください](#)"。

2025年10月6日

BlueXPはNetAppコンソールになりました

NetAppコンソールは、強化され再構築されたBlueXP基盤上に構築され、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとNetAppデータ サービスの集中管理を提供し、リアルタイムの分析情報、ワークフローの高速化、および高度なセキュリティとコンプライアンスを備えた簡素化された管理を実現します。

変更内容の詳細については、"[NetAppコンソールのリリースノート](#)"。

AWS でのCloud Volumes ONTAP の導入を簡素化

シングルノード構成と高可用性 (HA) 構成の両方で、クイック デプロイメント メソッドを使用して、AWS にCloud Volumes ONTAP をデプロイメントできるようになりました。この合理化されたプロセスにより、高度な方法に比べて手順数が削減され、1 ページにデフォルト値が自動的に設定され、ナビゲーションが最小限に抑えられ、展開がより迅速かつ容易になります。

```
https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-quick-deploy-aws.html["クイックデプロイメントを使用してAWSにCloud Volumes ONTAPをデプロイする"^] 。
```

2025年9月4日

Cloud Volumes ONTAP 9.17.1RC

BlueXPを使用して、Azure および Google Cloud でCloud Volumes ONTAP 9.17.1 のリリース候補 1 をデプロイおよび管理できるようになりました。ただし、このバージョンは AWS でのデプロイおよびアップグレードには使用できません。

"[Cloud Volumes ONTAPのこのリリースの詳細](#)"。

2025年8月11日

最適化ライセンスの提供終了

2025 年 8 月 11 日以降、Cloud Volumes ONTAP Optimized ライセンスは廃止され、Azure および Google

Cloud マーケットプレイスの従量課金制 (PAYGO) サブスクリプションで購入または更新できなくなります。Optimized ライセンスの年間契約を既に締結している場合は、契約終了までライセンスを引き続きご利用いただけます。Optimized ライセンスの有効期限が切れると、BlueXPでCloud Volumes ONTAP Essentials または Professional ライセンスを選択できます。

ただし、最適化されたライセンスを追加または更新する機能は、API を通じて利用できるようになります。

ライセンスパッケージの詳細については、以下を参照してください。 ["Cloud Volumes ONTAPのライセンス"](#)。

別の充電方法への切り替えについては、 ["容量ベースのライセンスを管理する"](#)。

2025年7月14日

透過プロキシのサポート

BlueXP は、既存の明示的なプロキシ接続に加えて、透過プロキシ サーバーをサポートするようになりました。BlueXPコネクタを作成または変更するときに、透過プロキシ サーバーを構成して、Cloud Volumes ONTAPとの間のネットワーク トラフィックを安全に管理できます。

Cloud Volumes ONTAPでのプロキシ サーバーの使用の詳細については、以下を参照してください。

- ["AWS でコネクタ プロキシをサポートするためのネットワーク構成"](#)
- ["Azure でコネクタ プロキシをサポートするためのネットワーク構成"](#)
- ["Google Cloud でコネクタ プロキシをサポートするためのネットワーク構成"](#)

Azure のCloud Volumes ONTAPでサポートされる新しい VM タイプ

Cloud Volumes ONTAP 9.13.1 以降、L8s_v3 は、新規および既存の高可用性 (HA) ペアの展開の両方で、Azure の単一および複数の可用性ゾーンの VM タイプとしてサポートされます。

詳細については、 ["Azureでサポートされている構成"](#)。

2025年6月25日

Cloud Volumes ONTAPの BYOL ライセンスの利用制限

2025年6月25日より、NetAppはCloud Volumes ONTAPのBYOL (Bring Your Own License) ライセンスモデルを制限いたします。この制限は、AWS、Azure、Google Cloudのすべてのお客様とCloud Volumes ONTAP 導入環境に適用されます。例外となるのは、米国公共部門のお客様と中国リージョンの導入環境です。

NetAppのサポートとサービスはBYOL契約の有効期限まで継続されますが、有効期限切れのライセンスは更新または延長されません。BYOLライセンスの有効期限が切れた場合は、クラウドマーケットプレイスのサブスクリプションを通じて容量ベースのライセンスを購入して切り替える必要があります。ハイパースケーラマーケットプレイスを通じた容量ベースのライセンスモデルは、ライセンス手続きを効率化し、より大きなビジネスメリットをもたらします。切り替えのオプションについてご相談いただくには、NetAppアカウントチームまたはカスタマーサクセス担当者までお問い合わせください。

詳細については、次の顧客向け通信を参照してください。 ["CPC-00661: Cloud Volumes ONTAP BYOLポリシーの変更"](#)。

2025年5月29日

Cloud Volumes ONTAP 9.15.1 でプライベート モードのデプロイメントが有効になりました

AWS、Azure、Google Cloud でCloud Volumes ONTAP 9.15.1 をプライベート モードでデプロイできるようになりました。プライベート モードは、Cloud Volumes ONTAP 9.15.1 のシングル ノードと高可用性 (HA) の両方の展開で有効になります。

プライベートモードの展開の詳細については、以下を参照してください。<https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["BlueXPの展開モードについて学ぶ"]。

2025年5月12日

BlueXPの Azure マーケットプレイスを通じて行われたデプロイメントの検出

BlueXPには、Azure マーケットプレイスを通じて直接導入されたCloud Volumes ONTAPシステムを検出できる機能が追加されました。つまり、他のCloud Volumes ONTAPシステムと同様に、これらのシステムをBlueXPの作業環境として追加および管理できるようになりました。

["AzureマーケットプレイスからCloud Volumes ONTAPをデプロイする"](#)

2025年4月16日

Azure でサポートされる新しいリージョン

次のリージョンの Azure の単一および複数のアベイラビリティゾーンにCloud Volumes ONTAP 9.12.1 GA以降をデプロイできるようになりました。これには、単一ノードと高可用性 (HA) の両方の展開のサポートが含まれます。

- スペイン中部
- メキシコ中央

すべての地域の一覧については、["Azure のグローバル地域マップ"](#)。

2025年4月14日

Google Cloud の API を通じてストレージ VM の作成を自動化

BlueXP API を使用して、Google Cloud でのストレージ VM の作成を自動化できるようになりました。この機能は、Cloud Volumes ONTAP の高可用性 (HA) 構成で使用されていましたが、単一ノードの展開でも使用できるようになりました。BlueXP API を使用すると、必要なネットワーク インターフェース、LIF、管理 LIFを手動で構成する必要なく、Google Cloud 環境で追加のデータ提供ストレージ VM を簡単に作成、名前変更、削除できます。この自動化により、ストレージ VM の管理プロセスが簡素化されます。

["Google Cloud でCloud Volumes ONTAPのデータ提供ストレージ VM を管理する"](#)

2025年4月3日

AWS の Cloud Volumes ONTAP 9.13.1 の中国リージョンのサポート

中国リージョンの AWS に Cloud Volumes ONTAP 9.13.1 をデプロイできるようになりました。これには、単一ノードと高可用性 (HA) の両方の展開のサポートが含まれます。NetApp から直接購入したライセンスのみがサポートされます。

地域ごとの提供状況については、"[Cloud Volumes ONTAP のグローバル リージョン マップ](#)"。

2025年3月28日

Cloud Volumes ONTAP 9.14.1 でプライベート モードのデプロイメントが有効になりました

AWS、Azure、Google Cloud で Cloud Volumes ONTAP 9.14.1 をプライベート モードでデプロイできるようになりました。プライベート モードは、Cloud Volumes ONTAP 9.14.1 のシングル ノードと高可用性 (HA) の両方の展開で有効になります。

プライベートモードの展開の詳細については、以下を参照してください。 <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-modes.html#restricted-mode>["BlueXP の展開モードについて学ぶ"]。

2025年3月12日

Azure の複数の可用性ゾーンの展開でサポートされる新しいリージョン

Cloud Volumes ONTAP 9.12.1 GA 以降では、次のリージョンで Azure の HA 複数可用性ゾーンの展開がサポートされるようになりました。

- 米国中部
- US Gov Virginia (米国政府地域 - バージニア州)

すべての地域のリストについては、"[Azure のグローバル地域マップ](#)"。

2025年3月10日

Azure の API を通じてストレージ VM の作成を自動化

BlueXP API を使用して、Azure の Cloud Volumes ONTAP 用の追加データ提供ストレージ VM を作成、名前変更、削除できるようになりました。API を使用すると、管理目的でストレージ VM を使用する必要がある場合、必要なネットワーク インターフェイス、LIF、管理 LIF の構成を含む、ストレージ VM の作成プロセスが自動化されます。

"[Azure で Cloud Volumes ONTAP のデータサービス ストレージ VM を管理する](#)"

2025年3月6日

Cloud Volumes ONTAP 9.16.1 GA

BlueXP を使用して、Azure および Google Cloud で Cloud Volumes ONTAP 9.16.1 一般提供リリースを展開および管理できるようになりました。ただし、このバージョンは AWS でのデプロイおよびアップグレードには使用できません。

"[Cloud Volumes ONTAP のこのリリースに含まれる新機能について学びましょう](#)"。

2025年3月3日

Azure のニュージーランド北部リージョンのサポート

Cloud Volumes ONTAP 9.12.1 GA 以降の単一ノードおよび高可用性 (HA) 構成では、Azure でニュージーランド北部リージョンがサポートされるようになりました。このリージョンでは Lsv3 インスタンス タイプはサポートされていないことに注意してください。

サポートされているすべての地域のリストについては、["Azure のグローバル地域マップ"](#)。

2025年2月18日

Azure マーケットプレイス直接展開のご紹介

Azure マーケットプレイスの直接展開を利用して、Azure マーケットプレイスから Cloud Volumes ONTAP を簡単かつ迅速に直接展開できるようになりました。この合理化された方法を使用すると、BlueXPコネクタをセットアップしたり、BlueXPを介して Cloud Volumes ONTAP を展開するために必要なその他のオンボーディング基準を満たしたりすることなく、環境内で Cloud Volumes ONTAP のコア機能や機能を探索できます。

- ["Azure での Cloud Volumes ONTAP の展開オプションについて学習します"](#)
- ["Azure マーケットプレイスから Cloud Volumes ONTAP をデプロイする"](#)

2025年2月10日

BlueXP から System Manager にアクセスするためのユーザー認証が有効になりました

BlueXP 管理者は、BlueXP から ONTAP System Manager にアクセスする ONTAP ユーザーの認証をアクティブ化できるようになりました。BlueXP Connector 設定を編集することで、このオプションを有効にすることができます。このオプションは標準モードとプライベートモードで使用できます。

["System Manager を使用して Cloud Volumes ONTAP を管理する"](#)。

BlueXP Advanced View が System Manager に名称変更されました

ONTAP System Manager を介して BlueXP から Cloud Volumes ONTAP を詳細に管理するためのオプションの名前が、**Advanced View** から **System Manager** に変更されました。

["System Manager を使用して Cloud Volumes ONTAP を管理する"](#)。

BlueXP digital wallet でライセンスをより簡単に管理する方法をご紹介します

BlueXP digital wallet 内の改善されたナビゲーション ポイントを使用することで、Cloud Volumes ONTAP ライセンスの管理が簡素化されました。

- 管理 > ライセンスとサブスクリプション > 概要/直接ライセンス タブから、Cloud Volumes ONTAP ライセンス情報に簡単にアクセスできます。
- 容量ベースのライセンスを包括的に理解するには、[概要] タブの Cloud Volume ONTAP パネルで [表示] をクリックします。この詳細ビューでは、ライセンスとサブスクリプションに関する詳細な情報が表示されます。
- 以前のインターフェースを希望する場合は、[従来のビューに切り替える] ボタンをクリックして、ライセ

ンスの詳細をタイプ別に表示し、ライセンスの課金方法を変更できます。

["容量ベースのライセンスを管理する"](#)。

2024年12月9日

ベストプラクティスに合わせて **Azure** でサポートされる **VM** のリストが更新されました

Azure にCloud Volumes ONTAPの新しいインスタンスを展開するときに、DS_v2 および Es_v3 マシン ファミリーはBlueXPで選択できなくなりました。これらのファミリーは、古い既存のシステムでのみ保持され、サポートされます。Cloud Volumes ONTAPの新しいデプロイメントは、9.12.1 リリース以降でのみ Azure でサポートされます。Es_v4 またはCloud Volumes ONTAP 9.12.1 以降と互換性のある他のシリーズに切り替えることをお勧めします。ただし、DS_v2 および Es_v3 シリーズのマシンは、API を通じて行われる新しいデプロイメントでは利用できるようになります。

["Azureでサポートされている構成"](#)

2024年11月11日

ノードベースライセンスの提供終了

NetApp は、Cloud Volumes ONTAPノードベース ライセンスの提供終了 (EOA) とサポート終了 (EOS) を計画しています。2024 年 11 月 11 日をもって、ノードベースのライセンスの限定提供は終了しました。ノードベースのライセンスのサポートは、2024 年 12 月 31 日に終了します。ノードベースのライセンスの EOA 後は、BlueXPライセンス変換ツールを使用して容量ベースのライセンスに移行する必要があります。

年間契約または長期契約の場合、NetApp、EOA 日付またはライセンス有効期限の前にNetApp の担当者に連絡して、移行の前提条件が満たされていることを確認することをお勧めします。Cloud Volumes ONTAPノードの長期契約がなく、オンデマンドの従量課金制 (PAYGO) サブスクリプションに対してシステムを実行している場合は、EOS 日付の前に変換を計画することが重要です。長期契約と PAYGO サブスクリプションの両方において、BlueXPライセンス変換ツールを使用してシームレスな変換を行うことができます。

["ノードベースライセンスの提供終了"](#) ["Cloud Volumes ONTAP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"](#)

BlueXPからのノードベースのデプロイメントの削除

ノードベースのライセンスを使用してCloud Volumes ONTAPシステムを展開するオプションは、BlueXPでは非推奨です。いくつかの特殊なケースを除き、どのクラウド プロバイダーでも、Cloud Volumes ONTAPデプロイメントにノードベースのライセンスを使用することはできません。

NetApp は、契約上の義務と運用上のニーズに準拠する次の固有のライセンス要件を認識しており、これらの状況でノードベースのライセンスを引き続きサポートします。

- 米国公共部門の顧客
- プライベートモードでのデプロイメント
- AWS におけるCloud Volumes ONTAPの中国リージョン展開
- 有効で期限切れでないノードごとのライセンス (BYOLライセンス) をお持ちの場合

["ノードベースライセンスの提供終了"](#)

Azure Blob ストレージ上のCloud Volumes ONTAPデータ用のコールド層の追加

BlueXPでは、Azure Blob ストレージに非アクティブな容量層データを保存するためにコールド層を選択できるようになりました。既存のホット層とクール層にコールド層を追加すると、より手頃なストレージ オプションが提供され、コスト効率が向上します。

["Azure のデータ階層化"](#)

Azure のストレージ アカウントへのパブリック アクセスを制限するオプション

Azure のCloud Volumes ONTAPシステムのストレージ アカウントへのパブリック アクセスを制限するオプションが追加されました。アクセスを無効にすると、組織のセキュリティ ポリシーに準拠する必要がある場合でも、同じ VNet 内であってもプライベート IP アドレスが公開されることを防ぐことができます。このオプションは、Cloud Volumes ONTAPシステムのデータ階層化も無効にし、単一ノードと高可用性ペアの両方に適用できます。

["セキュリティグループルール"](#)。

Cloud Volumes ONTAP導入後の WORM 有効化

BlueXPを使用して、既存のCloud Volumes ONTAPシステムで、Write Once、Read Many (WORM) ストレージをアクティブ化できるようになりました。この機能により、作成時に WORM が有効になっていなかった場合でも、作業環境で WORM を有効にする柔軟性が得られます。一度有効にすると、WORM を無効にすることはできません。

["Cloud Volumes ONTAP作業環境で WORM を有効にする"](#)

2024年10月25日

Google Cloud でサポートされる VM のリストがベスト プラクティスに合わせて更新されました

Google Cloud でCloud Volumes ONTAPの新しいインスタンスをデプロイするときに、n1 シリーズ マシンはBlueXPで選択できなくなりました。n1 シリーズのマシンは、古い既存のシステムでのみ保持され、サポートされます。Cloud Volumes ONTAPの新しいデプロイメントは、Google Cloud 9.8 リリース以降でのみサポートされます。Cloud Volumes ONTAP 9.8 以降と互換性のある n2 シリーズのマシン タイプに切り替えることをお勧めします。ただし、n1 シリーズのマシンは、API を通じて実行される新しいデプロイメントに使用できません。

["Google Cloud でサポートされている構成"](#)。

プライベートモードでの Amazon Web Services のローカルゾーンのサポート

BlueXP は、プライベート モードでのCloud Volumes ONTAP高可用性 (HA) デプロイメント用の AWS ローカルゾーンをサポートするようになりました。以前は標準モードのみに限定されていたサポートが、プライベート モードまで拡張されました。



BlueXP を制限モードで使用する場合、AWS ローカルゾーンはサポートされません。

HAデプロイメントを備えたAWSローカルゾーンの詳細については、以下を参照してください。["AWS ローカルゾーン"](#)。

2024年10月7日

アップグレードのバージョン選択におけるユーザーエクスペリエンスの向上

このリリース以降、BlueXP通知を使用してCloud Volumes ONTAPをアップグレードしようとする、使用するデフォルト、最新バージョン、互換性のあるバージョンに関するガイダンスが表示されます。また、Cloud Volumes ONTAPインスタンスと互換性のある最新のパッチまたはメジャーバージョンを選択したり、アップグレードするバージョンを手動で入力したりできるようになりました。

["Cloud Volumes ONTAPソフトウェアのアップグレード"](#)

2024年9月9日

WORMとARP機能は課金対象外となりました

WORM (Write Once Read Many) と ARP (Autonomous Ransomware Protection) の組み込みデータ保護およびセキュリティ機能は、Cloud Volumes ONTAPライセンスで追加料金なしで提供されます。新しい価格モデルは、AWS、Azure、Google Cloud の新規および既存の BYOL と PAYGO/マーケットプレースのサブスクリプションの両方に適用されます。容量ベースとノードベースの両方のライセンスには、単一ノードと高可用性 (HA) ペアを含むすべての構成の ARP と WORM が追加費用なしで含まれます。

簡素化された価格設定により、次のようなメリットがもたらされます。

- 現在 WORM と ARP が含まれているアカウントでは、これらの機能に対して料金が発生しなくなります。今後は、この変更以前と同様に、容量使用量に対する料金のみが請求されます。今後の請求書には WORM と ARP は含まれなくなります。
- 現在のアカウントにこれらの機能が含まれていない場合は、追加料金なしで WORM と ARP を選択できるようになりました。
- 新規アカウントのすべてのCloud Volumes ONTAPサービスでは、WORM と ARP の料金は除外されます。

これらの機能の詳細については、以下をご覧ください。

- ["Cloud Volumes ONTAPでNetAppランサムウェア保護ソリューションを有効にする"](#)
- ["WORMストレージ"](#)

2024年8月23日

AWS でカナダ西部リージョンのサポートが開始されました

Cloud Volumes ONTAP 9.12.1 GA 以降では、カナダ西部リージョンが AWS でサポートされるようになりました。

すべての地域のリストについては、["AWS のグローバルリージョンマップ"](#)。

2024年8月22日

Cloud Volumes ONTAP 9.15.1 GA

BlueXP は、AWS、Azure、Google Cloud でCloud Volumes ONTAP 9.15.1 一般提供リリースを展開および管

理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2024年8月8日

Edge Cache ライセンス パッケージは廃止されました

Edge Cache 容量ベースのライセンス パッケージは、Cloud Volumes ONTAPの今後の展開では利用できなくなります。ただし、API を使用してこの機能を利用することができます。

Azure の Flash Cache の最小バージョン サポート

Azure で Flash Cache を構成するために必要な最小のCloud Volumes ONTAPバージョンは 9.13.1 GA です。Azure のCloud Volumes ONTAPシステムに Flash Cache をデプロイするには、ONTAP 9.13.1 GA 以降のバージョンのみを使用できます。

サポートされている構成については、["Azureでサポートされている構成"](#)。

マーケットプレイスサブスクリプションの無料トライアルは廃止されました

クラウド プロバイダーのマーケットプレイスにおける従量課金制サブスクリプションの 30 日間の自動無料トライアルまたは評価ライセンスは、Cloud Volumes ONTAPでは利用できなくなります。マーケットプレイスのあらゆるタイプのサブスクリプション（PAYGO または年間契約）の課金は、無料試用期間なしで、最初の使用から有効になります。

2024年6月10日

Cloud Volumes ONTAP 9.15.0

BlueXP は、AWS、Azure、Google Cloud でCloud Volumes ONTAP 9.15.0 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2024年5月17日

Amazon Web Services ローカルゾーンのサポート

Cloud Volumes ONTAP HA デプロイメントで AWS ローカルゾーンのサポートが利用できるようになりました。AWS ローカルゾーンは、ストレージ、コンピューティング、データベース、およびその他の厳選された AWS サービスが大都市や産業地域の近くに配置されているインフラストラクチャ展開です。



BlueXP を標準モードで使用する場合、AWS ローカルゾーンがサポートされます。現時点では、BlueXP を制限モードまたはプライベートモードで使用する場合、AWS ローカルゾーンはサポートされません。

HAデプロイメントを備えたAWSローカルゾーンの詳細については、以下を参照してください。["AWS ローカルゾーン"](#)。

2024年4月23日

Azure の複数の可用性ゾーンの展開でサポートされる新しいリージョン

Cloud Volumes ONTAP 9.12.1 GA 以降では、次のリージョンで Azure の HA 複数可用性ゾーンの展開がサポートされるようになりました。

- ドイツ西中部
- ポーランド中央
- 米国西部3
- イスラエル中央
- イタリア北部
- カナダ中部

すべての地域のリストについては、["Azure のグローバル地域マップ"](#)。

Google Cloud でヨハネスブルグ リージョンがサポートされるようになりました

ヨハネスブルグ地域(`africa-south1` Google Cloud for Cloud Volumes ONTAP 9.12.1 GA 以降では、リージョンがサポートされるようになりました。

すべての地域のリストについては、["Google Cloud のグローバル地域マップ"](#)。

ボリュームテンプレートとタグはサポートされなくなりました

テンプレートからボリュームを作成したり、ボリュームのタグを編集したりすることはできなくなりました。これらのアクションは、現在は利用できなくなったBlueXP修復サービスに関連付けられていました。

2024年3月8日

Amazon インスタントメタデータサービス v2 のサポート

AWS では、Cloud Volumes ONTAP、Mediator、および Connector がすべての機能で Amazon Instant Metadata Service v2 (IMDSv2) をサポートするようになりました。IMDSv2 は脆弱性に対する保護を強化します。以前は IMDSv1 のみがサポートされていました。

セキュリティ ポリシーで必要な場合は、IMDSv2 を使用するように EC2 インスタンスを設定できます。手順については、["既存のコネクタを管理するためのBlueXP のセットアップおよび管理ドキュメント"](#)。

2024年3月5日

Cloud Volumes ONTAP 9.14.1 GA

BlueXP は、AWS、Azure、Google Cloud で Cloud Volumes ONTAP 9.14.1 一般提供リリースを展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2024年2月2日

Azure での **Edv5** シリーズ **VM** のサポート

Cloud Volumes ONTAP は、9.14.1 リリース以降、次の Edv5 シリーズ VM をサポートするようになりました。

- E4ds_v5
- E8ds_v5
- E20s_v5
- E32ds_v5
- E48ds_v5
- E64ds_v5

["Azureでサポートされている構成"](#)

2024年1月16日

BlueXPのパッチリリース

パッチ リリースは、BlueXPで、Cloud Volumes ONTAPの最新の 3 つのバージョンに対してのみ利用できます。

["Cloud Volumes ONTAP のアップグレード"](#)

2024年1月8日

Azure の複数の可用性ゾーン向けの新しい **VM**

Cloud Volumes ONTAP 9.13.1 以降、次の VM タイプは、新規および既存の高可用性ペアの展開に対して Azure の複数の可用性ゾーンをサポートします。

- L16s_v3
- L32s_v3
- L48s_v3
- L64s_v3

["Azureでサポートされている構成"](#)

2023年12月6日

Cloud Volumes ONTAP 9.14.1 RC1

BlueXP は、AWS、Azure、Google Cloud でCloud Volumes ONTAP 9.14.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

300 TiB FlexVol volumeの上限

Cloud Volumes ONTAP 9.12.1 P2 および 9.13.0 P2 以降では System Manager と ONTAP CLI を使用して、また Cloud Volumes ONTAP 9.13.1 以降では BlueXP を使用して、最大サイズ 300 TiB までの FlexVol volume を作成できるようになりました。

- ["AWSのストレージ制限"](#)
- ["Azure のストレージ制限"](#)
- ["Google Cloud のストレージ制限"](#)

2023年12月5日

以下の変更が導入されました。

Azure の新しいリージョンのサポート

単一のアベイラビリティゾーンリージョンのサポート

Cloud Volumes ONTAP 9.12.1 GA 以降では、次のリージョンで Azure の高可用性単一可用性ゾーンのデプロイメントがサポートされるようになりました。

- テルアビブ
- ミラノ

複数のアベイラビリティゾーンリージョンのサポート

Cloud Volumes ONTAP 9.12.1 GA 以降では、次のリージョンで Azure の高可用性の複数可用性ゾーンのデプロイメントがサポートされるようになりました。

- インド中部
- ノルウェー東部
- スイス北部
- 南アフリカ北部
- アラブ首長国連邦北部

すべての地域のリストについては、["Azure のグローバル地域マップ"](#)。

2023年11月10日

コネクタの 3.9.35 リリースでは、次の変更が導入されました。

Google Cloud でベルリン リージョンがサポートされるようになりました

Google Cloud の Cloud Volumes ONTAP 9.12.1 GA 以降では、ベルリン リージョンがサポートされるようになりました。

すべての地域のリストについては、["Google Cloud のグローバル地域マップ"](#)。

2023年11月8日

コネクタの 3.9.35 リリースでは、次の変更が導入されました。

AWSでテルアビブリージョンがサポートされるようになりました

Cloud Volumes ONTAP 9.12.1 GA 以降では、テルアビブ リージョンが AWS でサポートされるようになりました。

すべての地域のリストについては、"[AWS のグローバルリージョンマップ](#)"。

2023年11月1日

コネクタの 3.9.34 リリースでは、次の変更が導入されました。

Google Cloud でサウジアラビア リージョンがサポートされるようになりました

Google Cloud のCloud Volumes ONTAPおよび Connector for Cloud Volumes ONTAP 9.12.1 GA 以降で、サウジアラビア リージョンがサポートされるようになりました。

すべての地域のリストについては、"[Google Cloud のグローバル地域マップ](#)"。

2023年10月23日

コネクタの 3.9.34 リリースでは、次の変更が導入されました。

Azure の **HA** マルチアベイラビリティゾーン展開でサポートされる新しいリージョン

Azure の次のリージョンでは、Cloud Volumes ONTAP 9.12.1 GA 以降の高可用性の複数の可用性ゾーンの展開がサポートされるようになりました。

- オーストラリア東部
- 東アジア
- フランス中部
- 北ヨーロッパ
- カタール中央
- スウェーデン中央
- 西ヨーロッパ
- 米国西部2

複数のアベイラビリティゾーンをサポートするすべてのリージョンのリストについては、"[Azure のグローバル地域マップ](#)"。

2023年10月6日

コネクタの 3.9.34 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.14.0

BlueXP は、AWS、Azure、Google Cloud で Cloud Volumes ONTAP 9.14.0 一般提供リリースを展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2023年9月10日

コネクタの 3.9.33 リリースでは、次の変更が導入されました。

Azure での Lsv3 シリーズ VM のサポート

9.13.1 リリース以降、L48s_v3 および L64s_v3 インスタンス タイプが、単一および複数の可用性ゾーンでの共有管理対象ディスクを使用した単一ノードおよび高可用性ペアの展開で、Azure の Cloud Volumes ONTAP でサポートされるようになりました。これらのインスタンス タイプは Flash Cache をサポートします。

["Azure で Cloud Volumes ONTAP がサポートする構成を表示する"](#) ["Azure の Cloud Volumes ONTAP のストレージ制限を表示する"](#)

2023年7月30日

コネクタの 3.9.32 リリースでは、次の変更が導入されました。

Google Cloud のフラッシュ キャッシュと高速書き込みのサポート

Google Cloud for Cloud Volumes ONTAP 9.13.1 以降では、Flash Cache と高速書き込み速度を個別に有効にできます。サポートされているすべてのインスタンス タイプで、高速書き込み速度を利用できます。Flash Cache は次のインスタンス タイプでサポートされています。

- n2-標準-16
- n2-標準-32
- n2-標準-48
- n2-標準-64

これらの機能は、単一ノードと高可用性ペアの両方の展開で個別に、または一緒に使用できます。

["Google Cloud で Cloud Volumes ONTAP を起動する"](#)

使用状況レポートの機能強化

使用状況レポート内に表示される情報にさまざまな改善が加えられました。使用状況レポートの機能強化は次のとおりです。

- 列名に TiB 単位が含まれるようになりました。
- シリアル番号用の新しい「ノード」フィールドが追加されました。
- ストレージ VM 使用状況レポートに新しい「ワークロード タイプ」列が追加されました。
- 作業環境名がストレージ VM およびボリューム使用状況レポートに含まれるようになりました。

- ボリューム タイプ「ファイル」のラベルが「プライマリ (読み取り/書き込み)」になりました。
- ボリューム タイプ「セカンダリ」のラベルが「セカンダリ (DP)」に変更されました。

使用状況レポートの詳細については、以下を参照してください。 ["使用状況レポートをダウンロードする"](#)。

2023年7月26日

コネクタの 3.9.31 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.13.1 GA

BlueXP は、AWS、Azure、Google Cloud で Cloud Volumes ONTAP 9.13.1 一般提供リリースを展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2023年7月2日

コネクタの 3.9.31 リリースでは、次の変更が導入されました。

Azure での HA 複数可用性ゾーン展開のサポート

Azure の日本東部と韓国中部では、Cloud Volumes ONTAP 9.12.1 GA 以降の HA 複数可用性ゾーンの展開がサポートされるようになりました。

複数のアベイラビリティゾーンをサポートするすべてのリージョンのリストについては、["Azure のグローバル地域マップ"](#)。

自律型ランサムウェア保護のサポート

Autonomous Ransomware Protection (ARP) が Cloud Volumes ONTAP でサポートされるようになりました。ARP サポートは、Cloud Volumes ONTAP バージョン 9.12.1 以降で利用できます。

Cloud Volumes ONTAP を使用した ARP の詳細については、以下を参照してください。 ["自律型ランサムウェア対策"](#)。

2023年6月26日

コネクタの 3.9.30 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.13.1 RC1

BlueXP は、AWS、Azure、Google Cloud で Cloud Volumes ONTAP 9.13.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2023年6月4日

コネクタの 3.9.30 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAPアップグレード バージョン セレクターの更新

「Cloud Volumes ONTAP のアップグレード」ページから、Cloud Volumes ONTAPの最新バージョンにアップグレードするか、古いバージョンにアップグレードするかを選択できるようになりました。

BlueXP経由でCloud Volumes ONTAPをアップグレードする方法の詳細については、以下を参照してください。"[Cloud Volumes ONTAP のアップグレード](#)"。

2023年5月7日

コネクタの 3.9.29 リリースでは、次の変更が導入されました。

Google Cloud でカタルーニャ リージョンがサポートされるようになりました

カタルーニャ リージョンは、Google Cloud のCloud Volumes ONTAPおよび Connector for Cloud Volumes ONTAP 9.12.1 GA 以降でサポートされるようになりました。

Azure でスウェーデン中部リージョンがサポートされるようになりました

Cloud Volumes ONTAPおよび Connector for Cloud Volumes ONTAP 9.12.1 GA 以降では、Azure でスウェーデン セントラル リージョンがサポートされるようになりました。

Azure オーストラリア東部における HA マルチアベイラビリティゾーン展開のサポート

Azure のオーストラリア東部リージョンでは、Cloud Volumes ONTAP 9.12.1 GA 以降の HA 複数可用性ゾーンの展開がサポートされるようになりました。

充電使用量の内訳

容量ベースのライセンスをサブスクライブすると、何に対して課金されるのかがわかるようになります。BlueXPのデジタル ウォレットからは、次の種類の使用状況レポートをダウンロードできます。使用状況レポートには、サブスクリプションの容量の詳細が提供され、Cloud Volumes ONTAPサブスクリプション内のリソースに対してどのように課金されるかが示されます。ダウンロード可能なレポートは他のユーザーと簡単に共有できます。

- Cloud Volumes ONTAPパッケージの使用
- 高レベルの使用法
- ストレージVMの使用状況
- ボリューム使用量

<https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-manage-capacity-licenses.html>["容量ベースのライセンスを管理する"]。

マーケットプレイスサブスクリプションなしでBlueXPにアクセスすると通知が表示されるようになりました

マーケットプレイス サブスクリプションなしでBlueXPのCloud Volumes ONTAP にアクセスするたびに通知が表示されるようになりました。通知には、「この作業環境のマーケットプレイス サブスクリプションは、Cloud Volumes ONTAP の利用規約に準拠している必要があります」と記載されています。

2023年4月4日

AWS の中国リージョンのサポート

Cloud Volumes ONTAP 9.12.1 GA 以降、AWS では次のように中国リージョンがサポートされるようになりました。

- 単一ノード システムがサポートされています。
- NetAppから直接購入したライセンスがサポートされます。

地域ごとの提供状況については、"[Cloud Volumes ONTAPのグローバル リージョン マップ](#)"。

2023年4月3日

コネクタの 3.9.28 リリースでは、次の変更が導入されました。

トリノ地域が **Google Cloud** でサポートされるようになりました

トリノ リージョンは、Google Cloud のCloud Volumes ONTAPおよび Connector for Cloud Volumes ONTAP 9.12.1 GA 以降でサポートされるようになりました。

BlueXP digital walletの強化

BlueXP digital walletには、マーケットプレイスのプライベート オファーで購入したライセンス容量が表示されるようになりました。

["アカウントで消費された容量を確認する方法を学びます"](#)。

ボリューム作成時のコメントのサポート

このリリースでは、API を使用してCloud Volumes ONTAP FlexGroupボリュームまたはFlexVol volumeを作成するときにコメントを追加できるようになりました。

Cloud Volumes ONTAPの概要、ボリューム、アグリゲート ページのBlueXPユーザー インターフェースの再設計

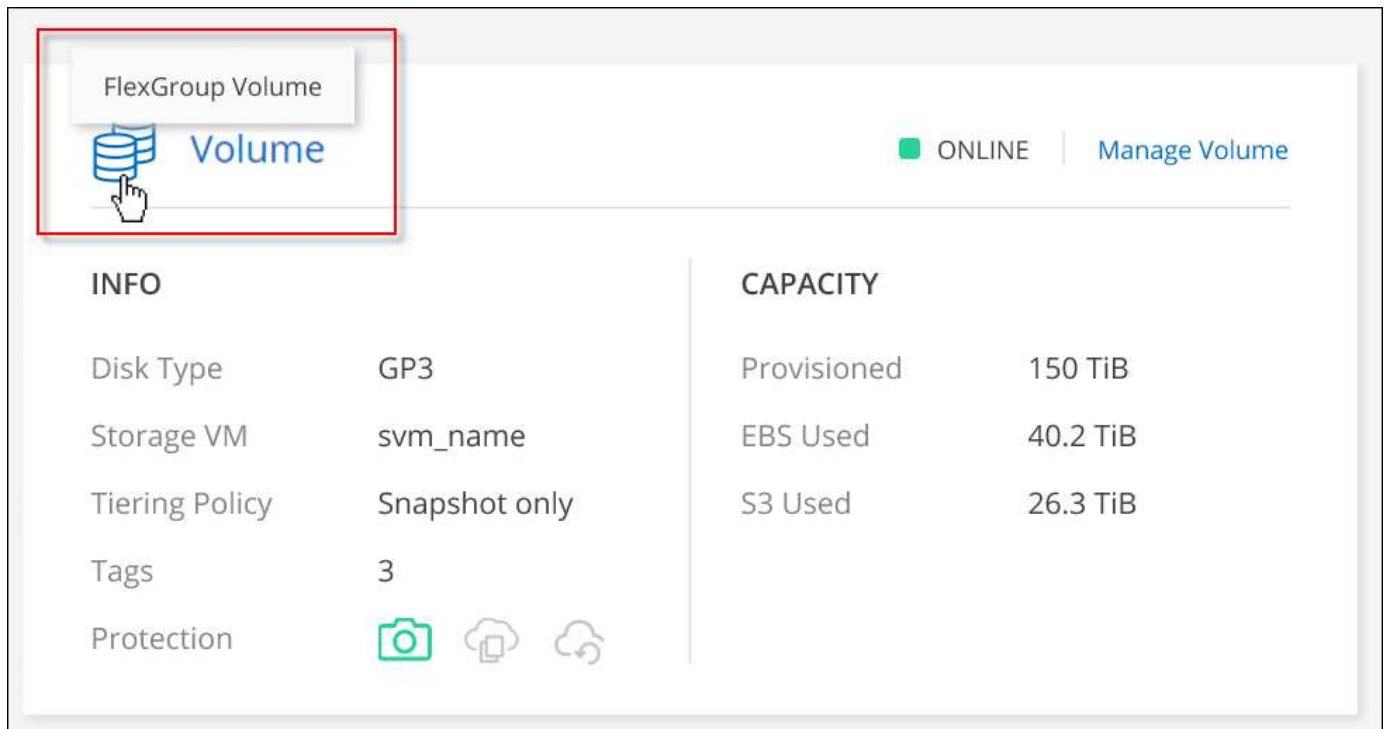
BlueXPでは、Cloud Volumes ONTAP の概要、ボリューム、およびアグリゲート ページのユーザー インターフェイスが再設計されました。タイルベースのデザインにより、各タイルにさらに包括的な情報が表示されるため、ユーザー エクスペリエンスが向上します。

Cloud Volumes ONTAPを通じて表示可能なFlexGroupボリューム

ONTAP System Manager またはONTAP CLI を通じて直接作成されたFlexGroupボリュームは、BlueXPの再設計されたボリューム タイルを通じて表示できるようになりました。FlexVolボリュームに提供される情報と同様に、BlueXP は専用のボリューム タイルを通じて、作成されたFlexGroupボリュームの詳細情報を提供します。



現在、BlueXPで既存のFlexGroupボリュームのみを表示できます。BlueXPでFlexGroupボリュームを作成する機能は現在利用できませんが、将来のリリースで提供される予定です。



"作成されたFlexGroupボリュームの表示の詳細について説明します。"

2023年3月13日

Azure の中国リージョンのサポート

Azure でのCloud Volumes ONTAP 9.12.1 GA および 9.13.0 GA の単一ノード展開で、China North 3 リージョンがサポートされるようになりました。これらのリージョンでは、NetAppから直接購入したライセンス (BYOL ライセンス) のみがサポートされます。



中国地域でのCloud Volumes ONTAPの新規導入は、9.12.1 GA および 9.13.0 GA でのみサポートされます。これらのバージョンを、Cloud Volumes ONTAPの新しいパッチおよびリリースにアップグレードできます。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。

地域ごとの提供状況については、"[Cloud Volumes ONTAPのグローバル リージョン マップ](#)"。

2023年3月5日

コネクタの 3.9.27 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.13.0

BlueXP は、AWS、Azure、Google Cloud でCloud Volumes ONTAP 9.13.0 を展開および管理できるようになりました。

"[Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう](#)"。

Azure での 16 TiB と 32 TiB のサポート

Cloud Volumes ONTAP は、Azure の管理ディスク上で実行される高可用性デプロイメント向けに、16 TiB および 32 TiB のディスク サイズをサポートするようになりました。

詳細はこちら ["Azureでサポートされているディスクサイズ"](#)。

MTEKM ライセンス

マルチテナント暗号化キー管理 (MTEKM) ライセンスは、バージョン 9.12.1 GA 以降を実行している新規および既存の Cloud Volumes ONTAP システムに含まれるようになりました。

マルチテナント外部キー管理により、NetApp Volume Encryption を使用するとき、個々のストレージ VM (SVM) が KMIP サーバーを通じて独自のキーを維持できるようになります。

["NetApp暗号化ソリューションを使用してボリュームを暗号化する方法を学びます"](#)。

インターネットのない環境のサポート

Cloud Volumes ONTAP は、インターネットから完全に分離されたあらゆるクラウド環境でサポートされるようになりました。これらの環境では、ノードベースのライセンス (BYOL) のみがサポートされます。容量ベースのライセンスはサポートされていません。開始するには、コネクタ ソフトウェアを手動でインストールし、コネクタ上で実行されている BlueXP コンソールにログインし、BYOL ライセンスを BlueXP digital wallet に追加して、Cloud Volumes ONTAP をデプロイします。

- ["インターネットにアクセスできない場所にコネクタをインストールする"](#)
- ["コネクタ上の BlueXP コンソールにアクセスする"](#)
- ["割り当てられていないライセンスを追加する"](#)

Google Cloud のフラッシュキャッシュと高速書き込み

Cloud Volumes ONTAP 9.13.0 リリースでは、一部のインスタンスにおいて、フラッシュ キャッシュ、高速書き込み、および 8,896 バイトの最大転送単位 (MTU) のサポートが利用できるようになりました。

詳細はこちら ["Google Cloud のライセンスでサポートされている構成"](#)。

2023年2月5日

コネクタの 3.9.26 リリースでは、次の変更が導入されました。

AWSでの配置グループの作成

AWS HA 単一アベイラビリティゾーン (AZ) デプロイメントでの配置グループ作成に新しい構成設定が利用できるようになりました。失敗した配置グループの作成をバイパスし、AWS HA 単一 AZ デプロイメントを正常に完了できるように選択できるようになりました。

配置グループの作成設定を構成する方法の詳細については、以下を参照してください。 ["AWS HA シングル AZ の配置グループ作成を構成する"](#)。

プライベート DNS ゾーン構成の更新

Azure Private Links を使用するとき、プライベート DNS ゾーンと仮想ネットワークの間にリンクが作成されないようにする新しい構成設定が利用できるようになりました。作成はデフォルトで有効になっています。

["BlueXPにAzureプライベートDNSの詳細を提供します"](#)

WORMストレージとデータ階層化

Cloud Volumes ONTAP 9.8 以降のシステムを作成するとき、データ階層化と WORM ストレージの両方を一緒に有効にできるようになりました。WORM ストレージによるデータ階層化を有効にすると、クラウド内のオブジェクトストアにデータを階層化できます。

["WORM ストレージについて学びます。"](#)

2023年1月1日

コネクタの 3.9.25 リリースでは、次の変更が導入されました。

Google Cloud で利用可能なライセンス パッケージ

最適化された Edge Cache 容量ベースのライセンス パッケージは、Google Cloud Marketplace のCloud Volumes ONTAPで従量課金制または年間契約としてご利用いただけます。

参照 ["Cloud Volumes ONTAPライセンス"](#)。

Cloud Volumes ONTAPのデフォルト設定

マルチテナント暗号化キー管理 (MTEKM) ライセンスは、新しいCloud Volumes ONTAPデプロイメントには含まれなくなりました。

Cloud Volumes ONTAPで自動的にインストールされるONTAP機能ライセンスの詳細については、以下を参照してください。 ["Cloud Volumes ONTAPのデフォルト設定"](#)。

2022年12月15日

Cloud Volumes ONTAP 9.12.0

BlueXP は、AWS および Google Cloud でCloud Volumes ONTAP 9.12.0 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2022年12月8日

Cloud Volumes ONTAP 9.12.1

BlueXPでは、新しい機能と追加のクラウド プロバイダー リージョンのサポートを含むCloud Volumes ONTAP 9.12.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)

2022年12月4日

コネクタの 3.9.24 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP の作成中に **WORM + Cloud Backup** が利用可能になりました

Cloud Volumes ONTAP の作成プロセス中に、Write Once Read Many (WORM) 機能と Cloud Backup 機能の両方をアクティブ化できるようになりました。

Google Cloud でイスラエル リージョンがサポートされるようになりました

Google Cloud のCloud Volumes ONTAPおよび Connector for Cloud Volumes ONTAP 9.11.1 P3 以降では、イスラエル リージョンがサポートされるようになりました。

2022年11月15日

コネクタの 3.9.23 リリースでは、次の変更が導入されました。

Google Cloud のONTAP S3 ライセンス

Google Cloud Platform でバージョン 9.12.1 以降を実行している新規および既存のCloud Volumes ONTAPシステムに、ONTAP S3 ライセンスが含まれるようになりました。

["ONTAPドキュメント: S3オブジェクトストレージサービスの設定と管理方法を学ぶ"](#)

2022年11月6日

コネクタの 3.9.23 リリースでは、次の変更が導入されました。

Azure でのリソース グループの移動

同じ Azure サブスクリプション内で、Azure のあるリソース グループから別のリソース グループに作業環境を移動できるようになりました。

<https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-moving-resource-groups-azure.html>["リソース グループの移動"]。

NDMPコピー認証

NDMP コピーが Cloud Volume ONTAPでの使用が認定されました。

NDMPの設定方法と使用方法については、["ONTAPドキュメント: NDMP設定の概要"](#)。

Azure のマネージド ディスク暗号化のサポート

新しい Azure アクセス許可が追加され、作成時にすべてのマネージド ディスクを暗号化できるようになりました。

この新機能の詳細については、以下を参照してください。 ["Azureで顧客管理キーを使用するようにCloud](#)

[Volumes ONTAPを設定する](#)。

2022年9月18日

コネクタの 3.9.22 リリースでは、次の変更が導入されました。

デジタルウォレットの機能強化

- デジタル ウォレットには、最適化された I/O ライセンス パッケージの概要と、アカウント全体のCloud Volumes ONTAPシステムにプロビジョニングされた WORM 容量が表示されるようになりました。

これらの詳細は、料金がどのように請求されるか、追加の容量を購入する必要があるかどうかをよりよく理解するのに役立ちます。

["アカウントで消費された容量を確認する方法を学びます"](#)。

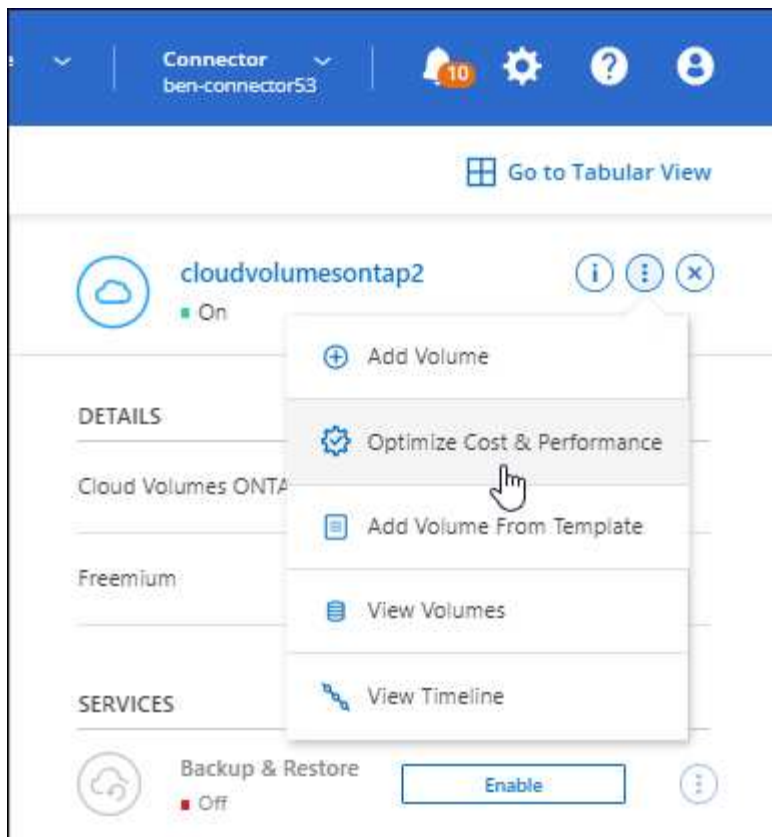
- 1 つの充電方法から最適化された充電方法に変更できるようになりました。

["充電方法の変更方法を学ぶ"](#)。

コストとパフォーマンスを最適化

Cloud Volumes ONTAPシステムのコストとパフォーマンスを Canvas から直接最適化できるようになりました。

作業環境を選択したら、*コストとパフォーマンスの最適化*オプションを選択して、Cloud Volumes ONTAP のインスタンスタイプを変更できます。より小さいサイズのインスタンスを選択するとコストを削減できますが、より大きなサイズのインスタンスに変更するとパフォーマンスを最適化できます。



AutoSupport通知

Cloud Volumes ONTAPシステムがAutoSupportメッセージを送信できない場合、BlueXP は通知を生成するようになりました。通知には、ネットワークの問題のトラブルシューティングに使用できる手順へのリンクが含まれています。

2022年7月31日

コネクタの 3.9.21 リリースでは、次の変更が導入されました。

MTEKMライセンス

マルチテナント暗号化キー管理 (MTEKM) ライセンスは、バージョン 9.11.1 以降を実行している新規および既存のCloud Volumes ONTAPシステムに含まれるようになりました。

マルチテナント外部キー管理により、NetApp Volume Encryption を使用するとき、個々のストレージ VM (SVM) が KMIP サーバーを通じて独自のキーを維持できるようになります。

["NetApp暗号化ソリューションを使用してボリュームを暗号化する方法を学びます"](#)。

プロキシ サーバ

BlueXP は、AutoSupportメッセージを送信するためのアウトバウンド インターネット接続が利用できない場合に、コネクタをプロキシ サーバーとして使用するようにCloud Volumes ONTAPシステムを自動的に構成するようになりました。

AutoSupport は、システムの健全性をプロアクティブに監視し、NetAppテクニカル サポートにメッセージを送信します。

唯一の要件は、コネクタのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コネクタをデプロイした後、このポートを開く必要があります。

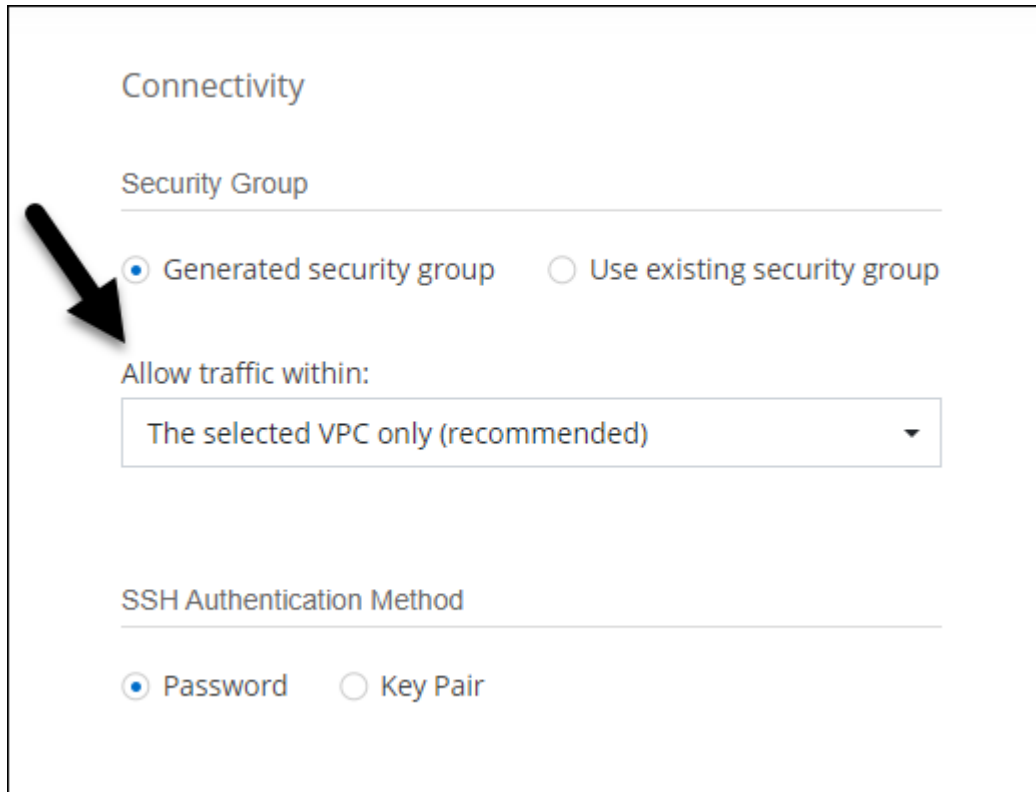
充電方法を変更する

容量ベースのライセンスを使用するCloud Volumes ONTAPシステムの課金方法を変更できるようになりました。たとえば、Essentials パッケージを使用してCloud Volumes ONTAPシステムを導入した場合、ビジネス ニーズの変化に応じて Professional パッケージに変更できます。この機能はデジタルウォレットから利用できます。

["充電方法の変更方法を学ぶ"](#)。

セキュリティグループの強化

Cloud Volumes ONTAP作業環境を作成するときに、ユーザー インターフェイスを使用して、事前定義されたセキュリティ グループで選択したネットワーク内のトラフィックのみを許可するか (推奨)、すべてのネットワーク内のトラフィックを許可するかを選択できるようになりました。



Connectivity

Security Group

☒ Generated security group ☐ Use existing security group

Allow traffic within:

The selected VPC only (recommended) ▼

SSH Authentication Method

☒ Password ☐ Key Pair

2022年7月18日

Azure の新しいライセンス パッケージ

Azure Marketplace サブスクリプションを通じて支払う場合、Azure のCloud Volumes ONTAPで次の 2 つの新しい容量ベースのライセンス パッケージを利用できます。

- 最適化: プロビジョニングされた容量と I/O 操作に対して個別に料金を支払います
- エッジキャッシュ: ライセンス ["クラウドボリュームエッジキャッシュ"](#)

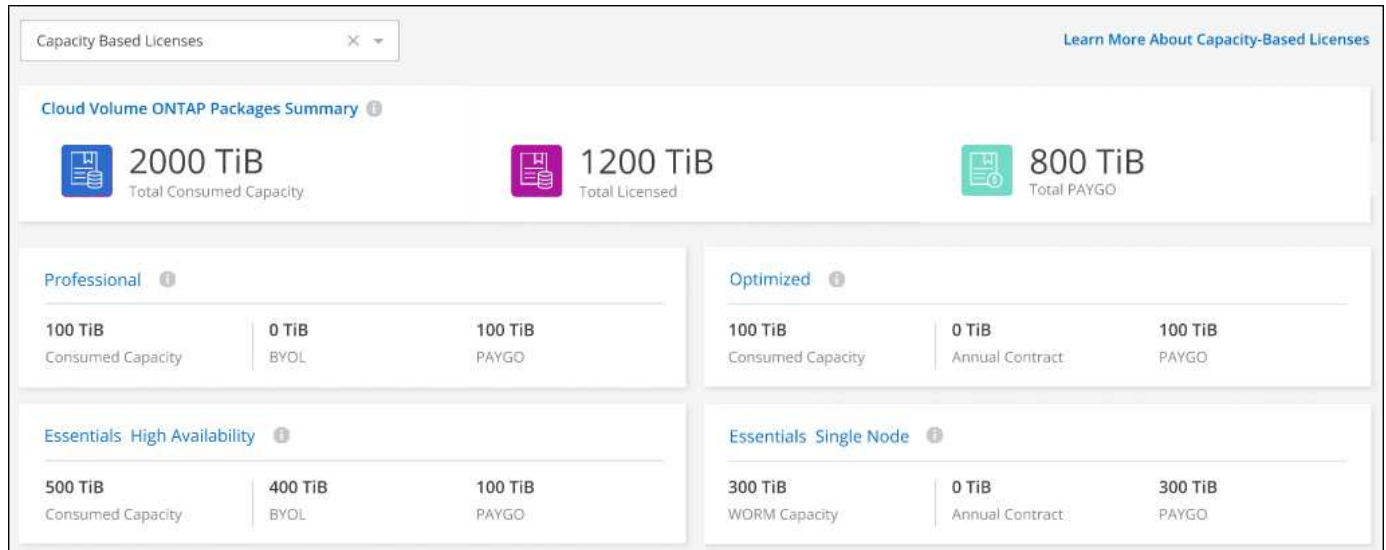
["これらのライセンスパッケージの詳細"](#)。

2022年7月3日

コネクタの 3.9.20 リリースでは、次の変更が導入されました。

デジタルウォレット

デジタル ウォレットには、アカウント内の消費済み容量の合計と、ライセンス パッケージ別の消費済み容量が表示されるようになりました。これにより、料金がどのように請求されるか、追加の容量を購入する必要があるかどうかを把握できます。



エラスティックボリュームの強化

BlueXP は、ユーザー インターフェイスからCloud Volumes ONTAP作業環境を作成するときに、Amazon EBS Elastic Volumes 機能をサポートするようになりました。gp3 または io1 ディスクを使用する場合、Elastic Volumes 機能はデフォルトで有効になります。ストレージのニーズに基づいて初期容量を選択し、Cloud Volumes ONTAP の導入後に修正することができます。

["AWS の Elastic Volumes のサポートについて詳しく見る"](#)。

AWS のONTAP S3 ライセンス

AWS でバージョン 9.11.0 以降を実行している新規および既存のCloud Volumes ONTAPシステムにONTAP S3 ライセンスが含まれるようになりました。

["ONTAPドキュメント: S3オブジェクトストレージサービスの設定と管理方法を学ぶ"](#)

新しい Azure クラウド リージョンのサポート

9.10.1 リリース以降、Cloud Volumes ONTAP はAzure West US 3 リージョンでサポートされるようになりました。

["Cloud Volumes ONTAPでサポートされているリージョンの完全なリストを表示します。"](#)

Azure のONTAP S3 ライセンス

Azure でバージョン 9.9.1 以降を実行している新規および既存のCloud Volumes ONTAPシステムにONTAP S3 ライセンスが含まれるようになりました。

["ONTAPドキュメント: S3オブジェクトストレージサービスの設定と管理方法を学ぶ"](#)

2022年6月7日

コネクタの 3.9.19 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.11.1

BlueXPでは、新しい機能と追加のクラウド プロバイダー リージョンのサポートを含むCloud Volumes ONTAP 9.11.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)

新しい詳細ビュー

Cloud Volumes ONTAPの高度な管理を実行する必要がある場合は、ONTAPシステムに付属の管理インターフェイスであるONTAP System Manager を使用して実行できます。高度な管理のためにBlueXPを離れる必要がないように、System Manager インターフェイスがBlueXP内に直接組み込まれています。

この詳細ビューは、Cloud Volumes ONTAP 9.10.0 以降でプレビューとして利用できます。今後のリリースでは、このエクスペリエンスを改良し、機能強化を追加する予定です。製品内チャットを使用してフィードバックをお送りください。

["詳細ビューの詳細"](#)。

Amazon EBS エラスティックボリュームのサポート

Cloud Volumes ONTAPアグリゲートによる Amazon EBS Elastic Volumes 機能のサポートにより、パフォーマンスが向上し、容量が追加されるとともに、BlueXP が必要に応じて基盤となるディスク容量を自動的に増やすことが可能になります。

Elastic Volumes のサポートは、新しいCloud Volumes ONTAP 9.11.0 システム以降、および gp3 および io1 EBS ディスク タイプで利用できます。

["エラスティックボリュームのサポートについて詳しくはこちら"](#)。

Elastic Volumes のサポートには、コネクタに対する新しい AWS 権限が必要であることに注意してください。

```
"ec2:DescribeVolumesModifications",  
"ec2:ModifyVolume",
```

BlueXPに追加した AWS 認証情報の各セットにこれらの権限を必ず付与してください。 ["AWSの最新のコネクタポリシーを見る"](#)。

共有AWSサブネットでのHAペアの導入をサポート

Cloud Volumes ONTAP 9.11.1 には、AWS VPC 共有のサポートが含まれています。このコネクタのリリースでは、API を使用するとき AWS 共有サブネットに HA ペアをデプロイできるようになりました。

["共有サブネットにHAペアを展開する方法を学ぶ"](#)。

サービスエンドポイント使用時のネットワークアクセスの制限

BlueXPでは、Cloud Volumes ONTAPとストレージ アカウント間の接続に VNet サービス エンドポイントを使用するときに、ネットワーク アクセスが制限されるようになりました。Azure Private Link 接続を無効にすると、BlueXP はサービス エンドポイントを使用します。

["Cloud Volumes ONTAPを使用した Azure Private Link 接続の詳細"](#)。

Google Cloud でのストレージ VM 作成のサポート

9.11.1 リリース以降、Google Cloud のCloud Volumes ONTAPで複数のストレージ VM がサポートされるようになりました。このコネクタのリリース以降、BlueXPAPI を使用して Google Cloud のCloud Volumes ONTAP HA ペア上にストレージ VM を作成できるようになりました。

ストレージ VM の作成をサポートするには、コネクタに対する新しい Google Cloud 権限が必要です。

```
- compute.instanceGroups.get  
- compute.addresses.get
```

単一ノード システムでストレージ VM を作成するには、ONTAP CLI または System Manager を使用する必要があることに注意してください。

- ["Google Cloud のストレージ VM 制限の詳細"](#)
- ["Google Cloud でCloud Volumes ONTAP用のデータ提供ストレージ VM を作成する方法を学びます"](#)

2022年5月2日

コネクタの 3.9.18 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.11.0

BlueXPでCloud Volumes ONTAP 9.11.0 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

メディアエーターのアップグレードの強化

BlueXP は、HA ペアのメディアエーターをアップグレードするときに、ブート ディスクを削除する前に、新しいメディアエーター イメージが利用可能であることを検証するようになりました。この変更により、アップグレード プロセスが失敗した場合でも、メディアエーターは引き続き正常に動作できるようになります。

K8s タブは削除されました

K8s タブは以前のリリースで非推奨となり、現在は削除されています。

Azureの年間契約

Essentials および Professional パッケージは、年間契約を通じて Azure で利用できるようになりました。年間契約を購入するには、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、作業環境の作成中に Azure Marketplace からサブスクライブするときに年間プランを選択できます。

["ライセンスについて詳しくはこちら"](#)。

S3 Glacier インスタント取得

Amazon S3 Glacier Instant Retrieval ストレージクラスに階層化されたデータを保存できるようになりました。

["階層化データのストレージクラスを変更する方法を学ぶ"](#)。

コネクタに必要な新しい AWS 権限

単一のアベイラビリティゾーン (AZ) に HA ペアを展開するときに AWS スプレッド配置グループを作成するには、次の権限が必要になりました。

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy",
```

BlueXP が配置グループを作成する方法を最適化するには、これらの権限が必要になりました。

BlueXPに追加した AWS 認証情報の各セットにこれらの権限を必ず付与してください。 ["AWSの最新のコネクタポリシーを見る"](#)。

新しい Google Cloud リージョンのサポート

Cloud Volumes ONTAP は、9.10.1 リリース以降、次の Google Cloud リージョンでサポートされるようになりました。

- デリー (アジア南2)
- メルボルン (オーストラリア南東部2)
- ミラノ (europe-west8) - 単一ノードのみ
- サンティアゴ (southamerica-west1) - 単一ノードのみ

["Cloud Volumes ONTAPでサポートされているリージョンの完全なリストを表示します。"](#)

Google Cloud での n2-standard-16 のサポート

9.10.1 リリース以降、n2-standard-16 マシンタイプが Google Cloud のCloud Volumes ONTAPでサポートされるようになりました。

["Google Cloud でサポートされているCloud Volumes ONTAPの構成を表示します"](#)

Google Cloud ファイアウォール ポリシーの機能強化

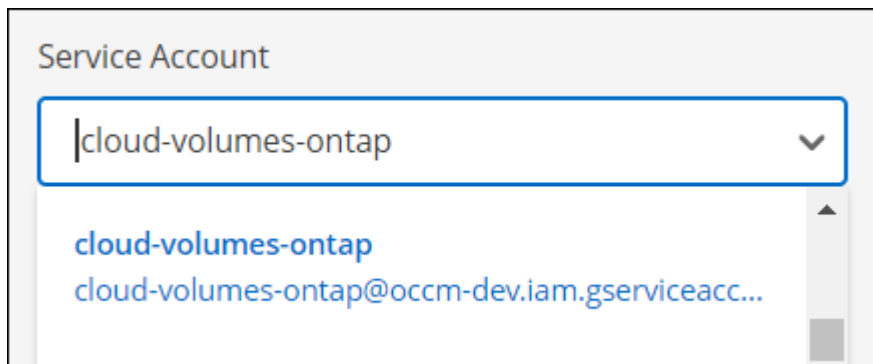
- Google Cloud でCloud Volumes ONTAP HA ペアを作成すると、BlueXP はVPC 内の既存のファイアウォール ポリシーをすべて表示するようになりました。

以前は、BlueXP はターゲット タグのない VPC-1、VPC-2、または VPC-3 のポリシーを表示しませんでした。

- Google Cloud でCloud Volumes ONTAPシングルノード システムを作成するときに、事前定義されたファイアウォール ポリシーで、選択した VPC 内のトラフィックのみを許可するか（推奨）、すべての VPC 内のトラフィックを許可するかを選択できるようになりました。

Google Cloud サービス アカウントの機能強化

Cloud Volumes ONTAPで使用する Google Cloud サービス アカウントを選択すると、BlueXPには各サービス アカウントに関連付けられているメール アドレスが表示されるようになりました。メールアドレスを表示すると、同じ名前を持つサービス アカウントを区別しやすくなります。



2022年4月3日

システムマネージャのリンクは削除されました

以前はCloud Volumes ONTAP作業環境内から利用できた System Manager リンクが削除されました。

Cloud Volumes ONTAPシステムに接続している Web ブラウザにクラスタ管理 IP アドレスを入力することで、System Manager に接続できます。 ["システムマネージャへの接続の詳細"](#)。

WORMストレージの課金

導入特別料金の有効期限が切れたため、WORM ストレージの使用に対して料金が発生するようになりました。課金は、WORM ボリュームのプロビジョニングされた合計容量に応じて時間単位で行われます。これは、新規および既存のCloud Volumes ONTAPシステムに適用されます。

["WORMストレージの価格について"](#)。

2022年2月27日

コネクタの 3.9.16 リリースでは、次の変更が導入されました。

ボリュームウィザードの再設計

最近導入された新しいボリュームの作成ウィザードは、*高度な割り当て*オプションから特定のアグリゲート上にボリュームを作成するときに使用できるようになりました。

["特定のアグリゲート上にボリュームを作成する方法を学ぶ"](#)。

2022年2月9日

マーケットプレイスのアップデート

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

これらの容量ベースの課金方法により、時間単位で支払いをしたり、クラウド プロバイダーから直接年間契約を購入したりすることができます。 NetAppから直接容量ライセンスを購入することもできます。

クラウド マーケットプレイスで既存のサブスクリプションがある場合は、これらの新しいサービスにも自動的にサブスクライブされます。新しいCloud Volumes ONTAP作業環境を展開するときに、容量による課金を選択できます。

新規顧客の場合、新しい作業環境を作成するときに、BlueXPサブスクリプションの申し込みを求められます。

- すべてのクラウド プロバイダー マーケットプレイスからのノード単位のライセンスは廃止され、新規加入者は利用できなくなりました。これには、年間契約と時間単位のサブスクリプション (Explore、Standard、Premium) が含まれます。

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

["Cloud Volumes ONTAPのライセンスオプションの詳細"](#)。

2022年2月6日

割り当てられていないライセンスを交換する

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

このアクションにより、Cloud Volumes ONTAPライセンスが取り消され、同じ有効期限を持つサービスに対してドル相当のライセンスが作成されます。

["割り当てられていないノードベースのライセンスを交換する方法を学ぶ"](#)。

2022年1月30日

コネクタの 3.9.15 リリースでは、次の変更が導入されました。

ライセンス選択の再設計

新しいCloud Volumes ONTAP作業環境を作成する際のライセンス選択画面を再設計しました。この変更は、2021 年 7 月に導入された容量ベースの課金方法に重点を置いたものであり、クラウド プロバイダー マーケットプレイスを通じて今後提供されるサービスをサポートします。

デジタルウォレットのアップデート

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

2022年1月2日

コネクタの 3.9.14 リリースでは、次の変更が導入されました。

追加の **Azure VM** タイプのサポート

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

- E4ds_v4
- E8ds_v4
- E32ds_v4
- E48ds_v4

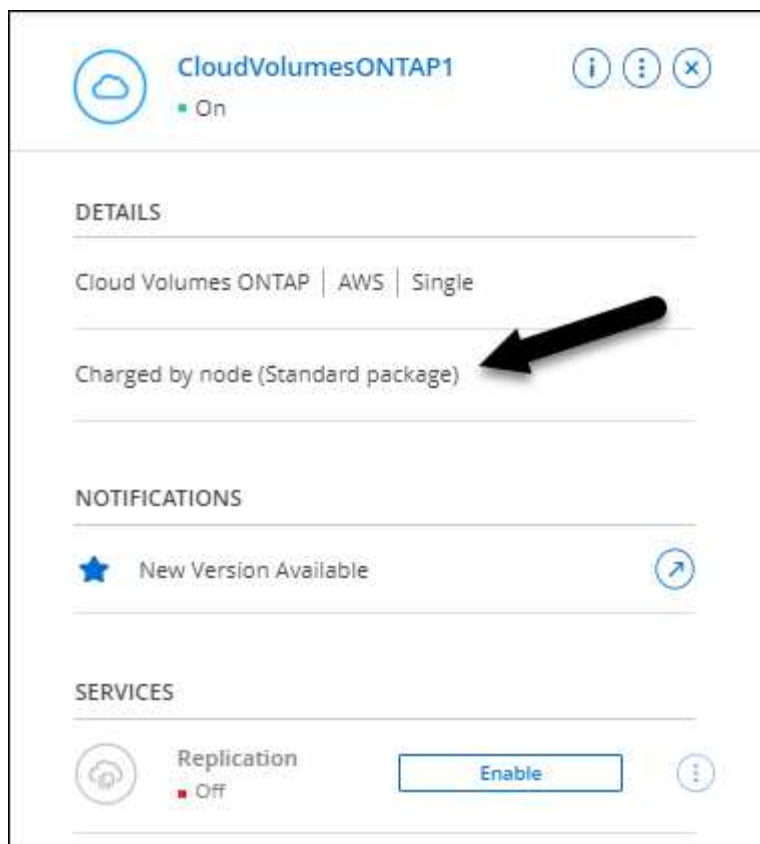
に行く ["Cloud Volumes ONTAPリリースノート"](#)サポートされている構成の詳細については、こちらをご覧ください。

FlexClone充電アップデート

使用する場合 ["容量ベースのライセンス"](#)Cloud Volumes ONTAPでは、FlexCloneボリュームで使用される容量に対して課金されなくなりました。

充電方法が表示されるようになりました

BlueXPでは、キャンバスの右側のパネルに、各Cloud Volumes ONTAP作業環境の課金方法が表示されるようになりました。



ユーザー名を決める

Cloud Volumes ONTAP作業環境を作成するときに、デフォルトの管理者ユーザー名の代わりに、希望するユーザー名を入力できるようになりました。

Credentials

User Name

Password

Confirm Password

ボリューム作成の機能強化

ボリューム作成にいくつかの機能強化を加えました。

- ボリューム作成ウィザードを使いやすく再設計しました。
- NFS のカスタム エクスポート ポリシーを選択できるようになりました。

✓ Details, Protection & Tags

2 Protocol

3 Disk Type

4 Usage Profile & Tiering Policy

5 Review

Volumes Protocol

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

Access Control

Custom export policy

Export Policy (1 rule defined)

Manage volume's export policy

2021年11月28日

コネクタの 3.9.13 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.10.1

BlueXP は、Cloud Volumes ONTAP 9.10.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

NetApp Keystoneサブスクリプション

Keystoneサブスクリプションを使用して、Cloud Volumes ONTAP HA ペアの支払いができるようになりました。

Keystoneサブスクリプションは、成長に合わせて支払うサブスクリプションベースのサービスであり、先行の CapEx やリースよりも OpEx 消費モデルを好むユーザーにシームレスなハイブリッド クラウド エクスペリエンスを提供します。

Keystoneサブスクリプションは、BlueXPから展開できるCloud Volumes ONTAPのすべての新しいバージョンでサポートされています。

- ["NetApp Keystoneサブスクリプションの詳細"](#)。
- ["BlueXPでKeystoneサブスクリプションを開始する方法を学びましょう"](#)。

新しい AWS リージョンのサポート

Cloud Volumes ONTAP がAWS アジアパシフィック (大阪) リージョン (ap-northeast-3) でサポートされるようになりました。

ポート削減

ポート 8023 と 49000 は、Azure のCloud Volumes ONTAPシステムでは、単一ノード システムと HA ペアの両方で開かなくなりました。

この変更は、コネクタの 3.9.13 リリース以降の新しいCloud Volumes ONTAPシステムに適用されます。

2021年10月4日

コネクタの 3.9.11 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.10.0

BlueXP は、Cloud Volumes ONTAP 9.10.0 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

展開時間の短縮

通常の書き込み速度が有効になっている場合、Microsoft Azure または Google Cloud にCloud Volumes ONTAP作業環境を展開するのにかかる時間を短縮しました。展開時間は平均で 3 ～ 4 分短縮されました。

2021年9月2日

コネクタの 3.9.10 リリースでは、次の変更が導入されました。

Azure の顧客管理暗号化キー

データはAzureのCloud Volumes ONTAPで自動的に暗号化されます。 ["Azure Storage Service Encryption"](#) Microsoft が管理するキーを使用します。ただし、次の手順を実行することで、代わりに独自の顧客管理暗号化キーを使用できるようになりました。

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. BlueXPから、API を使用して、キーを使用するCloud Volumes ONTAP作業環境を作成します。

["これらの手順について詳しくは"](#)。

2021年7月7日

コネクタの 3.9.8 リリースでは、次の変更が導入されました。

新しい充電方法

Cloud Volumes ONTAPでは新しい課金方法が利用可能になりました。

- 容量ベースの **BYOL**: 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。ライセンスはNetAppアカウントに関連付けられており、ライセンスで十分な容量が利用できる限り、複数のCloud Volumes ONTAPシステムを作成できます。容量ベースのライセンスは、*Essentials* または *Professional* のいずれかのパッケージ形式で利用できます。
- フリーミアム プラン: フリーミアム プランでは、NetAppのすべてのCloud Volumes ONTAP機能を無料で使用できます (クラウド プロバイダーの料金は引き続き適用されます)。プロビジョニングできる容量はシステムごとに 500 GiB に制限されており、サポート契約はありません。フリーミアム システムは最大 10 個まで使用できます。

["これらのライセンスオプションの詳細"](#)。

選択できる充電方法の例は次のとおりです。

Cloud Volumes ONTAP Charging Methods

[Learn more about our charging methods](#)

☐ Pay-As-You-Go by the hour

☒ Bring your own license

Bring your own license type

Capacity-Based

Package

Professional

☐ Freemium (Up to 500GB)

一般用途に利用可能な**WORM**ストレージ

一度書き込み、何度も読み取り可能な (WORM) ストレージはプレビューではなくなり、 Cloud Volumes ONTAPで一般使用できるようになりました。 ["WORMストレージについて詳しくはこちら"](#)。

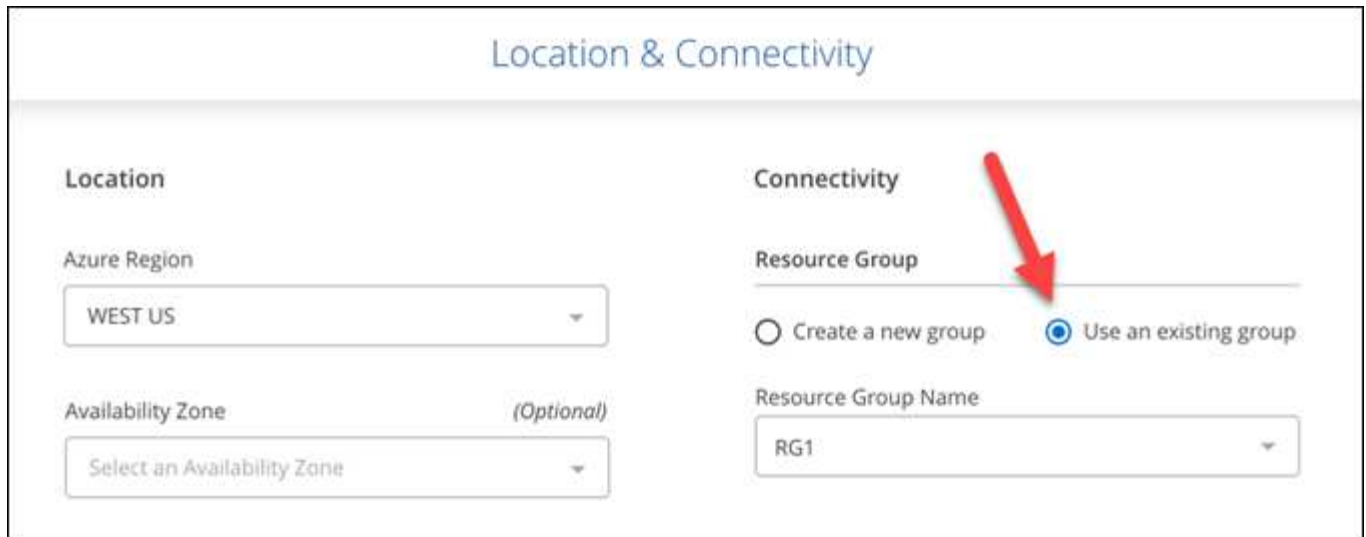
AWS での **m5dn.24xlarge** のサポート

9.9.1 リリース以降、 Cloud Volumes ONTAP は、PAYGO Premium、BYOL (お客様独自のライセンス使用)、Freemium の課金方法で m5dn.24xlarge インスタンス タイプをサポートするようになりました。

["AWS でCloud Volumes ONTAPがサポートする構成を表示する"](#)。

既存の**Azure**リソースグループを選択する

Azure でCloud Volumes ONTAPシステムを作成するときに、VM とその関連リソースの既存のリソース グループを選択できるようになりました。



Location & Connectivity

Location

Azure Region
WEST US

Availability Zone (Optional)
Select an Availability Zone

Connectivity

Resource Group

☐ Create a new group ☒ Use an existing group

Resource Group Name
RG1

次の権限により、BlueXP は、デプロイメントの失敗または削除の際に、リソース グループからCloud Volumes ONTAPリソースを削除できます。

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

BlueXPに追加した Azure 資格情報の各セットにこれらのアクセス許可を必ず付与してください。 ["Azureの最新のコネクタポリシーを表示する"](#)。

Azure で BLOB パブリック アクセスが無効になりました

セキュリティ強化のため、BlueXPでは、Cloud Volumes ONTAPのストレージ アカウントを作成するときに **Blob** パブリック アクセス が無効になるようになりました。

Azure プライベート リンクの機能強化

BlueXPでは、新しいCloud Volumes ONTAPシステムのブート診断ストレージ アカウントで Azure Private Link 接続がデフォルトで有効になるようになりました。

つまり、Cloud Volumes ONTAPのすべてのストレージ アカウントがプライベート リンクを使用ようになります。

["Cloud Volumes ONTAPで Azure Private Link を使用する方法の詳細"](#)。

Google Cloud のバランス永続ディスク

9.9.1 リリース以降、Cloud Volumes ONTAP はバランス永続ディスク (pd-balanced) をサポートするようになりました。

これらの SSD は、GiB あたりの IOPS を低くすることで、パフォーマンスとコストのバランスを実現します。

custom-4-16384 は **Google Cloud** でサポートされなくなりました

custom-4-16384 マシン タイプは、新しいCloud Volumes ONTAPシステムではサポートされなくなりました。

このマシン タイプで既存のシステムを実行している場合は、それを使い続けることもできますが、n2-standard-4 マシン タイプに切り替えることをお勧めします。

["GCP でCloud Volumes ONTAPがサポートする構成を表示する"](#)。

2021年5月30日

コネクタの 3.9.7 リリースでは、次の変更が導入されました。

AWS の新しいプロフェッショナル パッケージ

新しいプロフェッショナル パッケージでは、AWS Marketplace からの年間契約を使用して、Cloud Volumes ONTAPとCloud Backup Service をバンドルできます。支払いは TiB 単位となります。このサブスクリプションでは、オンプレミスのデータをバックアップすることはできません。

この支払いオプションを選択した場合、EBS ディスクと S3 オブジェクト ストレージ (単一ノードまたは HA) への階層化を通じて、Cloud Volumes ONTAPシステムごとに最大 2 PiB をプロビジョニングできます。

に行く ["AWSマーケットプレイスページ"](#)価格の詳細を表示するには ["Cloud Volumes ONTAPリリースノート"](#) このライセンス オプションの詳細については、こちらをご覧ください。

AWS の EBS ボリュームのタグ

BlueXP は、新しいCloud Volumes ONTAP作業環境を作成するときに、EBS ボリュームにタグを追加するようになりました。タグは、Cloud Volumes ONTAPがデプロイされた後に以前に作成されました。

この変更は、組織がサービス制御ポリシー (SCP) を使用してアクセス許可を管理している場合に役立ちます。

自動階層化ポリシーの最小冷却期間

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

["最小冷却期間を調整する方法を学びます。"](#)

カスタムエクスポートポリシーの強化

新しい NFS ボリュームを作成すると、BlueXP はカスタム エクスポート ポリシーを昇順で表示するようになり、必要なエクスポート ポリシーを見つけやすくなりました。

古いクラウドスナップショットの削除

BlueXP は、Cloud Volumes ONTAPシステムが展開されたとき、および電源がオフになるたびに作成されたルート ディスクとブート ディスクの古いクラウド スナップショットを削除するようになりました。ルート ボリュームとブート ボリュームの両方に対して、最新の 2 つのスナップショットのみが保持されます。

この機能強化により、不要になったスナップショットを削除することで、クラウド プロバイダーのコストが削減されます。

コネクタには、Azure スナップショットを削除する新しい権限が必要であることに注意してください。
["Azureの最新のコネクタポリシーを表示する"](#)。

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

2021年5月24日

Cloud Volumes ONTAP 9.9.1

BlueXPでCloud Volumes ONTAP 9.9.1 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"](#)。

2021年4月11日

コネクタの 3.9.5 リリースでは、次の変更が導入されました。

論理スペースのレポート

BlueXPでは、Cloud Volumes ONTAP用に作成される初期ストレージ VM の論理スペース レポートが有効になりました。

スペースが論理的に報告される場合、ONTAP は、ストレージ効率機能によって節約されたすべての物理スペースも使用済みとして報告されるようにボリューム スペースを報告します。

AWS での gp3 ディスクのサポート

Cloud Volumes ONTAP は、9.7 リリース以降、汎用 SSD (gp3) ディスクをサポートするようになりました。gp3 ディスクは、幅広いワークロードのコストとパフォーマンスのバランスが取れた最も低コストの SSD です。

["AWS でシステムのサイズを決定する"](#)。

AWS ではコールド HDD ディスクのサポートが終了しました

Cloud Volumes ONTAP は、Cold HDD (sc1) ディスクをサポートしなくなりました。

Azure ストレージ アカountの TLS 1.2

BlueXP がCloud Volumes ONTAP用に Azure にストレージ アカountを作成すると、ストレージ アカountの TLS バージョンはバージョン 1.2 になります。

2021年3月8日

コネクタの 3.9.4 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP 9.9.0

BlueXP は、Cloud Volumes ONTAP 9.9.0 を展開および管理できるようになりました。

["Cloud Volumes ONTAPのこのリリースに含まれる新機能について学びましょう"。](#)

AWS C2S環境のサポート

AWS Commercial Cloud Services (C2S) 環境にCloud Volumes ONTAP 9.8 を導入できるようになりました。

["AWS Secret Cloud または AWS Top Secret Cloud にCloud Volumes ONTAP を導入する"。](#)

カスタマー管理の CMK を使用した AWS 暗号化

BlueXP、AWS Key Management Service (KMS) を使用してCloud Volumes ONTAPデータを暗号化できるようになりました。Cloud Volumes ONTAP 9.9.0 以降では、顧客管理の CMK を選択した場合、EBS ディスク上のデータと S3 に階層化されたデータが暗号化されます。以前は、EBS データのみが暗号化されていました。

CMK を使用するには、Cloud Volumes ONTAP IAM ロールにアクセス権を付与する必要があることに注意してください。

["Cloud Volumes ONTAPを使用した AWS KMS の設定について詳しくは、こちらをご覧ください。"。](#)

Azure DoD のサポート

Azure 国防総省 (DoD) 影響レベル 6 (IL6) でCloud Volumes ONTAP 9.8 をデプロイできるようになりました。

Google Cloud における IP アドレスの削減

Google Cloud のCloud Volumes ONTAP 9.8 以降に必要な IP アドレスの数を削減しました。デフォルトでは、必要な IP アドレスが 1 つ少なくなります (クラスター間 LIF をノード管理 LIF と統合しました)。また、API を使用するときには SVM 管理 LIF の作成をスキップするオプションもあり、これにより追加の IP アドレスの必要性が軽減されます。

["Google Cloud の IP アドレス要件の詳細"。](#)

Google Cloud の共有 VPC サポート

Google Cloud でCloud Volumes ONTAP HA ペアをデプロイするときに、VPC-1、VPC-2、VPC-3 に共有 VPC を選択できるようになりました。以前は、共有 VPC として使用できるのは VPC-0 のみでした。この変更は、Cloud Volumes ONTAP 9.8 以降でサポートされています。

["Google Cloud のネットワーク要件の詳細"。](#)

2021年1月4日

コネクタの 3.9.2 リリースでは、次の変更が導入されました。

AWS アウトポスト

数か月前、Cloud Volumes ONTAP がAmazon Web Services (AWS) Outposts Ready 認定を取得したことを発表しました。本日、AWS Outposts でBlueXPとCloud Volumes ONTAP が検証されたことをお知らせいたしま

す。

AWS Outpost がある場合は、作業環境ウィザードで Outpost VPC を選択して、その Outpost に Cloud Volumes ONTAP をデプロイできます。エクスペリエンスは、AWS にある他の VPC と同じです。最初に AWS Outpost にコネクタをデプロイする必要があることに注意してください。

指摘すべき制限がいくつかあります。

- 現時点では、単一ノードの Cloud Volumes ONTAP システムのみがサポートされています。
- Cloud Volumes ONTAP で使用できる EC2 インスタンスは、Outpost で利用可能なものに限定されます。
- 現時点では汎用 SSD (gp2) のみがサポートされています

サポートされている Azure リージョンの Ultra SSD VNV RAM

Cloud Volumes ONTAP、E32s_v3 VM タイプを単一ノード システムで使用する場合、Ultra SSD を VNV RAM として使用できるようになりました。"[サポートされている Azure リージョン](#)"。

VNV RAM は書き込みパフォーマンスが向上します。

Azure でアベイラビリティゾーンを選択する

単一ノードの Cloud Volumes ONTAP システムをデプロイするアベイラビリティゾーンを選択できるようになりました。AZ を選択しない場合は、BlueXP が自動的に選択します。

Location

Azure Region

West US

Availability Zone (Optional)

Select an Availability Zone

None

1

2

3

Subnet

Select a subnet

Google Cloud の大容量ディスク

Cloud Volumes ONTAP は、GCP で 64 TB のディスクをサポートするようになりました。



GCP の制限により、ディスクのみの最大システム容量は 256 TB のままです。

Google Cloud の新しいマシンタイプ

Cloud Volumes ONTAP は、次のマシン タイプをサポートするようになりました。

- ExploreライセンスとBYOLを備えたn2-standard-4
- 標準ライセンスとBYOLを備えたn2-standard-8
- プレミアムライセンスとBYOLを備えたn2-standard-32

2020年11月3日

コネクタの 3.9.0 リリースでは、次の変更が導入されました。

Cloud Volumes ONTAP向け Azure Private Link

BlueXPでは、デフォルトで、Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間の Azure Private Link 接続が有効になります。プライベート リンクは、Azure 内のエンドポイント間の接続を保護します。

- ["Azure プライベートリンクの詳細"](#)
- ["Cloud Volumes ONTAPで Azure Private Link を使用する方法の詳細"](#)

既知の制限事項

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しないプラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

これらの制限は、NetAppコンソールのCloud Volumes ONTAP管理に固有のものです。Cloud Volumes ONTAPソフトウェア自体の制限事項を確認するには、["Cloud Volumes ONTAPリリースノートをご覧ください"](#)。

コンソールはFlexGroupボリュームの作成をサポートしていません

Cloud Volumes ONTAP はFlexGroupボリュームをサポートしていますが、コンソールは現在FlexGroupボリュームの作成をサポートしていません。ONTAP System ManagerまたはONTAP CLIからFlexGroupボリュームを作成する場合は、コンソールの容量管理モードを次のように設定する必要があります。Manual。`Automatic`モードはFlexGroupボリュームでは正しく動作しない可能性があります。



コンソールでFlexGroupボリュームを作成する機能は、将来のリリースで計画されています。

コンソールはCloud Volumes ONTAPを使用したS3をサポートしていません

Cloud Volumes ONTAP はスケールアウト ストレージのオプションとして S3 をサポートしていますが、コンソールではこの機能の管理機能は提供されていません。Cloud Volumes ONTAPから S3 クライアント アクセスを構成するには、CLI を使用するのがベスト プラクティスです。詳細については、["S3構成パワー ガイド"](#)。

["S3およびその他のクライアントプロトコルに対するCloud Volumes ONTAPのサポートの詳細"](#)。

コンソールはストレージ**VM**の災害復旧をサポートしていません

コンソールは、ストレージ VM (SVM) の災害復旧のためのセットアップやオーケストレーションのサポートを提供しません。ONTAP System Manager またはONTAP CLI を使用する必要があります。

["SVM災害復旧の詳細"](#)。

Cloud Volumes ONTAPリリースノート

Cloud Volumes ONTAPのリリース ノートには、リリース固有の情報が記載されています。リリースの新機能、サポートされている構成、ストレージの制限、製品の機能に影響を与える可能性のある既知の制限や問題。

["Cloud Volumes ONTAPのリリースノートをご覧ください"](#)

始めましょう

Cloud Volumes ONTAPについて学ぶ

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

Cloud Volumes ONTAPは、クラウドでONTAPデータ管理ソフトウェアを実行するソフトウェアのみのストレージ アプライアンスです。次の主要機能を備えたエンタープライズ グレードのストレージを提供します。

- ストレージ効率

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

- 高可用性

クラウド環境で障害が発生した場合でも、企業の信頼性と継続的な運用を確保します。

- データ保護

Cloud Volumes ONTAP は、業界をリードする NetApp のレプリケーション テクノロジーであるSnapMirrorを活用してオンプレミスのデータをクラウドに複製するため、複数のユース ケースで使用できるセカンダリ コピーを簡単に作成できます。

Cloud Volumes ONTAP はNetApp Backup and Recovery と統合されており、クラウド データの保護と長期アーカイブのためのバックアップおよび復元機能も提供します。

["バックアップとリカバリの詳細"](#)

- データ階層化

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

- アプリケーションの一貫性

NetApp SnapCenterを使用して、 NetApp Snapshot コピーの一貫性を確保します。

["SnapCenterについて詳しくはこちら"](#)

- Data security

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

- プライバシーコンプライアンス管理

NetApp Data Classification との統合により、データのコンテキストを理解し、機密データを識別できるようになります。



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

["サポートされているCloud Volumes ONTAP構成を表示する"](#)

["Cloud Volumes ONTAPの詳細"](#)

Cloud Volumes ONTAPデプロイメントでサポートされているONTAPバージョン

NetAppコンソールを使用すると、Cloud Volumes ONTAPシステムを追加するときに、複数の異なるONTAPバージョンから選択できます。

ここに記載されている以外のCloud Volumes ONTAPバージョンは、新しいデプロイメントには使用できません。アップグレードの詳細については、["サポートされているアップグレード パス"](#)。

AWS

シングル ノード

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

HAペア

- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5
- 9.5 P6

Azure

シングル ノード

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6
- 9.5 P6

HAペア

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1

- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.11.1 P3
- 9.10.1 P3
- 9.9.1 P8
- 9.9.1 P7
- 9.8 P10
- 9.7 P6

Google Cloud

シングル ノード

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA
- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8
- 9.7 P5

HAペア

- 9.17.1 RC1
- 9.16.1 GA
- 9.15.1 GA
- 9.15.0 P1
- 9.14.1 GA
- 9.14.1 RC1
- 9.14.0 GA

- 9.13.1 GA
- 9.12.1 GA
- 9.12.1 RC1
- 9.12.0 P1
- 9.11.1 P3
- 9.10.1
- 9.9.1 P6
- 9.8

Amazon Web Servicesを始める

AWS でのCloud Volumes ONTAPのクイックスタート

数ステップで AWS のCloud Volumes ONTAP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。 ["AWS でコンソールエージェントを作成する方法を学ぶ"](#)。

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コンソール ユーザー インターフェイス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。 ["詳細情報"](#)。

3

ネットワークを設定する

1. VPC 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してい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。

3. S3 サービスへの VPC エンドポイントを設定します。

Cloud Volumes ONTAPから低コストのオブジェクト ストレージにコールド データを階層化する場合、VPC エンドポイントが必要です。

["ネットワーク要件の詳細"](#)。

4

AWS KMSを設定する

Cloud Volumes ONTAPで Amazon 暗号化を使用する場合は、アクティブなカスタマーマスターキー (CMK) が存在することを確認する必要があります。また、コンソールエージェントに権限を提供する IAM ロールをキーユーザーとして追加して、各 CMK のキーポリシーを変更する必要があります。["詳細情報"](#)。

5

コンソールを使用して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

- ["AWS のコンソールエージェントを作成する"](#)
- ["AWS Marketplaceからコンソールエージェントを作成する"](#)
- ["オンプレミスでコンソールエージェントをインストールしてセットアップする"](#)
- ["コンソールエージェントのAWS権限"](#)

AWS でCloud Volumes ONTAP構成を計画する

AWS にCloud Volumes ONTAP を導入する場合、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 AWS 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"](#)。

新しい AWS リージョンでリソースを作成および管理するには、その前に新しい AWS リージョンを有効にする必要があります。["AWSドキュメント: リージョンを有効にする方法を学ぶ"](#)。

サポートされているローカルゾーンを選択してください

ローカルゾーンの選択はオプションです。Cloud Volumes ONTAPは、シンガポールを含む一部の AWS ローカルゾーンでサポートされています。AWS のCloud Volumes ONTAPは、単一のアベイラビリティゾーンで高可用性 (HA) モードのみをサポートします。単一ノードの展開はサポートされていません。



Cloud Volumes ONTAP は、AWS ローカルゾーンでのデータ階層化とクラウド階層化をサポートしていません。さらに、Cloud Volumes ONTAPに適合していないインスタンスを含むローカルゾーンはサポートされません。一例としてマイアミが挙げられますが、これはサポートされておらず、資格のない Gen6 インスタンスしかないため、ローカルゾーンとして使用できません。

["AWSドキュメント: ローカルゾーンの完全なリストを見る"](#)。ローカルゾーンでリソースを作成および管理するには、ローカルゾーンを有効にする必要があります。

["AWS ドキュメント: AWS Local Zones の使用開始"](#)。

サポートされているインスタンス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、いくつかのインスタンス タイプをサポートします。

["AWS でサポートされている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。

["AWS のCloud Volumes ONTAPのストレージ制限"](#)

AWS 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。インスタンスタイプ、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。

インスタンスタイプ

- ワークロード要件を、各 EC2 インスタンスタイプの最大スループットと IOPS に合わせて調整します。
- 複数のユーザーが同時にシステムに書き込む場合は、リクエストを管理するのに十分な CPU を備えたインスタンス タイプを選択します。
- 主に読み取りを行うアプリケーションがある場合は、十分な RAM を搭載したシステムを選択してください。
 - ["AWS ドキュメント: Amazon EC2 インスタンスタイプ"](#)
 - ["AWS ドキュメント: Amazon EBS 最適化インスタンス"](#)

EBSのディスク タイプ

大まかに言えば、EBS ディスク タイプ間の違いは次のとおりです。EBSディスクのユースケースの詳細については、以下を参照してください。 ["AWS ドキュメント: EBS ボリュームタイプ"](#)。

- 汎用 SSD (gp3) ディスクは、幅広いワークロードのコストとパフォーマンスのバランスが取れた最も低コストの SSD です。パフォーマンスは IOPS とスループットの観点から定義されます。gp3 ディスクは、Cloud Volumes ONTAP 9.7 以降でサポートされています。

gp3 ディスクを選択すると、NetAppコンソールは、選択したディスク サイズに基づいて、gp2 ディスクと同等のパフォーマンスを提供するデフォルトの IOPS とスループットの値を入力します。値を大きくするとコストは高くなりますが、パフォーマンスが向上する可能性があります。ただし、値を小さくするとパフォーマンスが低下する可能性があるため、値はサポートされていません。つまり、デフォルト値をそのまま使用するか、値を増やします。下げないでください。"[AWSドキュメント: gp3 ディスクとそのパフォーマンスについて詳しく知る](#)"。

Cloud Volumes ONTAP は、gp3 ディスクを使用した Amazon EBS Elastic Volumes 機能をサポートしていることに注意してください。"[Elastic Volumesのサポートについて詳しくはこちら](#)"。

- 汎用 SSD (gp2) ディスクは、幅広いワークロードのコストとパフォーマンスのバランスを実現します。パフォーマンスは IOPS で定義されます。
- *Provisioned IOPS SSD (io1)* ディスクは、より高いコストで最高のパフォーマンスを必要とする重要なアプリケーション向けです。

Cloud Volumes ONTAP は、io1 ディスクを使用した Amazon EBS Elastic Volumes 機能をサポートしていることに注意してください。"[Elastic Volumesのサポートについて詳しくはこちら](#)"。

- スループット最適化 HDD (st1) ディスクは、低価格で高速かつ一貫したスループットを必要とする、頻繁にアクセスされるワークロード向けです。



接続性がないため、AWS ローカルゾーンでは AWS S3 へのデータ階層化は利用できません。

EBSディスクサイズ

サポートされていない設定を選択した場合は、"[Amazon EBS エラスティックボリューム機能](#)"、Cloud Volumes ONTAPシステムを起動するときに初期ディスク サイズを選択する必要があります。その後は"[コンソールでシステムの容量を管理します](#)"ですが、もしあなたが"[自分で集計を作成する](#)"以下の点に注意してください。

- 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。
- EBS ディスクのパフォーマンスはディスク サイズに左右されます。サイズによって、SSD ディスクのベースライン IOPS と最大バースト期間、および HDD ディスクのベースラインとバースト スループットが決まります。
- 最終的には、必要な持続的なパフォーマンスを実現するディスク サイズを選択する必要があります。
- より大きなディスク (たとえば、4 TiB ディスク 6 台) を選択した場合でも、EC2 インスタンスが帯域幅制限に達する可能性があるため、すべての IOPS を取得できない可能性があります。

EBSディスクパフォーマンスの詳細については、"[AWS ドキュメント: EBS ボリュームタイプ](#)"。

前述のとおり、Amazon EBS Elastic Volumes 機能をサポートするCloud Volumes ONTAP構成では、ディスク サイズの選択はサポートされていません。"[Elastic Volumesのサポートについて詳しくはこちら](#)"。

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。

"AWS 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](#)"。

AWS Outpost にCloud Volumes ONTAPを導入する準備

AWS Outpost がある場合は、デプロイプロセス中に Outpost VPC を選択することで、その Outpost にCloud Volumes ONTAP をデプロイできます。エクスペリエンスは、AWS にある他の VPC と同じです。最初に AWS Outpost にコンソールエージェントをデプロイする必要があることに注意してください。

指摘すべき制限がいくつかあります。

- 現時点では、単一ノードのCloud Volumes ONTAPシステムのみがサポートされています。
- Cloud Volumes ONTAPで利用できるEC2インスタンスは、Outpostで利用可能なものに限定されます。
- 現時点では汎用SSD (gp2) のみがサポートされています

ネットワーク情報を収集する

AWS でCloud Volumes ONTAP を起動するときは、VPC 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。

単一 **AZ** 内の単一ノードまたは **HA** ペア

AWSの情報	あなたの価値
リージョン	
VPC	
サブネット	
セキュリティ グループ (独自のものを使用する場合)	

複数の**AZ**における**HA**ペア

AWSの情報	あなたの価値
リージョン	
VPC	
セキュリティ グループ (独自のものを使用する場合)	
ノード1のアベイラビリティゾーン	
ノード1サブネット	
ノード2のアベイラビリティゾーン	
ノード2サブネット	

AWSの情報	あなたの価値
メディアーターの可用性ゾーン	
メディアーターサブネット	
仲介者の鍵ペア	
クラスタ管理ポートのフローティングIPアドレス	
ノード1のデータ用のフローティングIPアドレス	
ノード2のデータ用のフローティングIPアドレス	
フローティングIPアドレスのルートテーブル	

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。

ネットワークを設定する

Cloud Volumes ONTAP用の AWS ネットワークを設定する

NetAppコンソールは、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。

一般要件

AWS で次の要件を満たしていることを確認してください。

Cloud Volumes ONTAPノードのアウトバウンド 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。セキュリティ要件が厳しい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接続します。使用される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	エンドポイントが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://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。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
AWSサービスの正確な商用エンドポイント（末尾に <code>amazonaws.com</code> ）は、使用している AWS リージョンによって異なります。参照 "詳細についてはAWSドキュメントをご覧ください" 。	• クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理 (IAM) • キー管理服务 (KMS) • セキュリティトークンサービス (STS) • シンプルストレージサービス (S3)	AWS サービスとの通信。	標準モードとプライベートモード。	Cloud Volumes ONTAP はAWS サービスと通信して AWS で特定の操作を実行することができません。
AWS サービスの正確な政府エンドポイントは、使用している AWS リージョンによって異なります。エンドポイントには、 <code>amazonaws.com</code> 、そして <code>c2s.ic.gov</code> 。参照 "AWS SDK" そして "AWS ドキュメント" 詳細についてはこちらをご覧ください。	• クラウドフォーメーション • エラスティックコンピューティングクラウド (EC2) • アイデンティティとアクセス管理 (IAM) • キー管理服务 (KMS) • セキュリティトークンサービス (STS) • シンプルストレージサービス (S3)	AWS サービスとの通信。	制限モード。	Cloud Volumes ONTAP はAWS サービスと通信して AWS で特定の操作を実行することができません。

HAメディアエーターのアウトバウンドインターネットアクセス

HA メディアエーターインスタンスには、ストレージフェイルオーバーを支援できるように、AWS EC2 サービスへの送信接続が必要です。接続を提供するには、パブリック IP アドレスを追加したり、プロキシ サーバーを指定したり、手動オプションを使用したりできます。

手動オプションとしては、ターゲットサブネットから AWS EC2 サービスへの NAT ゲートウェイまたはイン

ターフェース VPC エンドポイントが考えられます。VPCエンドポイントの詳細については、"[AWS ドキュメント: インターフェイス VPC エンドポイント \(AWS PrivateLink\)](#)"。

NetAppコンソールエージェントのネットワークプロキシ構成

NetAppコンソール 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](#)"。

プライベートIPアドレス

コンソールは、必要な数のプライベート IP アドレスをCloud Volumes ONTAPに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。

コンソールがCloud Volumes ONTAPに割り当てる LIF の数は、単一ノード システムを展開するか、HA ペアを展開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。

単一ノードシステムのIPアドレス

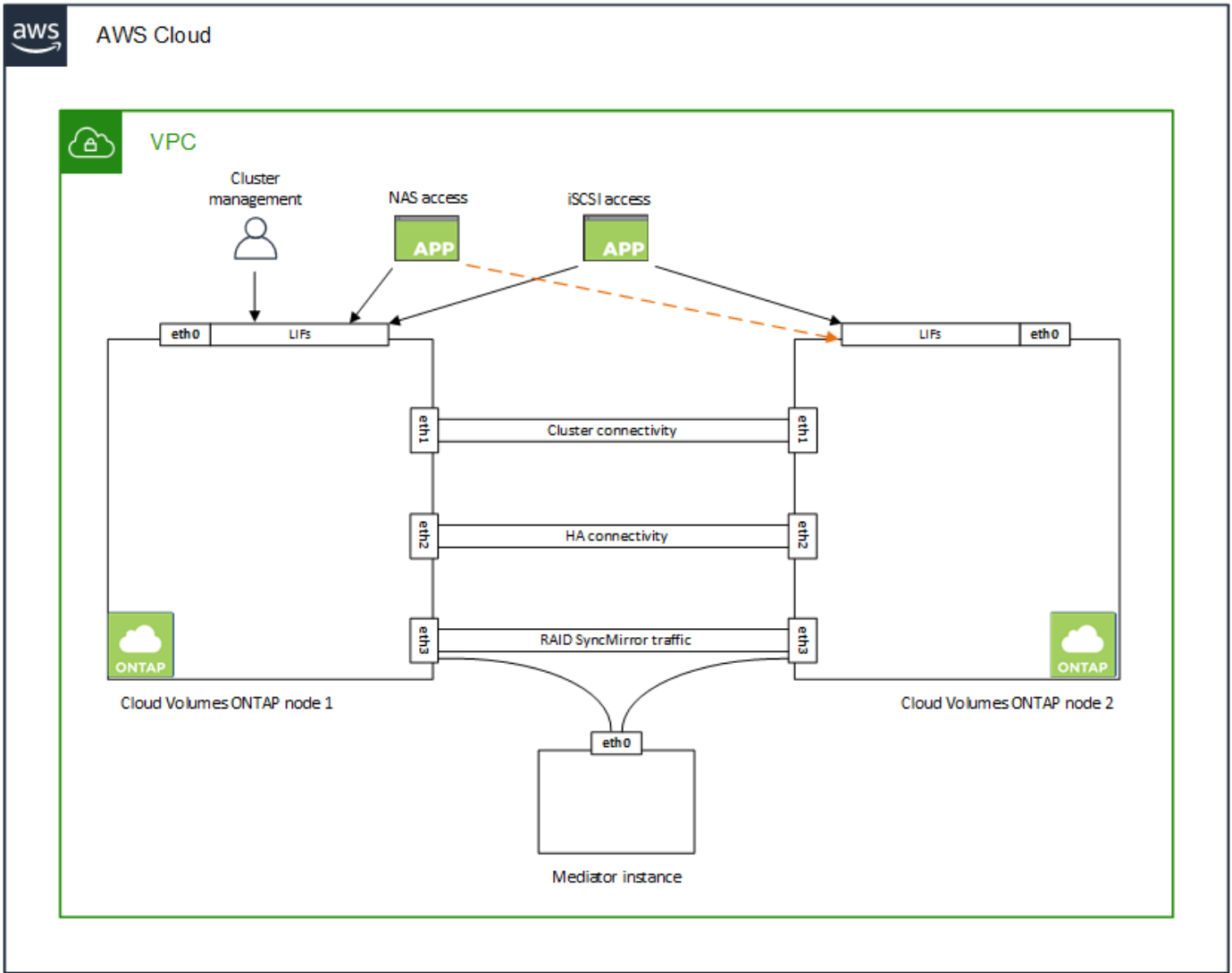
コンソールは、単一ノード システムに 6 つの IP アドレスを割り当てます。

次の表は、各プライベート IP アドレスに関連付けられている LIF の詳細を示しています。

LIF	目的
クラスタ管理	クラスタ全体 (HA ペア) の管理。
ノード管理	ノードの管理。
インタークラスター	クラスター間の通信、バックアップ、およびレプリケーション。
NASデータ	NAS プロトコル経由のクライアント アクセス。
iSCSIデータ	iSCSI プロトコル経由のクライアント アクセス。他の重要なネットワーク ワークフローでもシステムによって使用されます。この LIF は必須であり、削除しないでください。
ストレージVM管理	ストレージ VM 管理 LIF は、SnapCenterなどの管理ツールで使用されます。

HAペアのIPアドレス

HA ペアでは、単一ノード システムよりも多くの IP アドレスが必要です。次の図に示すように、これらの IP アドレスは、異なるイーサネット インターフェイスに分散されています。



HA ペアに必要なプライベート IP アドレスの数は、選択する展開モデルによって異なります。単一の AWS アベイラビリティゾーン (AZ) に展開された HA ペアには 15 個のプライベート IP アドレスが必要ですが、複数の AZ に展開された HA ペアには 13 個のプライベート IP アドレスが必要です。

次の表は、各プライベート IP アドレスに関連付けられている LIF の詳細を示しています。

LIF	インターフェイス	ノード	目的
クラスタ管理	eth0	ノード1	クラスタ全体（HA ペア）の管理。
ノード管理	eth0	ノード1とノード2	ノードの管理。
インタークラスター	eth0	ノード1とノード2	クラスター間の通信、バックアップ、およびレプリケーション。
NASデータ	eth0	ノード1	NAS プロトコル経由のクライアント アクセス。

LIF	インターフェイス	ノード	目的
iSCSIデータ	eth0	ノード1とノード2	iSCSI プロトコル経由のクライアント アクセス。他の重要なネットワーク ワークフローでもシステムによって使用されます。これらの LIF は必須であり、削除しないでください。
クラスター接続	eth1	ノード1とノード2	ノードが相互に通信し、クラスター内でデータを移動できるようにします。
HA接続	eth2	ノード1とノード2	フェイルオーバーの場合の 2 つのノード間の通信。
RSM iSCSIトラフィック	eth3	ノード1とノード2	RAID SyncMirror iSCSI トラフィック、および 2 つのCloud Volumes ONTAPノードとメディアーター間の通信。
メディアーター	eth0	メディアーター	ストレージの引き継ぎとギブバックのプロセスを支援するための、ノードとメディアーター間の通信チャネル。

LIF	インターフェイス	ノード	目的
ノード管理	eth0	ノード1とノード2	ノードの管理。
インタークラスター	eth0	ノード1とノード2	クラスター間の通信、バックアップ、およびレプリケーション。
iSCSIデータ	eth0	ノード1とノード2	iSCSI プロトコル経由のクライアント アクセス。これらの LIF は、ノード間のフローティング IP アドレスの移行も管理します。これらの LIF は必須であり、削除しないでください。
クラスター接続	eth1	ノード1とノード2	ノードが相互に通信し、クラスター内でデータを移動できるようにします。
HA接続	eth2	ノード1とノード2	フェイルオーバーの場合の 2 つのノード間の通信。
RSM iSCSIトラフィック	eth3	ノード1とノード2	RAID SyncMirror iSCSI トラフィック、および 2 つのCloud Volumes ONTAPノードとメディアーター間の通信。
メディアーター	eth0	メディアーター	ストレージの引き継ぎとギブバックのプロセスを支援するための、ノードとメディアーター間の通信チャネル。



複数のアベイラビリティゾーンに展開する場合、複数のLIFが関連付けられます。**"フローティングIPアドレス"**これらはAWS プライベート IP 制限にはカウントされません。

セキュリティ グループ

コンソールが自動的にセキュリティ グループを作成するので、セキュリティ グループを作成する必要はありません。独自のものを使用する必要がある場合は、**"セキュリティグループルール"**。



コンソール エージェントに関する情報をお探しですか? ["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"](#)

データ階層化のための接続

EBS をパフォーマンス層として使用し、AWS S3 を容量層として使用する場合は、Cloud Volumes ONTAP がS3 に接続されていることを確認する必要があります。この接続を提供する最善の方法は、S3 サービスへの VPC エンドポイントを作成することです。手順については、["AWS ドキュメント: ゲートウェイエンドポイントの作成"](#)。

VPC エンドポイントを作成するときは、Cloud Volumes ONTAP インスタンスに対応するリージョン、VPC、ルートテーブルを選択してください。また、セキュリティ グループを変更して、S3 エンドポイントへのトラフィックを有効にする送信 HTTPS ルールを追加する必要があります。そうしないと、Cloud Volumes ONTAP はS3 サービスに接続できません。

問題が発生した場合は、["AWS サポート ナレッジセンター: ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか?"](#)

ONTAPシステムへの接続

AWS 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、AWS VPC 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、["AWS ドキュメント: AWS VPN 接続の設定"](#)。

CIFS の DNS と Active Directory

CIFS ストレージをプロビジョニングする場合は、AWS で DNS と Active Directory を設定するか、オンプレミスの設定を AWS に拡張する必要があります。

DNS サーバーは、Active Directory 環境に対して名前解決サービスを提供する必要があります。デフォルトの EC2 DNS サーバーを使用するように DHCP オプション セットを設定できます。このサーバーは、Active Directory 環境で使用される DNS サーバーであってはなりません。

手順については、["AWS ドキュメント: AWS クラウド上の Active Directory ドメインサービス: クイックスタートリファレンスデプロイ"](#)。

VPC共有

9.11.1 リリース以降、Cloud Volumes ONTAP HA ペアは VPC 共有により AWS でサポートされるようになりました。VPC 共有により、組織はサブネットを他の AWS アカウントと共有できるようになります。この構成を使用するには、AWS 環境をセットアップし、API を使用して HA ペアをデプロイする必要があります。

["共有サブネットにHAペアを展開する方法を学ぶ"](#)。

複数のAZにおけるHAペアの要件

複数のアベイラビリティゾーン (AZ) を使用するCloud Volumes ONTAP HA 構成には、追加の AWS ネットワーク要件が適用されます。Cloud Volumes ONTAPシステムを追加するときにコンソールにネットワークの詳細を入力する必要があるため、HA ペアを起動する前にこれらの要件を確認する必要があります。

HAペアの仕組みを理解するには、以下を参照してください。["ハイアベイラビリティ ペア"](#)。

アベイラビリティ ゾーン

この HA 展開モデルでは、複数の AZ を使用してデータの高可用性を確保します。各 Cloud Volumes ONTAP インスタンスとメディアエーター インスタンスには専用の AZ を使用する必要があります。これにより、HA ペア間の通信チャネルが提供されます。

各アベイラビリティゾーンでサブネットが利用可能である必要があります。

NASデータとクラスタ/SVM管理用のフローティングIPアドレス

複数の AZ の HA 構成では、障害が発生した場合にノード間で移行されるフローティング IP アドレスが使用されます。VPCの外部からはネイティブにアクセスできません。["AWSトランジットゲートウェイを設定する"](#)。

1 つのフローティング IP アドレスはクラスター管理用、1 つはノード 1 の NFS/CIFS データ用、もう 1 つはノード 2 の NFS/CIFS データ用です。SVM 管理用の 4 番目のフローティング IP アドレスはオプションです。



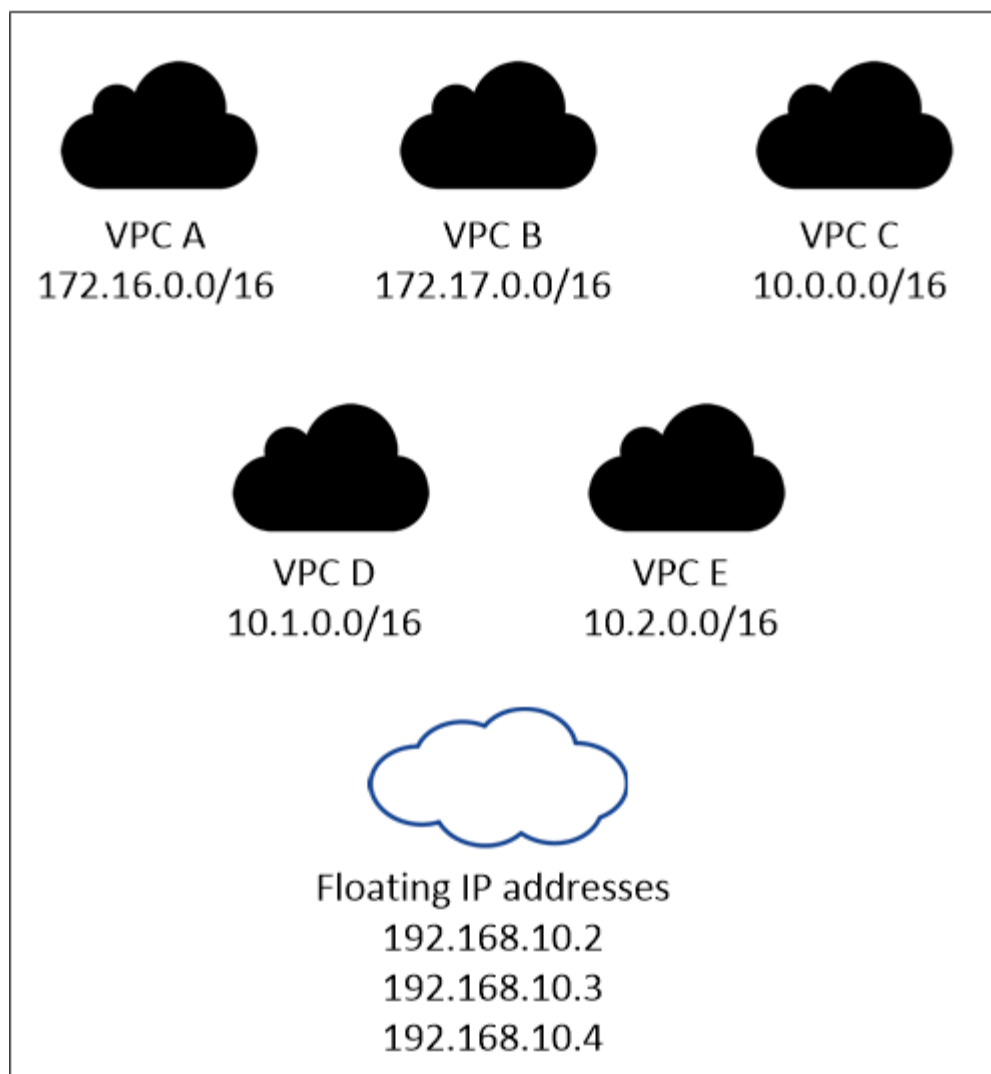
HA ペアで SnapDrive for Windows または SnapCenter を使用する場合は、SVM 管理 LIF にフローティング IP アドレスが必要です。

Cloud Volumes ONTAP HA システムを追加するときは、フローティング IP アドレスを入力する必要があります。コンソールは、システムを起動するときに、HA ペアに IP アドレスを割り当てます。

フローティング IP アドレスは、HA 構成を展開する AWS リージョン内のすべての VPC の CIDR ブロックの外側にある必要があります。フローティング IP アドレスは、リージョン内の VPC の外部にある論理サブネットと考えてください。

次の例は、AWS リージョン内のフローティング IP アドレスと VPC の関係を示しています。フローティング IP アドレスはすべての VPC の CIDR ブロックの外側にありますが、ルートテーブルを通じてサブネットにルーティングできます。

AWS region



コンソールは、iSCSI アクセスおよび VPC 外部のクライアントからの NAS アクセス用に静的 IP アドレスを自動的に作成します。これらのタイプの IP アドレスについては、いかなる要件も満たす必要はありません。

VPC 外部からのフローティング IP アクセスを可能にするトランジット ゲートウェイ

必要であれば、"[AWS トランジットゲートウェイを設定する](#)" HA ペアが存在する VPC の外部から HA ペアのフローティング IP アドレスにアクセスできるようにします。

ルートテーブル

フローティング IP アドレスを指定すると、フローティング IP アドレスへのルートを含めるルート テーブルを選択するように求められます。これにより、クライアントは HA ペアにアクセスできるようになります。

VPC 内のサブネットにルート テーブルが 1 つだけある場合 (メイン ルート テーブル)、コンソールはフローティング IP アドレスをそのルート テーブルに自動的に追加します。ルート テーブルが複数ある場合は、HA ペアを起動するときに正しいルート テーブルを選択することが非常に重要です。そうしないと、一部のクライアントが Cloud Volumes ONTAP にアクセスできなくなる可能性があります。

たとえば、異なるルート テーブルに関連付けられた 2 つのサブネットがある場合があります。ルート テー

ブル A を選択し、ルート テーブル B を選択しない場合、ルート テーブル A に関連付けられたサブネット内のクライアントは HA ペアにアクセスできますが、ルート テーブル B に関連付けられたサブネット内のクライアントはアクセスできません。

ルートテーブルの詳細については、"[AWS ドキュメント: ルートテーブル](#)"。

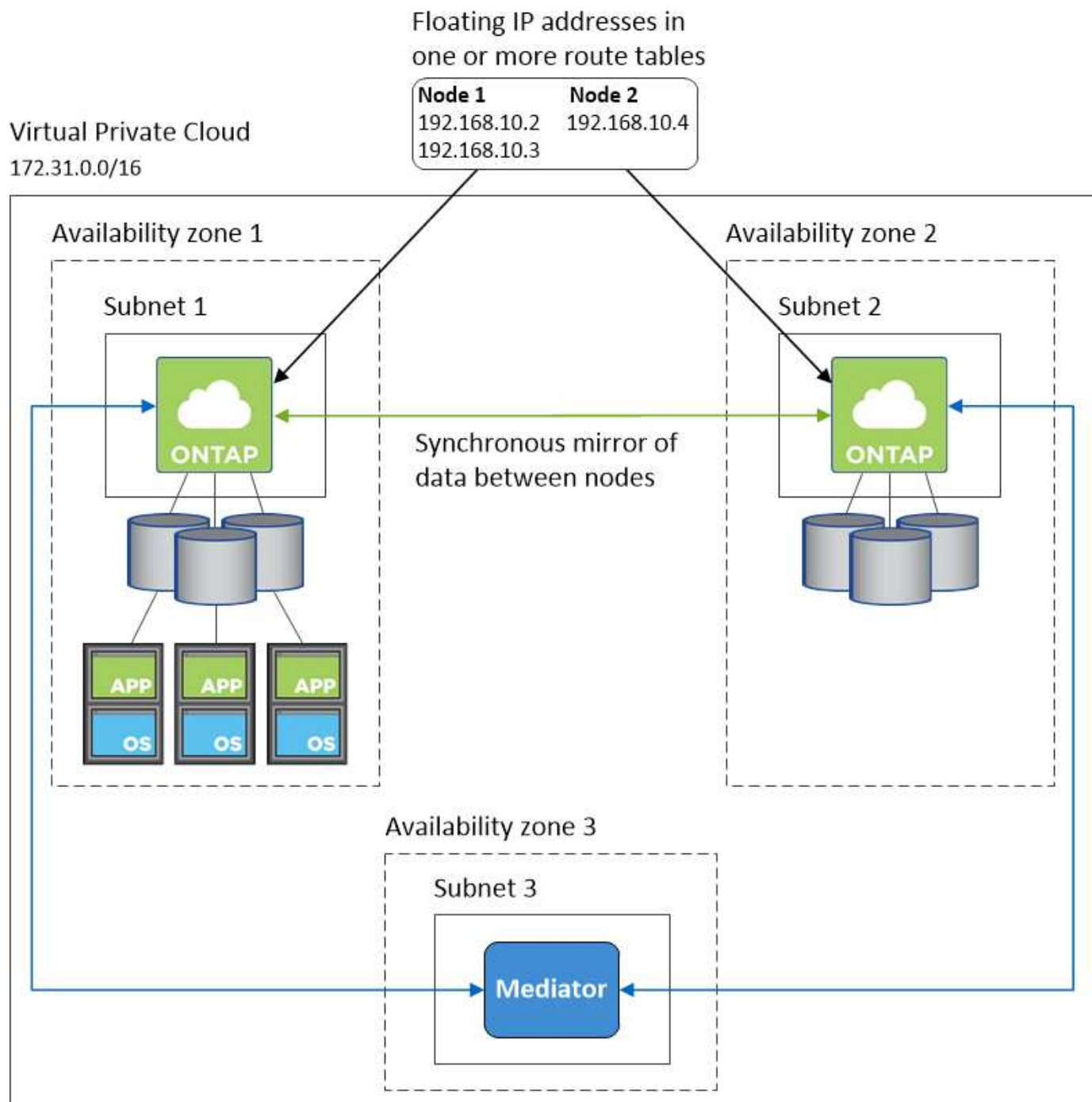
NetApp管理ツールへの接続

複数の AZ にある HA 構成でNetApp管理ツールを使用するには、次の 2 つの接続オプションがあります。

1. NetApp管理ツールを別のVPCに導入し、"[AWSトランジットゲートウェイを設定する](#)"。ゲートウェイにより、VPC の外部からクラスター管理インターフェースのフローティング IP アドレスにアクセスできるようになります。
2. NAS クライアントと同様のルーティング構成を使用して、同じ VPC にNetApp管理ツールを展開します。

HA構成の例

次の図は、複数の AZ 内の HA ペアに固有のネットワーク コンポーネント (3 つのアベイラビリティ ゾーン、3 つのサブネット、フローティング IP アドレス、およびルート テーブル) を示しています。



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、ネットワーク要件を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"
- "AWS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"。

Cloud Volumes ONTAP HAペア用のAWSトランジットゲートウェイを設定する

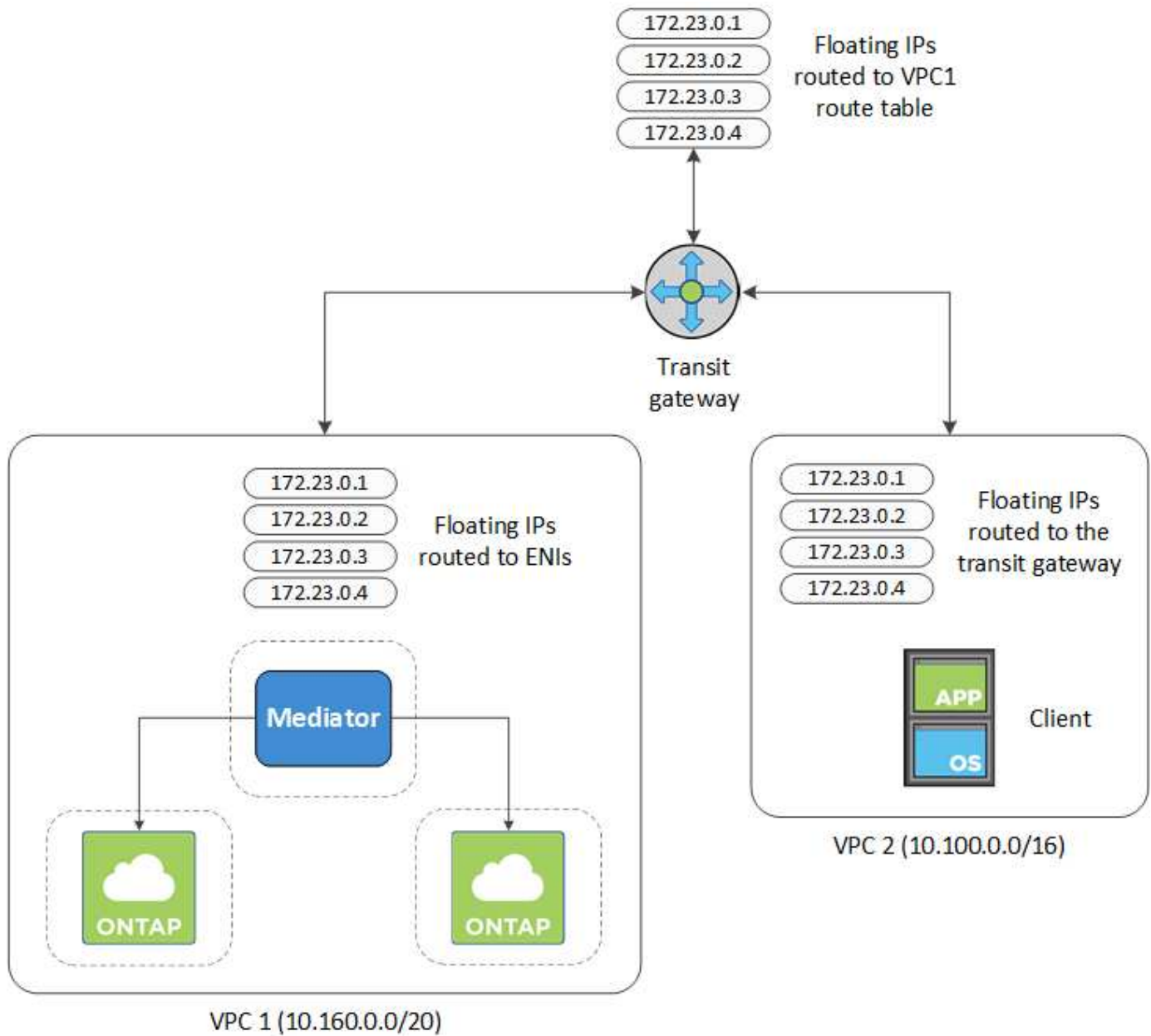
AWSトランジットゲートウェイを設定してHAペアのアクセスを有効にする"[フローティングIPアドレス](#)"HA ペアが存在する VPC の外部から。

Cloud Volumes ONTAP HA 構成が複数の AWS アベイラビリティゾーンに分散されている場合、VPC 内からの NAS データ アクセスにはフローティング IP アドレスが必要です。これらのフローティング IP アドレスは、障害が発生したときにノード間で移行できますが、VPC の外部からはネイティブにアクセスできません。個別のプライベート IP アドレスは VPC 外部からのデータ アクセスを提供しますが、自動フェイルオーバーは提供しません。

クラスタ管理インターフェイスとオプションの SVM 管理 LIF にもフローティング IP アドレスが必要です。

AWS トランジットゲートウェイを設定すると、HA ペアが存在する VPC の外部からフローティング IP アドレスへのアクセスが可能になります。つまり、VPC 外部の NAS クライアントとNetApp管理ツールはフローティング IP にアクセスできます。

以下は、トランジットゲートウェイによって接続された 2 つの VPC を示す例です。HA システムは 1 つの VPC に存在し、クライアントは別の VPC に存在します。その後、フローティング IP アドレスを使用してクライアントに NAS ボリュームをマウントできます。



次の手順では、同様の構成を設定する方法を示します。

手順

1. "トランジットゲートウェイを作成し、VPC をゲートウェイに接続する"。
2. VPC をトランジット ゲートウェイ ルート テーブルに関連付けます。
 - a. **VPC** サービスで、**Transit Gateway** ルート テーブル をクリックします。
 - b. ルート テーブルを選択します。
 - c. *関連付け*をクリックし、*関連付けの作成*を選択します。
 - d. 関連付ける添付ファイル (VPC) を選択し、[関連付けの作成] をクリックします。
3. HA ペアのフローティング IP アドレスを指定して、トランジット ゲートウェイのルート テーブルにルートを作成します。

フローティング IP アドレスは、NetAppコンソールのシステム情報ページで確認できます。次に例を示し

ます。

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management : 172.23.0.1

Data (nfs,cifs) : Node 1: 172.23.0.2 | Node 2: 172.23.0.3

Access

SVM Management : 172.23.0.4

次のサンプル画像は、トランジット ゲートウェイのルート テーブルを示しています。これには、Cloud Volumes ONTAPで使用する 2 つの VPC の CIDR ブロックと 4 つのフローティング IP アドレスへのルートが含まれます。

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details

Associations

Propagations

Routes

Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route

Replace route

Delete route

Filter by attributes or search by keyword

☐	CIDR	Attachment	Resource type	Route type	Route state
☐	10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
☐	10.160.0.0/20	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC1	propagated	active
☐	172.23.0.1/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	VPC	static	active
☐	172.23.0.2/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP Addresses	static	active
☐	172.23.0.3/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP Addresses	static	active
☐	172.23.0.4/32	tgw-attach-00eba3eac3250d7db vpc-673ae603	Floating IP Addresses	static	active

4. フローティング IP アドレスにアクセスする必要がある VPC のルート テーブルを変更します。

- フローティング IP アドレスにルート エントリを追加します。
- HA ペアが存在する VPC の CIDR ブロックにルートエントリを追加します。

次のサンプル画像は、VPC 1 へのルートとフローティング IP アドレスを含む VPC 2 のルートテーブルを示しています。

Route Table: rtb-0569a1bd740ed033f

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.100.0.0/16	local	active	No
0.0.0.0/0	lgw-07250bd01781e67df	active	No
10.160.0.0/20	tgw-015b7c249661ac279	active	No
172.23.0.1/32	tgw-015b7c249661ac279	active	No
172.23.0.2/32	tgw-015b7c249661ac279	active	No
172.23.0.3/32	tgw-015b7c249661ac279	active	No
172.23.0.4/32	tgw-015b7c249661ac279	active	No

VPC1
Floating IP
Addresses

5. フローティング IP アドレスへのアクセスが必要な VPC にルートを追加して、HA ペアの VPC のルートテーブルを変更します。

このステップは、VPC 間のルーティングを完了するため重要です。

次のサンプル画像は、VPC 1 のルートテーブルを示しています。これには、フローティング IP アドレスと、クライアントが存在する VPC 2 へのルートが含まれます。コンソールは、HA ペアを展開するときに、フローティング IP をルートテーブルに自動的に追加しました。

Summary Routes Subnet Associations Route Propagation Tags

Edit routes

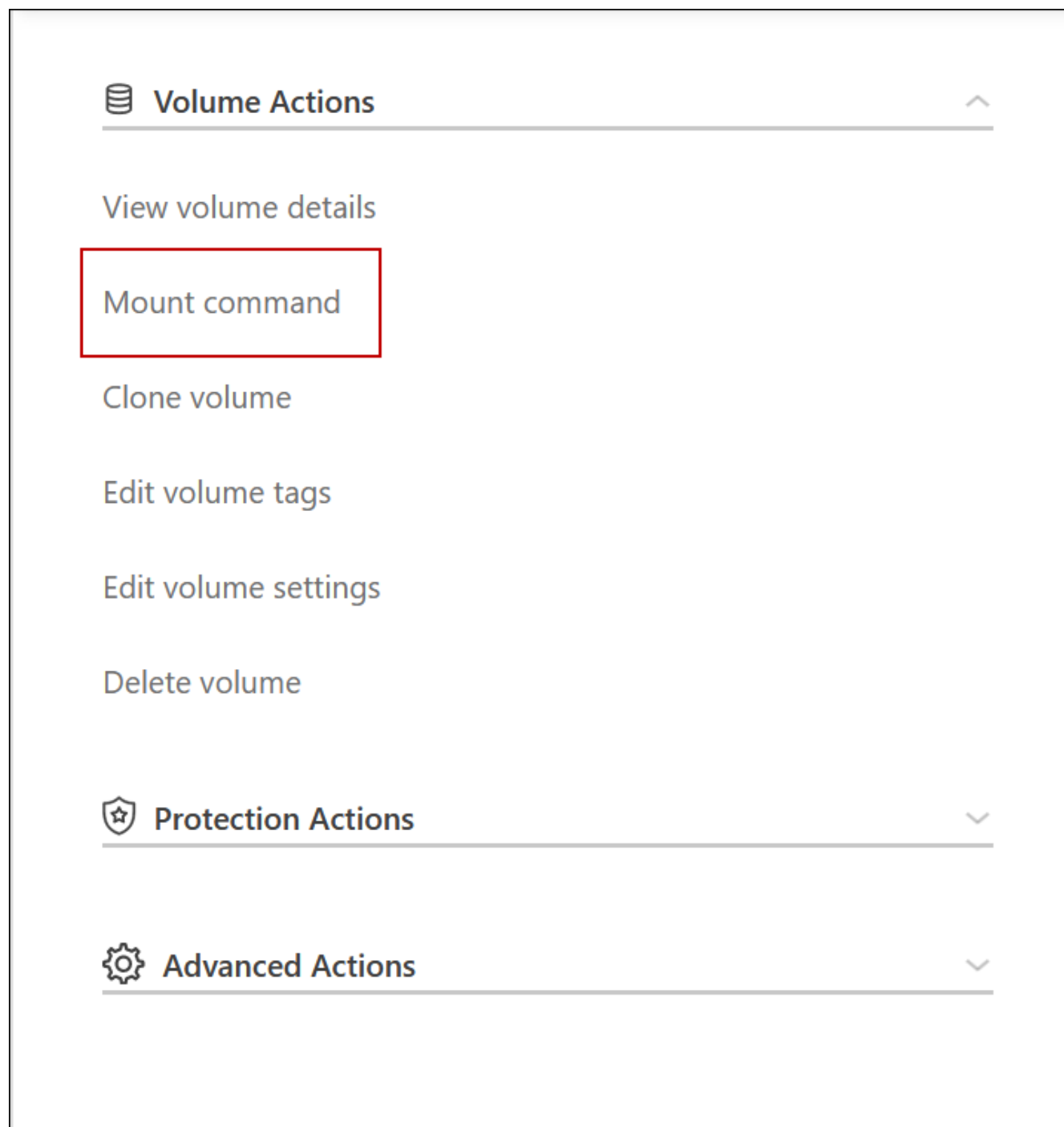
View All routes

Destination	Target	Status
10.160.0.0/20	local	active
pl-68a54001 (com.amazonaws.us-west-2.s3, 54.231.160.0/19, 52.218.128.0/17, 52.92.32.0/22)	vpce-cb51a0a2	active
0.0.0.0/0	lgw-b2182dd7	active
10.60.29.0/25	pcx-589c3331	active
10.100.0.0/16	tgw-015b7c249661ac279	active
10.129.0.0/20	pcx-f7e1396	active
172.23.0.1/32	eni-0854d4715559c3cdb	active
172.23.0.2/32	eni-0854d4715559c3cdb	active
172.23.0.3/32	eni-0f76681216c3108ed	active
172.23.0.4/32	eni-0854d4715559c3cdb	active

VPC2
Floating
act IP
Addresses

6. VPC のセキュリティ グループ設定をすべてのトラフィックに更新します。
- 仮想プライベートクラウドの下で、*サブネット*をクリックします。
 - ルート テーブル タブをクリックし、HA ペアのフローティング IP アドレスの 1 つに対して目的の環境を選択します。
 - *セキュリティ グループ*をクリックします。
 - *受信規則の編集*を選択します。
 - *ルールを追加*をクリックします。
 - [タイプ] で [すべてのトラフィック] を選択し、VPC IP アドレスを選択します。
 - 変更を適用するには、[ルールを保存] をクリックします。
7. フローティング IP アドレスを使用してボリュームをクライアントにマウントします。

コンソールの「ボリュームの管理」パネルの下にある マウント コマンド オプションを通じて、コンソールで正しい IP アドレスを見つけることができます。



8. NFS ボリュームをマウントする場合は、クライアント VPC のサブネットと一致するようにエクスポートポリシーを設定します。

["ボリュームの編集方法を学ぶ"](#)。

関連リンク

- ["AWSのハイアベイラビリティ ペア"](#)

- "AWS におけるCloud Volumes ONTAPのネットワーク要件"

AWS共有サブネットにCloud Volumes ONTAP HAペアをデプロイする

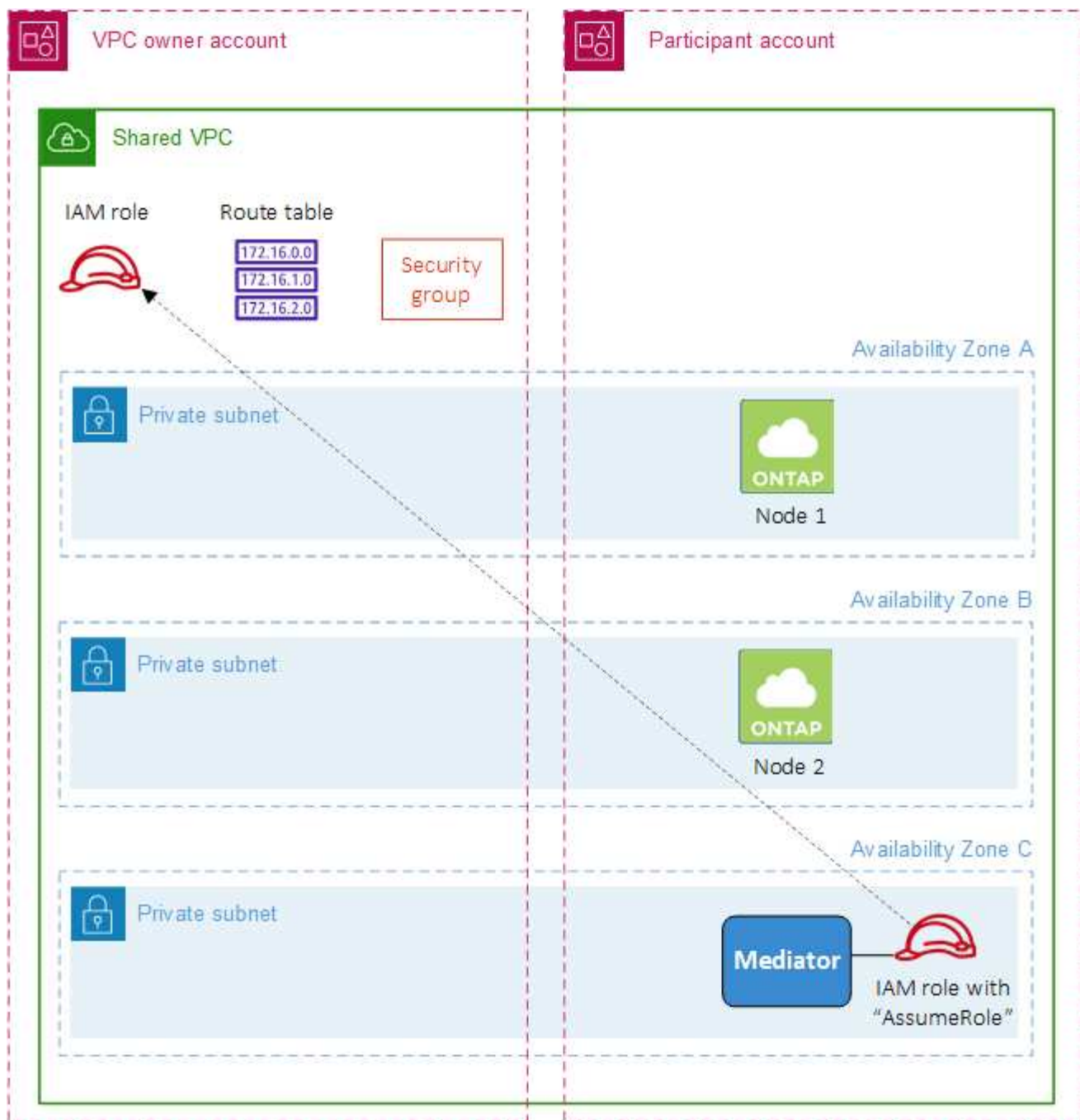
9.11.1 リリース以降、Cloud Volumes ONTAP HA ペアは VPC 共有により AWS でサポートされるようになりました。VPC 共有により、組織はサブネットを他の AWS アカウントと共有できるようになります。この構成を使用するには、AWS 環境をセットアップし、API を使用して HA ペアをデプロイする必要があります。

と "VPC共有"Cloud Volumes ONTAP HA 構成は 2 つのアカウントに分散されています。

- ネットワーク (VPC、サブネット、ルートテーブル、Cloud Volumes ONTAPセキュリティグループ) を所有する VPC 所有者アカウント
- EC2 インスタンスが共有サブネットにデプロイされている参加者アカウント (2 つの HA ノードとメディアエーターを含む)

複数のアベイラビリティゾーンにまたがってデプロイされたCloud Volumes ONTAP HA 構成の場合、HA メディアエーターには、VPC 所有者アカウントのルート テーブルに書き込むための特定の権限が必要です。メディアエーターが引き受けることができる IAM ロールを設定して、これらの権限を付与する必要があります。

次の図は、この展開に関係するコンポーネントを示しています。



以下の手順で説明するように、参加者アカウントとサブネットを共有し、VPC 所有者アカウントに IAM ロールとセキュリティグループを作成する必要があります。

Cloud Volumes ONTAPシステムを作成すると、NetAppコンソールによって IAM ロールが自動的に作成され、メディエーターにアタッチされます。このロールは、HA ペアに関連付けられたルートテーブルに変更を加えるために、VPC 所有者アカウントで作成した IAM ロールを引き継ぎます。

手順

1. VPC 所有者アカウントのサブネットを参加者アカウントと共有します。

この手順は、共有サブネットに HA ペアを展開するために必要です。

["AWS ドキュメント: サブネットの共有"](#)

2. VPC 所有者アカウントで、Cloud Volumes ONTAPのセキュリティ グループを作成します。

["Cloud Volumes ONTAPのセキュリティグループルールを参照してください"](#)。HA メディエーター用のセキュリティ グループを作成する必要はありません。コンソールがそれを実行します。

3. VPC 所有者アカウントで、次の権限を含む IAM ロールを作成します。

```

Action": [
    "ec2:AssignPrivateIpAddresses",
    "ec2:CreateRoute",
    "ec2>DeleteRoute",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
    "ec2:DescribeVpcs",
    "ec2:ReplaceRoute",
    "ec2:UnassignPrivateIpAddresses"

```

4. API を使用して新しいCloud Volumes ONTAPシステムを作成します。

次のフィールドを指定する必要があることに注意してください。

- 「セキュリティグループID」

「securityGroupId」フィールドには、VPC 所有者アカウントで作成したセキュリティ グループを指定する必要があります (上記の手順 2 を参照)。

- 「haParams」 オブジェクトの「assumeRoleArn」

「assumeRoleArn」フィールドには、VPC 所有者アカウントで作成した IAM ロールの ARN を含める必要があります (上記の手順 3 を参照)。

例えば：

```

"haParams": {
    "assumeRoleArn":
    "arn:aws:iam::642991768967:role/mediator_role_assume_fromdev"
}

```

+

["Cloud Volumes ONTAP APIについて学ぶ"](#)

AWS の単一 AZ でCloud Volumes ONTAP HA ペアの配置グループ作成を構成する

配置グループの作成に失敗すると、AWS 単一アベイラビリティゾーン (AZ) でのCloud Volumes ONTAP高可用性 (HA) デプロイメントが失敗し、ロールバックされる可能性があります。Cloud Volumes ONTAPノードとメディエーターインスタンスが利用できない

場合は、配置グループの作成も失敗し、デプロイメントはロールバックされます。これを回避するには、配置グループの作成が失敗した場合でもデプロイメントが完了するように構成を変更します。

ロールバック プロセスをバイパスすると、Cloud Volumes ONTAP のデプロイメント プロセスが正常に完了し、配置グループの作成が完了していないことが通知されます。

手順

1. SSH を使用してNetAppコンソール エージェント ホストに接続し、ログインします。
2. 移動先 `/opt/application/netapp/cloudmanager/docker_occm/data`。
3. 編集 `app.conf` の値を変更することで ``rollback-on-placement-group-failure`` パラメータに ``false``。このパラメータのデフォルト値は `true`。

```
{
  "occm" : {
    "aws" : {
      "rollback-on-placement-group-failure" : false
    }
  }
}
```

4. ファイルを保存し、コンソール エージェントからログオフします。コンソール エージェントを再起動する必要はありません。

Cloud Volumes ONTAPの AWS セキュリティグループのインバウンドおよびアウトバウンドルール

NetAppコンソールは、Cloud Volumes ONTAP が正常に動作するために必要なインバウンドルールとアウトバウンドルールを含む AWS セキュリティグループを作成します。テスト目的の場合、または独自のセキュリティ グループを使用する場合は、ポートを参照することをお勧めします。

Cloud Volumes ONTAPのルール

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。

インバウンドルール

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 **VPC** のみ: 受信トラフィックのソースは、Cloud Volumes ONTAPシステムの VPC 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 VPC 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 **VPC**: 受信トラフィックのソースは 0.0.0.0/0 IP 範囲です。

プロトコル	ポート	目的
すべてのICMP	全て	インスタンスにpingを実行する
HTTP	80	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
HTTPS	443	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
SSH	22	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
TCP	111	NFS のリモート プロシージャ コール
TCP	139	CIFSのNetBIOSサービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
TCP	635	NFSマウント
TCP	749	Kerberos
TCP	2049	NFSサーバ デーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFSロック デーモン
TCP	4046	NFS のネットワーク ステータス モニター
TCP	10000	NDMPを使用したバックアップ
TCP	11104	SnapMirrorのクラスタ間通信セッションの管理
TCP	11105	クラスタ間LIFを使用したSnapMirrorデータ転送
UDP	111	NFS のリモート プロシージャ コール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFSマウント
UDP	2049	NFSサーバ デーモン
UDP	4045	NFSロック デーモン
UDP	4046	NFS のネットワーク ステータス モニター
UDP	4049	NFS rquotadプロトコル

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。

プロトコル	ポート	目的
すべてのICMP	全て	すべての送信トラフィック
すべてTCP	全て	すべての送信トラフィック
すべてUDP	全て	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	プロトコル	ポート	ソース	デスティネーション	目的
Active Directory	TCP	88	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
	UDP	137	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
	UDP	138	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
	TCP	139	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
	TCP とUDP	389	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	TCP	445	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
	TCP	464	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)
	UDP	464	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
	TCP	749	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)
	TCP	88	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
	UDP	137	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
	UDP	138	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
	TCP	139	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
	TCP とUDP	389	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	TCP	445	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
	TCP	464	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)
	UDP	464	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
	TCP	749	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	プロトコル	ポート	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
S3へのバックアップ	TCP	5010	クラスタ間LIF	バックアップエンドポイントまたは復元エンドポイント	S3へのバックアップ機能のバックアップと復元操作
クラスタ	すべてのトラフィック	すべてのトラフィック	すべてのLIFを1つのノードに	他のノード上のすべてのLIF	クラスタ間通信 (Cloud Volumes ONTAP HAのみ)
	TCP	3000	ノード管理LIF	HA Mediator	ZAPI 呼び出し (Cloud Volumes ONTAP HA のみ)
	ICMP	1	ノード管理LIF	HA Mediator	キープアライブ (Cloud Volumes ONTAP HAのみ)
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	UDP	68	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	UDP	67	ノード管理LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理LIFとデータLIF (NFS、CIFS)	DNS	DNS
NDMP	TCP	18600~18699	ノード管理LIF	宛先サーバー	NDMPコピー
SMTP	TCP	25	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

サービス	プロトコル	ポート	ソース	デスティネーション	目的
SNMP	TCP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	TCP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
SnapMirror	TCP	11104	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
	TCP	11105	クラスタ間LIF	ONTAPクラスタ間LIF	SnapMirrorデータ転送
syslog	UDP	514	ノード管理LIF	syslogサーバ	Syslog転送メッセージ

HAメディアエーター外部セキュリティグループのルール

Cloud Volumes ONTAP HA メディアエーターの定義済み外部セキュリティグループには、次のインバウンドルールとアウトバウンドルールが含まれています。

インバウンドルール

HA メディアエーターの定義済みセキュリティグループには、次の受信ルールが含まれています。

プロトコル	ポート	ソース	目的
TCP	3000	コンソールエージェントのCIDR	コンソールエージェントからのRESTful APIアクセス

アウトバウンドルール

HA メディアエーター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

HA メディアエーター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。

プロトコル	ポート	目的
すべてTCP	全て	すべての送信トラフィック
すべてUDP	全て	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、HA メディアエーター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。

プロトコル	ポート	デスティネーション	目的
HTTP	80	AWS EC2 インスタンス上のコンソールエージェントの IP アドレス	メディエーターのアップグレードをダウンロード
HTTPS	443	ec2.amazonaws.com	ストレージフェイルオーバーの支援
UDP	53	ec2.amazonaws.com	ストレージフェイルオーバーの支援



ポート 443 と 53 を開く代わりに、ターゲットサブネットから AWS EC2 サービスへのインターフェイス VPC エンドポイントを作成できます。

HA構成内部セキュリティグループのルール

Cloud Volumes ONTAP HA 構成の定義済み内部セキュリティ グループには、次のルールが含まれています。このセキュリティ グループにより、HA ノード間およびメディエーターとノード間の通信が可能になります。

コンソールは常にこのセキュリティ グループを作成します。独自のものを使用するオプションはありません。

インバウンドルール

定義済みのセキュリティ グループには、次の受信規則が含まれています。

プロトコル	ポート	目的
すべてのトラフィック	全て	HAメディエーターとHAノード間の通信

アウトバウンドルール

定義済みのセキュリティ グループには、次の送信ルールが含まれています。

プロトコル	ポート	目的
すべてのトラフィック	全て	HAメディエーターとHAノード間の通信

コンソールエージェントのルール

["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"](#)

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

Cloud Volumes ONTAPで Amazon 暗号化を使用する場合は、AWS Key Management Service (KMS) を設定する必要があります。

手順

1. アクティブなカスタマー マスター キー (CMK) が存在することを確認します。

CMK は、AWS 管理の CMK またはカスタマー管理の CMK にすることができます。これは、NetAppコンソールおよびCloud Volumes ONTAPと同じ AWS アカウントにすることも、別の AWS アカウントにする

こともできます。

"AWS ドキュメント: カスタマーマスターキー (CMK)"

2. コンソールへの権限を提供する IAM ロールを キー ユーザー として追加して、各 CMK のキー ポリシーを変更します。

Identity and Access Management (IAM) ロールをキーユーザーとして追加すると、コンソールにCloud Volumes ONTAPで CMK を使用する権限が付与されます。

"AWS ドキュメント: キーの編集"

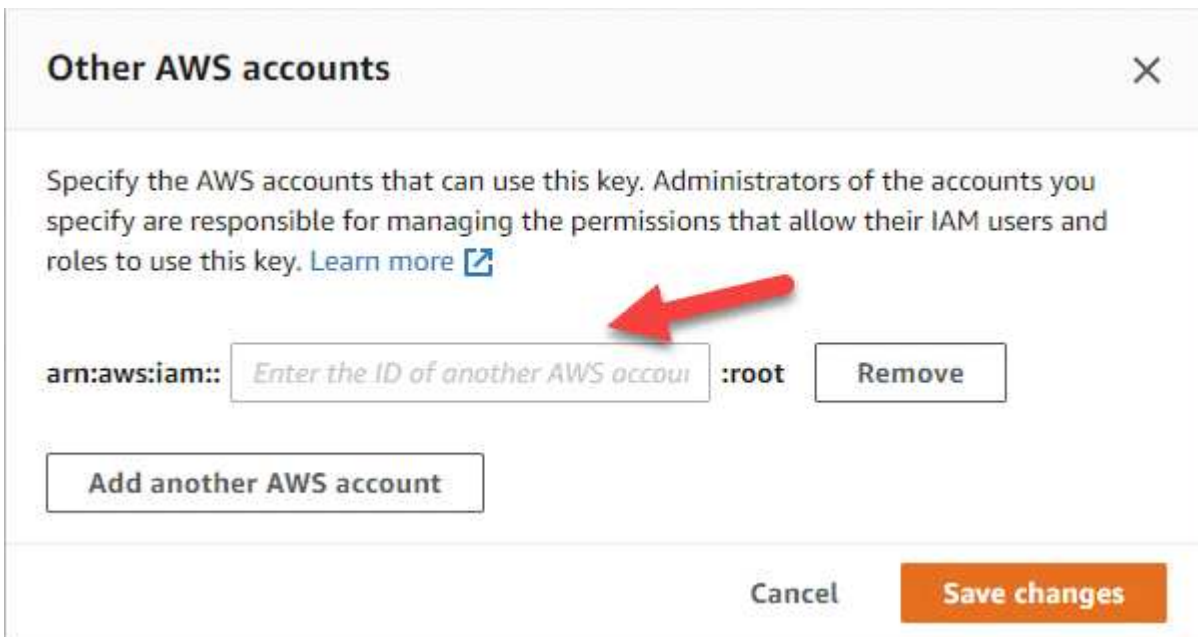
3. CMK が別の AWS アカウントにある場合は、次の手順を実行します。

- a. CMK が存在するアカウントから KMS コンソールに移動します。
- b. キーを選択します。
- c. 一般設定 ペインで、キーの ARN をコピーします。

Cloud Volumes ONTAPシステムを作成するときに、コンソールに ARN を提供する必要があります。

- d. その他の **AWS** アカウント ペインで、コンソールに権限を付与する AWS アカウントを追加します。

通常、これはコンソールが展開されるアカウントです。コンソールが AWS にインストールされていない場合は、コンソールに AWS アクセスキーを提供したアカウントを使用します。



- e. 次に、コンソールに権限を付与する AWS アカウントに切り替えて、IAM コンソールを開きます。
- f. 以下にリストされている権限を含む IAM ポリシーを作成します。
- g. コンソールに権限を提供する IAM ロールまたは IAM ユーザーにポリシーをアタッチします。

次のポリシーは、コンソールが外部 AWS アカウントの CMK を使用するために必要な権限を提供します。「リソース」セクションのリージョンとアカウント ID を必ず変更してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUseOfTheKey",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalkeyid"
      ]
    },
    {
      "Sid": "AllowAttachmentOfPersistentResources",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": [
        "arn:aws:kms:us-east-1:externalaccountid:key/externalaccountid"
      ],
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
```

+

このプロセスの詳細については、["AWSドキュメント: 他のアカウントのユーザーがKMSキーを使用できるようにする"](#)。

4. カスタマー管理の CMK を使用している場合は、Cloud Volumes ONTAP IAM ロールを キー ユーザー として追加して、CMK のキー ポリシーを変更します。

Cloud Volumes ONTAPでデータ階層化を有効にし、S3 バケットに保存されているデータを暗号化する場合は、この手順が必要です。

Cloud Volumes ONTAPシステムを作成すると IAM ロールが作成されるため、Cloud Volumes ONTAP をデプロイした後でこの手順を実行する必要があります。(もちろん、既存のCloud Volumes ONTAP IAM ロールを使用するオプションもあるため、この手順を事前に実行することも可能です。)

["AWS ドキュメント: キーの編集"](#)

Cloud Volumes ONTAPノードのAWS IAMロールを設定する

必要な権限を持つ AWS Identity and Access management (IAM) ロールを各Cloud Volumes ONTAPノードに添付する必要があります。HA メディエーターについても同様です。NetAppコンソールで IAM ロールを作成するのが最も簡単ですが、独自のロールを使用することもできます。

このタスクはオプションです。Cloud Volumes ONTAPシステムを作成する場合、デフォルトのオプションでは、コンソールによって IAM ロールが自動的に作成されます。会社のセキュリティ ポリシーにより IAM ロールを自分で作成する必要がある場合は、以下の手順に従ってください。



AWS Secret Cloud では独自の IAM ロールを提供する必要があります。["C2SでCloud Volumes ONTAPを展開する方法を学ぶ"](#)。

手順

1. AWS IAM コンソールに移動します。
2. 次の権限を含む IAM ポリシーを作成します。
 - Cloud Volumes ONTAPノードの基本ポリシー

標準地域

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws:s3:::fabric-pool-*",
    "Effect": "Allow"
  }
]
```

GovCloud (米国) リージョン

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-us-gov:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-us-gov:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

極秘地域

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

秘密の地域


```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso-b:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

◦ Cloud Volumes ONTAPノードのバックアップポリシー

Cloud Volumes ONTAPシステムでNetApp Backup and Recovery を使用する予定の場合は、ノードの IAM ロールに以下に示す 2 番目のポリシーを含める必要があります。

標準地域

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}
```

GovCloud (米国) リージョン

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-us-gov:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

極秘地域

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

秘密の地域

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws-iso-b:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws-iso-b:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```

- HA Mediator

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses",
      "sts:AssumeRole",
      "ec2:DescribeSubnets"
    ],
    "Resource": "*"
  }]
}
```

3. IAM ロールを作成し、作成したポリシーをロールにアタッチします。

結果

これで、新しいCloud Volumes ONTAPシステムを作成するときに選択できる IAM ロールが用意されました。

詳細情報

- ["AWSドキュメント: IAMポリシーの作成"](#)
- ["AWSドキュメント: IAMロールの作成"](#)

AWS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コンソール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. *詳細と認証情報*ページで、*認証情報の編集 > 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AWS Marketplaceの従量課金制サービスに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、マーケットプレイ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

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ Pay-Per-TiB - Annual Contract
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ Pay-as-you-go
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

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

▼

["AWS でCloud Volumes ONTAP を起動するための手順をご覧ください"](#)。

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、次の消費モデルで利用できます。

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

["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できる必要があります。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. コンソールの 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. [*詳細と認証情報*](#)ページで、[*認証情報の編集 > 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AWS Marketplaceの従量課金制サービスに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

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☐ Pay-Per-TiB - Annual Contract

Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☒ Pay-as-you-go

Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

1 AWS Marketplace

Subscribe and then click **Set Up Your Account** to configure your account.

2 Cloud Manager

Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue

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



"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください"。

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 AWS Marketplace で入手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Cloud Volumes ONTAP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. *詳細と認証情報*ページで、*認証情報の編集>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AWS Marketplaceの従量課金制サービスにサブスクライブします。

The screenshot shows a dialog box titled "Edit Credentials & Add Subscription". Below the title, there is a instruction: "Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe." There are two radio button options: "Pay-Per-TiB - Annual Contract" (described as paying annually upfront) and "Pay-as-you-go" (described as paying at an hourly rate). The "Pay-as-you-go" option is selected. Below these options, a section titled "The next steps:" lists two steps: 1. "AWS Marketplace" (Subscribe and then click **Set Up Your Account** to configure your account.) and 2. "Cloud Manager" (Save your subscription and associate the Marketplace subscription with your AWS credentials.) At the bottom right, there are two buttons: "Continue" (in blue) and "Cancel" (in grey).

- 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

▼

"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください"。



AWS アカウントに関連付けられている AWS Marketplace サブスクリプションは、[設定] > [認証情報] ページから管理できます。"[AWSアカウントとサブスクリプションの管理方法を学ぶ](#)"

年間契約

クラウド プロバイダーのマーケットプレイスから年間契約を購入して、毎年支払います。

時間単位のサブスクリプションと同様に、コンソールでは、AWS Marketplace で利用可能な年間契約にサブスクライブするように求められます。

手順

1. *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. *詳細と認証情報*ページで、*認証情報の編集 > 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AWS Marketplaceで年間契約をサブスクライブします。

Edit Credentials & Add Subscription

Select a subscription option and click **Continue**. The AWS Marketplace enables you to view pricing details and then subscribe.

☒ **Pay-Per-TiB - Annual Contract**
Pay for Cloud Volumes ONTAP with an annual, upfront payment.

☐ **Pay-as-you-go**
Pay for Cloud Volumes ONTAP at an hourly rate.

The next steps:

- 1 AWS Marketplace**
Subscribe and then click **Set Up Your Account** to configure your account.
- 2 Cloud Manager**
Save your subscription and associate the Marketplace subscription with your AWS credentials.

Continue **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	▼

"AWS でCloud Volumes ONTAP を起動するための手順をご覧ください"。

Keystoneサブスクリプション

Keystoneサブスクリプションは、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に問い合わせ](#) して、1 つ以上のKeystoneサブスクリプションでユーザー アカウントを承認してください。
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

"[AWS でCloud Volumes ONTAP を起動するための手順をご覧ください](#)"。

クイックデプロイメントを使用して**AWS**に**Cloud Volumes ONTAP**をデプロイする

単一ノードと高可用性 (HA) 構成の両方に対して、クイック デプロイメント メソッドを使用して、AWS にCloud Volumes ONTAP をデプロイできます。この簡素化されたプロセスにより、高度な方法と比較して展開手順が削減されます。また、1 ページにデフォルト値を自動的に設定し、ナビゲーションを最小限に抑えることで、ワークフローがより明確になります。

開始する前に

NetAppコンソールから AWS にCloud Volumes ONTAPシステムを追加するには、以下が必要です。

- 稼働中のコンソール エージェント。
 - あなたは ["プロジェクトまたはワークスペース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。

構成を選択し、管理者から AWS ネットワーク情報を取得して準備しておく必要があります。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"](#)。

- CIFS 構成用の DNS および Active Directory。

詳細については、["AWS におけるCloud Volumes ONTAPのネットワーク要件"](#)。

タスク概要

Cloud Volumes ONTAPシステムを作成するとすぐに、NetAppコンソールは指定された VPC でテストインスタンスを起動して接続を確認します。成功した場合、コンソールは直ちにインスタンスを終了し、システムの展開を開始します。コンソールが接続を確認できない場合、システムの作成は失敗します。テストインスタンスは、t2.nano（デフォルトのVPCテナンシーの場合）または m3.medium(専用 VPC テナンシーの場合)。

手順

- 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。
- Canvas ページで、[システムの追加] をクリックし、指示に従います。
- Amazon Web Services** > * Cloud Volumes ONTAP* > *新規追加*を選択します。デフォルトでは*クイック作成*オプションが選択されています。



Quick create
Use the recommended and default configuration options. You can change most of these options later.



Advanced create
You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

System details

Show API request

Cloud provider account	Instance Profile Account ID: 2	▼
Name	① Action required	▼
ONTAP Credentials	① Action required	▼
Tags	0 Tags	▼

Deployment and Configuration

Deployment Type	Single node	▼
Network configuration	US East - N. Virginia VPC name - 172.31.0.0/16 Subnet name -	▼

Charging and Services

Marketplace subscription	Sub2-ByCapacityByNodePYGO_delete_after_1234	▼
License	Freemium (Up to 500 GiB)	▼
Data services and features	Netapp Backup and Recovery	▼
NetApp Support Site account	No existing account	▼

Summary

Overview	▼

Create

Cancel

システムの詳細

- クラウド プロバイダー アカウント: アカウントの詳細は、選択したコンソール エージェントに基づいて自動的に入力されます。複数のアカウントをお持ちの場合は、使用するアカウントを選択してください。コンソールエージェントが利用できない場合は、"[コンソールエージェントを作成する](#)"。
- 名前: システム名。コンソールは、システム (クラスター) 名を使用して、Cloud Volumes ONTAPシステムと Amazon EC2 インスタンスに名前を付けます。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。
- * ONTAP認証情報* これらは、Cloud Volumes ONTAPクラスター管理者アカウントの認証情報です。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 *admin* ユーザー名をそのまま使用することも、カスタム ユーザー名に変更することもできます。
- タグ AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAPインスタン

スト、インスタンスに関連付けられている各 AWS リソースにタグを追加します。Cloud Volumes ONTAP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 15 個のタグを追加でき、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、["AWS ドキュメント: Amazon EC2 リソースのタグ付け"](#)。

展開と構成

1. デプロイメント タイプ: 使用するデプロイメント タイプ (単一ノード、単一の可用性ゾーン (AZ) での高可用性 (HA)、または複数の AZ での HA) を選択します。
2. ネットワーク設定: 記録したネットワーク情報を入力します。 ["AWS ワークシート"](#)。
 - a. **AWS リージョン**: デフォルトでは、サブネット リソースを持つ VPC を持つ関連クラウド アカウントのリージョンが選択されます。
 - b. **VPC**: サブネットを持つ AWS リージョンの VPC を入力します。サブネットがない場合、VPC のデフォルト値が選択されます。
 - c. サブネット: 単一ノードのデプロイメントまたは単一 AZ 内の HA デプロイメントの場合にのみ、VPC のサブネットを選択できます。

高可用性

HA 構成を選択した場合は、次の情報を入力します。

単一AZのHA

1. メディエーター アクセス: メディエーター アクセス情報を指定します。メディエーターは、HA ペアの健全性を監視し、障害発生時にクォーラムを提供する別のインスタンスです。キーペア名を指定して、メディエーターインスタンスが AWS EC2 サービスに接続できるようにし、接続方法を選択します。

複数のAZでのHA

1. アベイラビリティゾーンとメディエーター: 各ノードとメディエーターのアベイラビリティゾーン (AZ) と、Cloud Volumes ONTAP HA ペアを展開する対応するサブネットを選択します。
2. フローティング IP: 複数の AZ を選択した場合は、NFS および CIFS サービスとクラスターおよび SVM 管理のフローティング IP アドレスを指定します。IP アドレスは、リージョン内のすべての VPC の CIDR ブロックの外側にある必要があります。詳細については、["複数の AZ におけるCloud Volumes ONTAP HA の AWS ネットワーク要件"](#)。
3. メディエーター アクセス: メディエーター アクセス情報を指定します。メディエーターは、HA ペアの健全性を監視し、障害発生時にクォーラムを提供する別のインスタンスです。キーペア名を指定して、メディエーターインスタンスが AWS EC2 サービスに接続できるようにし、接続方法を選択します。
4. ルート テーブル: 複数の AZ を選択した場合は、フローティング IP アドレスへのルートを含むルート テーブルを選択します。ルート テーブルが複数ある場合は、正しいルート テーブルを選択することが重要です。そうしないと、一部のクライアントがCloud Volumes ONTAP HA ペアにアクセスできなくなる可能性があります。ルートテーブルの詳細については、["AWS ドキュメント: ルートテーブル"](#)。

充電とサービス

1. マーケットプレイス サブスクリプション: このCloud Volumes ONTAPシステムで使用する AWS マーケットプレイス サブスクリプションを選択します。
2. ライセンス: このCloud Volumes ONTAPシステムで使用するライセンスの種類を選択します。

Professional、Essential、Premium のライセンスから選択できます。さまざまなライセンスの詳細については、以下を参照してください。"[Cloud Volumes ONTAPライセンスについて学ぶ](#)"。

3. データ サービスと機能: Cloud Volumes ONTAPで使用しないサービスを有効のままにするか、無効にします。
 - "[NetAppの分類について詳しくはこちら](#)"
 - "[NetAppバックアップとリカバリの詳細](#)"
 - "[Cloud Volumes ONTAPの WORM ストレージについて学ぶ](#)"



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。

- * NetAppサポート サイト アカウント*: 複数のアカウントがある場合は、使用するアカウントを選択します。

まとめ

入力した詳細を確認または編集し、「作成」をクリックします。

関連リンク

- "[Cloud Volumes ONTAP構成の計画](#)"
- "[高度なデプロイメントを使用して AWS にCloud Volumes ONTAPをデプロイする](#)"

AWS でCloud Volumes ONTAP を起動

Cloud Volumes ONTAP は、単一システム構成で、または AWS の HA ペアとして起動できます。この方法では、クイック デプロイメント メソッドよりも多くの構成オプションと柔軟性を備えた高度なデプロイメント エクスペリエンスが提供されます。

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。

構成を選択し、管理者から AWS ネットワーク情報を取得して準備しておく必要があります。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](#)"。

- CIFS 構成用の DNS および Active Directory。

詳細については、"[AWS におけるCloud Volumes ONTAPのネットワーク要件](#)"。

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

AWS でCloud Volumes ONTAPを起動する場合は、NetAppコンソールで新しいシステムを作成する必要があります。

タスク概要

システムを作成するとすぐに、コンソールは指定された VPC でテストインスタンスを起動して接続を確認します。成功した場合、コンソールはインスタンスを直ちに終了し、Cloud Volumes ONTAPシステムのデプロイを開始します。接続を検証できない場合、システムの作成は失敗します。テストインスタンスは、t2.nano（デフォルトのVPCテナンシーの場合）または m3.medium(専用 VPC テナンシーの場合)。

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. **Amazon Web Services** と * Cloud Volumes ONTAP Single Node* を選択します。
4. *詳細作成*を選択します。デフォルトでは*クイック作成*モードが選択されているため、デフォルト値に関するメッセージが表示される場合があります。*続行*をクリックします。
5. 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"](#)。
6. 詳細と認証情報: オプションで AWS 認証情報とサブスクリプションを変更し、システム名を入力し、必要に応じてタグを追加して、パスワードを入力します。

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
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 Amazon EC2 インスタンス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。
タグを追加する	AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAPインスタンスと、インスタンスに関連付けられている各 AWS リソースにタグを追加します。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、 "AWS ドキュメント: Amazon EC2 リソースのタグ付け" 。
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。

フィールド	説明
資格情報の編集	このシステムをデプロイするアカウントに関連付けられている AWS 認証情報を選択します。このCloud Volumes ONTAPシステムで使用する AWS マーケットプレイス サブスクリプションに関連付けることもできます。「サブスクリプションを追加」をクリックすると、選択した認証情報が新しいAWSマーケットプレイスサブスクリプションに関連付けられます。サブスクリプションは年間契約または時間単位でCloud Volumes ONTAPをお支払いいただくことができます。NetApp https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html ["NetApp コンソールにAWS認証情報を追加する方法を学びます"]。

複数の IAM ユーザーが同じ AWS アカウントで作業する場合は、各ユーザーがサブスクライブする必要があります。最初のユーザーがサブスクライブすると、AWS マーケットプレイスは、以下の画像に示すように、後続のユーザーにすでにサブスクライブしていることを通知します。AWS アカウントにサブスクリプションが設定されている場合は、各 IAM ユーザーが自分自身をそのサブスクリプションに関連付ける必要があります。以下のメッセージが表示された場合は、「ここをクリック」リンクをクリックしてコンソールの Web サイトに移動し、プロセスを完了してください。



NetApp Cloud Volumes ONTAP (CVO), delivered by ePlus Info

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

[Subscribe](#)

You are already subscribed to this product

Pricing Details

Software Fees

- サービス: サービスを有効のままにするか、Cloud Volumes ONTAPで使用しない個々のサービスを無効にします。
 - "NetAppデータ分類の詳細"
 - "NetAppバックアップとリカバリの詳細"



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리를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。

- 場所と接続: 記録したネットワーク情報を入力します。"AWS ワークシート"。

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
VPC	AWS Outpost がある場合は、Outpost VPC を選択して、その Outpost に単一ノードのCloud Volumes ONTAPシステムをデプロイできます。エクスペリエンスは、AWS にある他の VPC と同じです。

フィールド	説明
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 VPC 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 VPC 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 VPC 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 VPC 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。
既存のセキュリティグループを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ"。

9. データ暗号化: データ暗号化なし、または AWS 管理の暗号化を選択します。

AWS 管理の暗号化の場合、自分のアカウントまたは別の AWS アカウントから別のカスタマーマスターキー (CMK) を選択できます。



Cloud Volumes ONTAPシステムを作成した後、AWS データ暗号化方法を変更することはできません。

"[Cloud Volumes ONTAP用の AWS KMS を設定する方法を学びます](#)"。

"[サポートされている暗号化技術の詳細](#)"。

10. 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](#)"。

11. * Cloud Volumes ONTAP構成* (年間 AWS マーケットプレイス契約のみ): デフォルトの構成を確認して [続行] をクリックするか、[構成の変更] をクリックして独自の構成を選択します。

デフォルト構成を維持する場合は、ボリュームを指定して、構成を確認して承認するだけです。

12. 事前構成済みパッケージ: いずれかのパッケージを選択してCloud Volumes ONTAP をすばやく起動するか、*構成の変更*をクリックして独自の構成を選択します。

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て承認するだけです。

13. **IAM** ロール: コンソールでロールを自動的に作成できるように、デフォルト オプションを維持するのが最適です。

独自のポリシーを使用する場合は、次の条件を満たす必要があります。"[Cloud Volumes ONTAPノードのポリシー要件](#)"。

14. ライセンス: 必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンス タイプとインスタンス テナancy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、コンソールはシステムの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。

15. 基盤となるストレージ リソース: ディスク タイプを選択し、基盤となるストレージを構成し、データ階層化を有効のまま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 タイプは初期ボリューム (およびアグリゲート) 用です。後続のボリューム (およびアグリゲート) には、異なるディスク タイプを選択できます。
- gp3 または io1 ディスクを選択した場合、コンソールは AWS の Elastic Volumes 機能を使用して、必要に応じて基盤となるストレージ ディスク容量を自動的に増加します。ストレージのニーズに基づいて初期容量を選択し、Cloud Volumes ONTAP の導入後に修正することができます。["AWS の Elastic Volumes のサポートについて詳しく見る"](#)。
- gp2 または st1 ディスクを選択した場合は、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ディスク サイズを選択できます。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。
- 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。

["データ階層化の仕組みを学ぶ"](#)。

16. 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。

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。

17. 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

ABDcv5689

Storage VM (SVM)

svm_CVO1

Volume Size

100

Unit

GiB

Snapshot Policy

default

default policy

18. **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。AWS Managed Microsoft AD を Cloud Volumes ONTAP の AD サーバーとして設定する場合は、このフィールドに OU=Computers,OU=corp と入力する必要があります。
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 コンソール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。

19. 使用プロファイル、ディスク タイプ、階層化ポリシー: ストレージ効率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編集します。

詳細については、"[ボリューム使用プロファイルの理解](#)"、"[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?](#)"

20. 確認と承認: 選択内容を確認して確定します。

- 構成の詳細を確認します。
- 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 AWS リソースの詳細を確認できます。
- 理解しました... チェックボックスを選択します。
- [Go] をクリックします。

結果

コンソールはCloud Volumes ONTAPインスタンスを起動します。*監査*ページで進捗状況を追跡できます。

Cloud Volumes ONTAPインスタンスの起動で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。

AWSでCloud Volumes ONTAP HAペアを起動する

AWS 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。

制限

現時点では、HA ペアはAWS Outposts ではサポートされていません。

タスク概要

Cloud Volumes ONTAPシステムを作成するとすぐに、コンソールは指定された VPC でテストインスタンスを起動して接続を確認します。成功した場合、コンソールはインスタンスを直ちに終了し、Cloud Volumes ONTAPシステムのデプロイを開始します。接続を検証できない場合、システムの作成は失敗します。テストインスタンスは、t2.nano（デフォルトのVPCテナンシーの場合）またはm3.medium(専用 VPC テナンシーの場合)。

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. **Amazon Web Services** と * Cloud Volumes ONTAP HA* を選択します。

いくつかのAWS ローカルゾーンが利用可能です。

AWS Local Zones を使用する前に、Local Zones を有効にし、AWS アカウントの Local Zone にサブネットを作成する必要があります。AWSローカルゾーンにオプトインする*とAmazon VPCをローカルゾーンに拡張する*の手順に従ってください。["AWS チュートリアル「AWS ローカルゾーンを使用した低レイテンシーアプリケーションのデプロイ開始」](#)。

コンソールエージェント3.9.36以前を実行している場合は、DescribeAvailabilityZones AWS EC2 コンソールのAWS ロールへの権限。

4. 詳細と認証情報: オプションでAWS 認証情報とサブスクリプションを変更し、システム名を入力し、必要に応じてタグを追加して、パスワードを入力します。

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
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Amazon EC2 インスタンス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
タグを追加する	AWS タグは、AWS リソースのメタデータです。コンソールは、Cloud Volumes ONTAP インスタンスと、インスタンスに関連付けられている各 AWS リソースにタグを追加します。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、 "AWS ドキュメント: Amazon EC2 リソースのタグ付け" 。
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 AWS 認証情報とマーケットプレイスサブスクリプションを選択してください。「サブスクリプションを追加」をクリックすると、選択した認証情報が新しい AWS マarketプレイスサブスクリプションに関連付けられます。サブスクリプションは年間契約または時間単位で Cloud Volumes ONTAP をお支払いいただくことができます。NetApp から直接ライセンスを購入された場合（NetApp (Bring Your Own License)）、AWS サブスクリプションは不要です。NetApp 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" 。https://docs.netapp.com/us-en/bluexp-setup-admin/task-adding-aws-accounts.html["コンソールに AWS 認証情報を追加する方法を学びます"]。

複数の IAM ユーザーが同じ AWS アカウントで作業する場合は、各ユーザーがサブスクライブする必要があります。最初のユーザーがサブスクライブすると、AWS マーケットプレイスは、以下の画像に示すように、後続のユーザーにすでにサブスクライブしていることを通知します。AWS アカウントにサブスクリプションが設定されている場合は、各 IAM ユーザーが自分自身をそのサブスクリプションに関連付ける必要があります。以下のメッセージが表示された場合は、「ここをクリック」リンクをクリックしてコンソールの Web サイトに移動し、プロセスを完了してください。



NetApp Cloud Volumes ONTAP (CVO), delivered by ePlus Info

You are currently subscribed to this product and will be charged for your accumulated usage at the end of your next billing cycle, based on the costs listed in Pricing information on the right.

Having issues signing up for your product?
If you were unable to complete the set-up process for this software, please [click here](#) to be taken to the product's registration area.

Subscribe

You are already subscribed to this product

Pricing Details

Software Fees

5. サービス: サービスを有効のままにするか、この Cloud Volumes ONTAP システムで使用しない個々のサービスを無効にします。

- ["NetApp データ分類の詳細"](#)
- ["バックアップとリカバリの詳細"](#)



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:** HA 構成を選択します。

展開モデルの概要については、以下を参照してください。"[AWS 向けCloud Volumes ONTAP HA](#)"。

7. **場所と接続 (単一のアベイラビリティゾーン (AZ)) または リージョンと VPC (複数の AZ):** AWS ワークシートに記録したネットワーク情報を入力します。

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
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 VPC 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 VPC 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 VPC 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 VPC 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。
既存のセキュリティグループを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。" Cloud Volumes ONTAPのファイアウォールルールについて学ぶ "。

8. **接続と SSH 認証:** HA ペアとメディエーターの接続方法を選択します。

9. **フローティング IP:** 複数の AZ を選択した場合は、フローティング IP アドレスを指定します。

IP アドレスは、リージョン内のすべての VPC の CIDR ブロックの外側にある必要があります。詳細については、"[複数の AZ におけるCloud Volumes ONTAP HA の AWS ネットワーク要件](#)"。

10. **ルート テーブル:** 複数の AZ を選択した場合は、フローティング IP アドレスへのルートを含めるルート テーブルを選択します。

ルート テーブルが複数ある場合は、正しいルート テーブルを選択することが非常に重要です。そうしないと、一部のクライアントがCloud Volumes ONTAP HA ペアにアクセスできなくなる可能性があります。ルートテーブルの詳細については、"[AWS ドキュメント: ルートテーブル](#)"。

11. **データ暗号化:** データ暗号化なし、または AWS 管理の暗号化を選択します。

AWS 管理の暗号化の場合、自分のアカウントまたは別の AWS アカウントから別のカスタマーマスターキー (CMK) を選択できます。



Cloud Volumes ONTAPシステムを作成した後、AWS データ暗号化方法を変更することはできません。

"[Cloud Volumes ONTAP用の AWS KMS を設定する方法を学びます](#)"。

"[サポートされている暗号化技術の詳細](#)"。

12. **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"](#)。

13. * Cloud Volumes ONTAP構成* (年間 AWS Marketplace 契約のみ): デフォルトの構成を確認して [続行] をクリックするか、[構成の変更] をクリックして独自の構成を選択します。

デフォルト構成を維持する場合は、ボリュームを指定して、構成を確認して承認するだけです。

14. 事前構成済みパッケージ (時間単位またはBYOLのみ) : いずれかのパッケージを選択してCloud Volumes ONTAPをすばやく起動するか、*構成の変更*をクリックして独自の構成を選択します。

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て承認するだけです。

15. **IAM** ロール: コンソールでロールを自動的に作成できるように、デフォルト オプションを維持するのが最適です。

独自のポリシーを使用する場合は、次の条件を満たす必要があります。["Cloud Volumes ONTAPノードとHAメディアエーターのポリシー要件"](#)。

16. ライセンス: 必要に応じてCloud Volumes ONTAP のバージョンを変更し、インスタンス タイプとインスタンス テナancy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、コンソールはシステムの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。

17. 基盤となるストレージ リソース: ディスク タイプを選択し、基盤となるストレージを構成し、データ階層化を有効のまま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 タイプは初期ボリューム (およびアグリゲート) 用です。後続のボリューム (およびアグリゲート) には、異なるディスク タイプを選択できます。
- gp3 または io1 ディスクを選択した場合、コンソールは AWS の Elastic Volumes 機能を使用して、必要に応じて基盤となるストレージ ディスク容量を自動的に増加します。ストレージのニーズに基づいて初期容量を選択し、Cloud Volumes ONTAP の導入後に修正することができます。["AWS の Elastic Volumes のサポートについて詳しく見る"](#)。
- gp2 または st1 ディスクを選択した場合は、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ディスク サイズを選択できます。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。
- 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。

["データ階層化の仕組みを学ぶ"](#)。

18. 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。

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。

19. 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。

フィールド	説明
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

ABDcv5689

Storage VM (SVM)

svm_c...CVO1

Volume Size

100

Unit

GiB

Snapshot Policy

default

default policy

20. **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。AWS Managed Microsoft AD をCloud Volumes ONTAP の AD サーバーとして設定する場合は、このフィールドに OU=Computers,OU=corp と入力する必要があります。

フィールド	説明
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コンソール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。

21. 使用プロファイル、ディスク タイプ、階層化ポリシー: ストレージ効率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編集します。

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"そして"データ階層化の概要"](#)。

22. 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 AWS 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 HA ペアを起動します。*監査*ページで進捗状況を追跡できます。

HA ペアの起動時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。

関連リンク

- ["Cloud Volumes ONTAP構成の計画"](#)
- ["クイックデプロイメントを使用してAWSにCloud Volumes ONTAPをデプロイする"](#)

AWS Secret Cloud または **AWS Top Secret Cloud** に**Cloud Volumes ONTAP** を導入する

標準のAWSリージョンと同様に、NetAppコンソールは["AWS シークレットクラウド"](#)そ

して["AWSトップシークレットクラウド"](#)クラウド ストレージにエンタープライズ クラスの機能を提供するCloud Volumes ONTAPを導入します。AWS Secret Cloud と Top Secret Cloud は、米国インテリジェンスコミュニティに固有のクローズドリージョンです。このページの手順は、AWS Secret Cloud および Top Secret Cloud リージョンのユーザーにのみ適用されます。

開始する前に

始める前に、AWS Secret Cloud と Top Secret Cloud でサポートされているバージョンを確認し、コンソールのプライベートモードについて学んでください。

- AWS Secret Cloud および Top Secret Cloud でサポートされている次のバージョンを確認します。
 - Cloud Volumes ONTAP 9.12.1 P2
 - コンソールエージェントのバージョン3.9.32

AWS でCloud Volumes ONTAP をデプロイおよび管理するには、コンソール エージェントが必要です。コンソール エージェントのインスタンスにインストールされるソフトウェアからコンソールにログインします。コンソールの SaaS ウェブサイトは、AWS Secret Cloud および Top Secret Cloud ではサポートされていません。

- プライベートモードについて学ぶ

AWS Secret Cloud および Top Secret Cloud では、コンソールは プライベート モード で動作します。プライベート モードでは、コンソールから SaaS レイヤーに接続できません。コンソール エージェントにアクセスできるローカルの Web ベースのアプリケーションを通じてコンソールにアクセスできます。

プライベートモードの仕組みの詳細については、以下を参照してください。["コンソールのプライベート展開モード"](#)。

ステップ1: ネットワークを設定する

Cloud Volumes ONTAP が適切に動作するように AWS ネットワークを設定します。

手順

1. コンソール エージェントのインスタンスとCloud Volumes ONTAPインスタンスを起動する VPC とサブネットを選択します。
2. VPC 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していることを確認します。
3. S3 サービスへの VPC エンドポイントを設定します。

Cloud Volumes ONTAPから低コストのオブジェクト ストレージにコールド データを階層化する場合は、VPC エンドポイントが必要です。

ステップ2: 権限を設定する

AWS Secret Cloud または Top Secret Cloud でアクションを実行するために必要な権限をコンソールエージェントとCloud Volumes ONTAP に付与する IAM ポリシーとロールを設定します。

次のそれぞれに対して IAM ポリシーと IAM ロールが必要です。

- コンソールエージェントのインスタンス
- Cloud Volumes ONTAPインスタンス
- HAペアの場合、Cloud Volumes ONTAP HAメディエーターインスタンス（HAペアを展開する場合）

手順

1. AWS IAM コンソールに移動し、*ポリシー*をクリックします。
2. コンソール エージェントのインスタンスのポリシーを作成します。



これらのポリシーは、AWS 環境内の S3 バケットをサポートするために作成します。後でバケットを作成するときに、バケット名に接頭辞が付けられていることを確認してください。fabric-pool-。この要件は、AWS Secret Cloud リージョンと Top Secret Cloud リージョンの両方に適用されます。


```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
    ]
  }]
}
```

```

        "iam:PassRole",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:ListInstanceProfiles",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",

```

```

        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:volume/*"
    ]
}
]
}

```

極秘地域

```

{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:DescribeRouteTables",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:DescribeVolumes",
            "ec2:ModifyVolumeAttribute",
            "ec2>DeleteVolume",
            "ec2:CreateSecurityGroup",
            "ec2>DeleteSecurityGroup",
            "ec2:DescribeSecurityGroups",

```

```
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateNetworkInterface",
"ec2:DescribeNetworkInterfaces",
"ec2>DeleteNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DescribeSubnets",
"ec2:DescribeVpcs",
"ec2:DescribeDhcpOptions",
"ec2:CreateSnapshot",
"ec2>DeleteSnapshot",
"ec2:DescribeSnapshots",
"ec2:GetConsoleOutput",
"ec2:DescribeKeyPairs",
"ec2:DescribeRegions",
"ec2>DeleteTags",
"ec2:DescribeTags",
"cloudformation:CreateStack",
"cloudformation>DeleteStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"iam:PassRole",
"iam:CreateRole",
"iam>DeleteRole",
"iam:PutRolePolicy",
"iam:ListInstanceProfiles",
"iam:CreateInstanceProfile",
"iam>DeleteRolePolicy",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam>DeleteInstanceProfile",
"s3:GetObject",
"s3:ListBucket",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListAllMyBuckets",
"kms:List*",
"kms:Describe*",
"ec2:AssociateIamInstanceProfile",
"ec2:DescribeIamInstanceProfileAssociations",
"ec2:DisassociateIamInstanceProfile",
"ec2:DescribeInstanceAttribute",
"ec2:CreatePlacementGroup",
```

```

        "ec2:DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}

```

```
}  
]
```

3. Cloud Volumes ONTAPのポリシーを作成します。

秘密の地域

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso-b:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3>DeleteObject"
    ],
    "Resource": "arn:aws-iso-b:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}
```

極秘地域

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": "s3:ListAllMyBuckets",
    "Resource": "arn:aws-iso:s3:::*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }, {
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": "arn:aws-iso:s3:::fabric-pool-*",
    "Effect": "Allow"
  }]
}

```

HA ペアの場合、Cloud Volumes ONTAP HA ペアを展開する予定であれば、HA メディエーターのポリシーを作成します。


```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AssignPrivateIpAddresses",
      "ec2:CreateRoute",
      "ec2>DeleteRoute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeVpcs",
      "ec2:ReplaceRoute",
      "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": "*"
  }]
}
```

4. ロールタイプが Amazon EC2 の IAM ロールを作成し、前の手順で作成したポリシーをアタッチします。

ロールを作成します。

ポリシーと同様に、コンソール エージェント用に IAM ロールを 1 つ、Cloud Volumes ONTAP ノード用に IAM ロールを 1 つ用意する必要があります。HA ペアの場合: ポリシーと同様に、コンソール エージェント用に 1 つの IAM ロール、Cloud Volumes ONTAP ノード用に 1 つ、HA メディエーター用に 1 つ (HA ペアを展開する場合) の IAM ロールが必要です。

役割を選択してください:

コンソール エージェントのインスタンスを起動するときに、コンソール エージェントの IAM ロールを選択する必要があります。コンソールから Cloud Volumes ONTAP システムを作成するときに、Cloud Volumes ONTAP の IAM ロールを選択できます。HA ペアの場合、Cloud Volumes ONTAP システムを作成するときに、Cloud Volumes ONTAP と HA メディエーターの IAM ロールを選択できます。

ステップ3: AWS KMSを設定する

Cloud Volumes ONTAP で Amazon 暗号化を使用する場合は、AWS Key Management Service (KMS) の要件が満たされていることを確認してください。

手順

1. 自分のアカウントまたは別の AWS アカウントにアクティブなカスタマーマスターキー (CMK) が存在することを確認します。

CMK は、AWS 管理の CMK またはカスタマー管理の CMK にすることができます。

2. CMK が、Cloud Volumes ONTAP をデプロイする予定のアカウントとは別の AWS アカウントにある場合は、そのキーの ARN を取得する必要があります。

Cloud Volumes ONTAPシステムを作成するときは、コンソールに ARN を提供する必要があります。

3. インスタンスの IAM ロールを CMK のキーユーザーのリストに追加します。

これにより、コンソールにCloud Volumes ONTAPで CMK を使用する権限が付与されます。

ステップ4: コンソールエージェントをインストールしてコンソールを設定する

コンソールを使用して AWS にCloud Volumes ONTAPをデプロイする前に、コンソール エージェントをインストールしてセットアップする必要があります。これにより、コンソールはパブリック クラウド環境 (Cloud Volumes ONTAPを含む) 内のリソースとプロセスを管理できるようになります。

手順

1. Privacy Enhanced Mail (PEM) Base-64 エンコード X.509 形式で証明機関 (CA) によって署名されたルート証明書を取得します。証明書を取得するための組織のポリシーと手順を参照してください。



AWS Secret Cloudリージョンの場合は、`NSS Root CA 2`証明書、そしてTop Secret Cloudの場合は、`Amazon Root CA 4`証明書。チェーン全体ではなく、これらの証明書のみをアップロードするようにしてください。証明書チェーンのファイルは大きいため、アップロードが失敗する可能性があります。追加の証明書がある場合は、次の手順で説明するように後でアップロードできます。

セットアッププロセス中に証明書をアップロードする必要があります。コンソールは、HTTPS 経由で AWS にリクエストを送信するときに、信頼された証明書を使用します。

2. コンソール エージェントのインスタンスを起動します。
 - a. コンソールの AWS Intelligence Community Marketplace ページに移動します。
 - b. [カスタム起動] タブで、EC2 コンソールからインスタンスを起動するオプションを選択します。
 - c. 指示に従ってインスタンスを構成します。

インスタンスを構成する際には、次の点に注意してください。

- t3.xlarge をお勧めします。
- 権限を設定するときに作成した IAM ロールを選択する必要があります。
- デフォルトのストレージ オプションを維持する必要があります。
- コンソール エージェントに必要な接続方法は、SSH、HTTP、および HTTPS です。

3. インスタンスに接続しているホストからコンソールを設定します。
 - a. ウェブブラウザを開いて入力してください `<a href="https://<em>ipaddress</em>" class="bare">https://<em>ipaddress</em></a>` ここで、ipaddress は、コンソール エージェントをインストールした Linux ホストの IP アドレスです。
 - b. AWS サービスへの接続用のプロキシサーバーを指定します。
 - c. 手順 1 で取得した証明書をアップロードします。
 - d. 指示に従って新しいシステムをセットアップします。
 - システムの詳細: コンソール エージェントの名前と会社名を入力します。

- 管理者ユーザーの作成: システムの管理者ユーザーを作成します。

このユーザー アカウントはシステム上でローカルに実行されます。コンソール経由で利用できる auth0 サービスへの接続がありません。

- 確認: 詳細を確認し、ライセンス契約に同意して、[セットアップ] を選択します。

- e. CA 署名証明書のインストールを完了するには、EC2 コンソールからコンソールエージェントインスタンスを再起動します。

4. コンソール エージェントが再起動したら、セットアップ ウィザードで作成した管理者ユーザー アカウントを使用してログインします。

ステップ5: (オプション) プライベートモード証明書をインストールする

この手順は、AWS Secret Cloud および Top Secret Cloud リージョンではオプションであり、前の手順でインストールしたルート証明書とは別に追加の証明書がある場合にのみ必要です。

手順

1. 既存のインストールされている証明書を一覧表示します。

- a. occm コンテナの docker ID (識別名「ds-occm-1」) を収集するには、次のコマンドを実行します。

```
docker ps
```

- b. occm コンテナ内に入るには、次のコマンドを実行します。

```
docker exec -it <docker-id> /bin/sh
```

- c. 「TRUST_STORE_PASSWORD」環境変数からパスワードを収集するには、次のコマンドを実行します。

```
env
```

- d. トラストストアにインストールされているすべての証明書を一覧表示するには、次のコマンドを実行し、前の手順で収集したパスワードを使用します。

```
keytool -list -v -keystore occm.truststore
```

2. 証明書を追加します。

- a. occm コンテナの docker ID (識別名「ds-occm-1」) を収集するには、次のコマンドを実行します。

```
docker ps
```

- b. occm コンテナ内に入るには、次のコマンドを実行します。

```
docker exec -it <docker-id> /bin/sh
```

新しい証明書ファイルを内部に保存します。

- c. 「TRUST_STORE_PASSWORD」環境変数からパスワードを収集するには、次のコマンドを実行します。

```
env
```

- d. 証明書をトラストストアに追加するには、次のコマンドを実行し、前の手順のパスワードを使用します。

```
keytool -import -alias <alias-name> -file <certificate-file-name>  
-keystore occm.truststore
```

- e. 証明書がインストールされていることを確認するには、次のコマンドを実行します。

```
keytool -list -v -keystore occm.truststore -alias <alias-name>
```

- f. occm コンテナを終了するには、次のコマンドを実行します。

```
exit
```

- g. occm コンテナをリセットするには、次のコマンドを実行します。

```
docker restart <docker-id>
```

ステップ6: コンソールにライセンスを追加する

NetAppからライセンスを購入した場合は、新しいCloud Volumes ONTAPシステムを作成するときにライセンスを選択できるように、コンソールに追加する必要があります。これらのライセンスは、新しいCloud Volumes ONTAPシステムに関連付けるまで未割り当てのままになります。

手順

1. 左側のナビゲーションメニューから、[ライセンスとサブスクリプション]を選択します。
2. * Cloud Volumes ONTAP*パネルで、*表示*を選択します。
3. * Cloud Volumes ONTAP*タブで、*ライセンス>ノードベースのライセンス*を選択します。
4. *未割り当て*をクリックします。
5. *未割り当てのライセンスの追加*をクリックします。

6. ライセンスのシリアル番号を入力するか、ライセンス ファイルをアップロードします。
7. ライセンス ファイルがまだない場合は、netapp.com からライセンス ファイルを手動でアップロードする必要があります。
 - a. に行く ["NetApp License File Generator"](#) NetApp サポート サイトの認証情報を使用してログインします。
 - b. パスワードを入力し、製品を選択し、シリアル番号を入力し、プライバシー ポリシーを読んで同意したことを確認してから、[送信] をクリックします。
 - c. serialnumber.NLF JSON ファイルを電子メールで受け取るか、直接ダウンロードするかを選択します。
8. *ライセンスの追加* をクリックします。

結果

コンソールは、新しい Cloud Volumes ONTAP システムに関連付けるまで、ライセンスを未割り当てとして追加します。ライセンスは、左側のナビゲーション メニューの **[ライセンスとサブスクリプション] > [Cloud Volumes ONTAP] > [表示] > [ライセンス]** で確認できます。

ステップ7: コンソールから Cloud Volumes ONTAP を起動する

コンソールで新しいシステムを作成することにより、AWS Secret Cloud および Top Secret Cloud で Cloud Volumes ONTAP インスタンスを起動できます。

開始する前に

HA ペアの場合、HA メディエーターへのキーベースの SSH 認証を有効にするにはキー ペアが必要です。

手順

1. *システム* ページで、*システムの追加* をクリックします。
2. *作成* で、Cloud Volumes ONTAP を選択します。

HA の場合: 作成 で、Cloud Volumes ONTAP または Cloud Volumes ONTAP HA を選択します。

3. ウィザードの手順を完了して、Cloud Volumes ONTAP システムを起動します。



ウィザードで選択を行う際は、[サービス] の [データ センス & コンプライアンス] と [クラウドへのバックアップ*] を選択しないでください。*事前構成パッケージ*の下で、*構成の変更*のみを選択し、他のオプションを選択していないことを確認します。事前設定されたパッケージは AWS Secret Cloud および Top Secret Cloud リージョンではサポートされていないため、選択した場合、デプロイは失敗します。

Cloud Volumes ONTAP HA を複数のアベイラビリティゾーンに導入する場合の注意事項

HA ペアのウィザードを完了する際には、次の点に注意してください。

- Cloud Volumes ONTAP HA を複数のアベイラビリティゾーン (AZ) にデプロイする場合は、トランジットゲートウェイを構成する必要があります。手順については、["AWS トランジットゲートウェイを設定する"](#)。
- 公開時点では AWS Top Secret Cloud で利用できる AZ は 2 つだけだったので、次のように構成を展開します。

- ノード1: アベイラビリティゾーンA
- ノード2: アベイラビリティゾーンB
- メディエーター: アベイラビリティゾーン A または B

Cloud Volumes ONTAPを単一ノードとHAノードの両方に導入する場合の注意事項

ウィザードを完了する際には、次の点に注意してください。

- 生成されたセキュリティ グループを使用するには、デフォルト オプションのままにしておく必要があります。

事前定義されたセキュリティ グループには、Cloud Volumes ONTAP が正常に動作するために必要なルールが含まれています。独自のセキュリティ グループを使用する必要がある場合は、以下のセキュリティ グループのセクションを参照してください。

- AWS 環境を準備するときに作成した IAM ロールを選択する必要があります。
- 基盤となる AWS ディスクタイプは、初期のCloud Volumes ONTAP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す。

- AWS ディスクのパフォーマンスはディスクサイズに左右されます。

必要な持続的なパフォーマンスを実現するディスク サイズを選択する必要があります。EBS パフォーマンスの詳細については、AWS のドキュメントを参照してください。

- ディスク サイズは、システム上のすべてのディスクのデフォルト サイズです。



後で異なるサイズが必要になった場合は、詳細割り当てオプションを使用して、特定のサイズのディスクを使用するアグリゲートを作成できます。

結果

Cloud Volumes ONTAPインスタンスが起動します。*監査*ページで進捗状況を追跡できます。

ステップ8: データ階層化のためのセキュリティ証明書をインストールする

AWS Secret Cloud および Top Secret Cloud リージョンでデータ階層化を有効にするには、セキュリティ証明書を手動でインストールする必要があります。

開始する前に

1. S3 バケットを作成します。



バケット名に接頭辞が付いていることを確認してください fabric-pool-。`例えば` fabric-pool-testbucket。

2. インストールしたルート証明書を保管してください`step 4`ハンディ。

手順

1. インストールしたルート証明書からテキストをコピーします。 step 4。

2. CLI を使用してCloud Volumes ONTAPシステムに安全に接続します。
3. ルート証明書をインストールします。押す必要があるかもしれませんが `ENTER` キーを複数回押す:

```
security certificate install -type server-ca -cert-name <certificate-name>
```

4. プロンプトが表示されたら、コピーしたテキスト全体（およびを含む）を入力します。----- BEGIN CERTIFICATE -----`に `----- END CERTIFICATE -----。
5. 将来の参照用に、CA 署名付きデジタル証明書のコピーを保管してください。
6. CA 名と証明書のシリアル番号を保持します。
7. AWS Secret Cloud および Top Secret Cloud リージョンのオブジェクト ストアを構成します。set -privilege advanced -confirmations off
8. このコマンドを実行してオブジェクト ストアを構成します。



すべてのAmazonリソース名（ARN）には、-iso-b、のような arn:aws-iso-b。たとえば、リソースにリージョン付きのARNが必要な場合は、Top Secret Cloudでは次のような命名規則を使用します。us-iso-b`のために `server` フラグ。AWS Secret Cloud の場合は、`us-iso-b-1。

```
storage aggregate object-store config create -object-store-name  
<S3Bucket> -provider-type AWS_S3 -auth-type EC2-IAM -server <s3.us-iso-  
b-1.server_name> -container-name <fabric-pool-testbucket> -is-ssl  
-enabled true -port 443
```

9. オブジェクト ストアが正常に作成されたことを確認します。storage aggregate object-store show -instance
10. オブジェクト ストアをアグリゲートに接続します。これを新しい集計ごとに繰り返す必要があります。storage aggregate object-store attach -aggregate <aggr1> -object-store-name <S3Bucket>

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コンソールに依存しています。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コンソール
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"
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コンソールから利用可能
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コンソールのドキュメント"](#)

NetAppコンソールで始める

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コンソール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"](#)。

4

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コンソールは、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コンソールは、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。セキュリティ要件が厳しい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

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://vault.azure.net	キーボールド	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.net/app.com/aods/asupmessage https://mysupport.net/app.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://blueexpinfraproduct.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。
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。

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.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コンソールエージェントのネットワークプロキシ構成

NetAppコンソール 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 システムを展開するか、HA ペアを展開するかによって異なります。LIF は物理ポートに関連付けられた IP アドレスです。SnapCenterなどの管理ツールには、SVM 管理 LIF が必要です。



iSCSI LIF は、iSCSI プロトコルを介したクライアント アクセスを提供し、システム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

コンソールは、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。

コンソールは 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) がフェールオーバー 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"](#)。

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レプリケートするには、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

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
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
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、「AllowAzureLoadBalancerInBound」ルールに示されているように、ロード バランサーからのトラフィックは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コンソールから、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. ["キーコンテナーにキーを生成する"](#)。

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 コンテナー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コンソール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、マーケットプレイ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

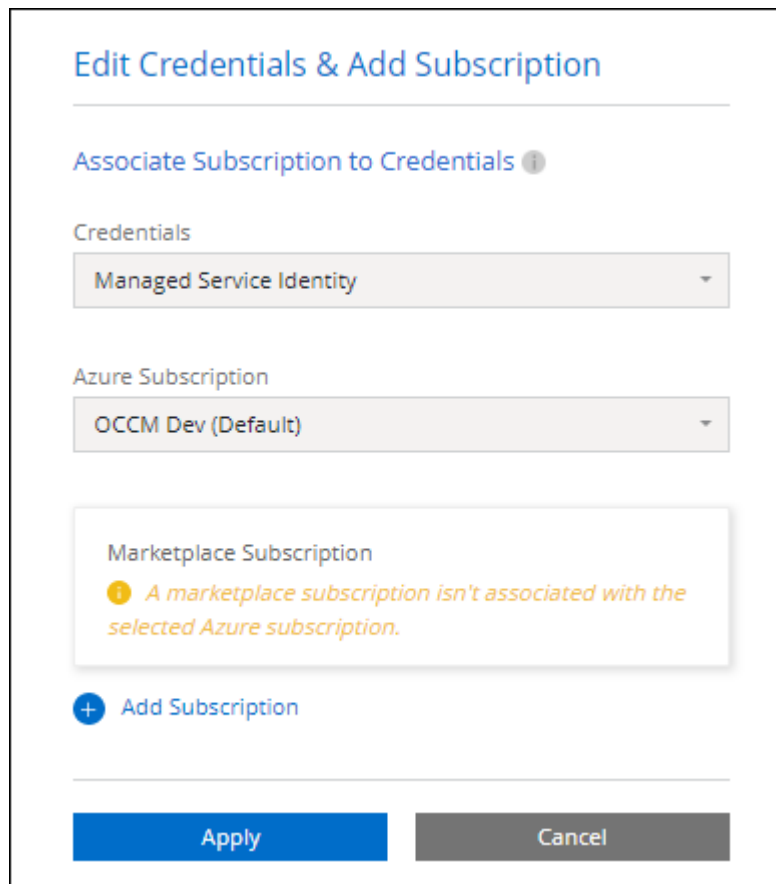
1. ["ライセンスを取得するには、NetApp の営業担当者にお問い合わせください。"](#)
2. ["NetAppサポートサイトのアカウントをコンソールに追加します"](#)

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できる必要があります。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 からサブスクライ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、[サブスクライブ] 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 v

☐ 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"](#)。

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

計画外のフェイルオーバー時間を短縮し、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。このモードでは、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。

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、NetAppコンソールではこれらの詳細が求められます。

次の点に注意してください。

- Cloud Volumes ONTAP HA ペアの高可用性に問題はありません。この Azure 機能はONTAPと連携して動作し、計画外のフェイルオーバー 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。

「所有者」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。

手順

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/fe
atures/EnableHighAvailabilityMode",
  "name": "Microsoft.Network/EnableHighAvailabilityMode",
  "properties": {
    "state": "Registered"
  },
  "type": "Microsoft.Features/providers/features"
}
```

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

NetAppコンソールでCloud Volumes ONTAPシステムを作成することにより、Azure で単一ノード システムまたは HA ペアを起動できます。

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。

フィールド	説明
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データ分類の詳細](#)"
- "[NetAppバックアップとリカバリの詳細](#)"



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を、Cloud Volumes ONTAPの新しいパッチおよびリリースにアップグレードできます。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。

フィールド	説明
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、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。

12. **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、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は、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の見方については、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、["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。

フィールド	説明
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: ABDcv5689

Storage VM (SVM): svm_c...CVO1

Volume Size: 100

Unit: GiB

Snapshot Policy: default

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。

フィールド	説明
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コンソール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。
- 構成の詳細を確認します。
 - 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。
 - 理解しました... チェックボックスを選択します。
 - [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。

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。
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データ分類の詳細"](#)
 - ["NetAppバックアップとリカバリの詳細"](#)



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は、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、["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。

フィールド	説明
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 displays the 'Volume Details & Protection' configuration interface. It includes the following fields and values:

- Volume Name:** ABDcv5689
- Storage VM (SVM):** svm_c...CVO1
- Volume Size:** 100
- Unit:** GiB
- Snapshot Policy:** default

Information icons (i) are present next to the Volume Name, Volume Size, and Snapshot Policy fields.

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。

フィールド	説明
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コンソール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。
- 構成の詳細を確認します。
 - 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。
 - 理解しました... チェックボックスを選択します。
 - [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。

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別な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

- ["ページフォールトブログ: 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
...
```

- 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を使用する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	<code>ontap_cloud_direct_gen2</code>
9.17.1以降	NetAppコンソール	<code>ontap_cloud_gen2</code>
9.16.1	Azureマーケットプレイス	<code>ontap_cloud_direct</code>
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	<code>ontap_cloud_byol</code>
9.15.0	コンソール、高可用性 (HA) 展開	<code>ontap_cloud_byol_ha</code>

- 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

- 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-
xxxxxx.blueexpinfraprod.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
```

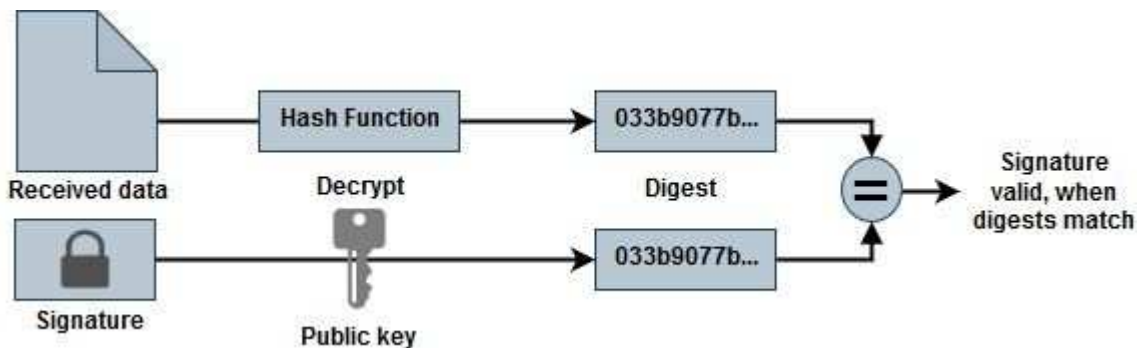
ファイルの署名を検証する

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イメージをダウンロードするには ["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 分かかる場合がある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 コンソール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 コンソールで検出されたときに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るのに役立ちます。
 - 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。

展開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"](#)。

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"](#)

Google Cloud を使い始める

Google Cloud でのCloud Volumes ONTAPのクイック スタート

数ステップで Google Cloud のCloud Volumes ONTAP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。 ["Google Cloud 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コンソール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。

["構成の計画について詳しくは"](#)。

3

ネットワークを設定する

1. VPC 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していることを確認します。
2. データ階層化を有効にする場合は、 ["プライベート Google アクセス用にCloud Volumes ONTAPサブネットを構成する"](#)。
3. HA ペアをデプロイする場合は、それぞれ独自のサブネットを持つ 4 つの VPC があることを確認してく

ださい。

4. 共有 VPC を使用している場合は、コンソール エージェント サービス アカウントに *Compute Network User* ロールを付与します。
5. 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"](#)。

4

サービスアカウントを設定する

Cloud Volumes ONTAP、2 つの目的で Google Cloud サービス アカウントが必要です。1つ目は、["データ階層化"](#)コールドデータを Google Cloud の低コストのオブジェクト ストレージに階層化します。2つ目は、["NetAppバックアップとリカバリ"](#)ボリュームを低コストのオブジェクト ストレージにバックアップします。

1 つのサービス アカウントを設定して、両方の目的に使用できます。サービス アカウントには **Storage Admin** ロールが必要です。

["ステップバイステップの説明を読む"](#)。

5

Google Cloud API を有効にする

["プロジェクトで次の Google Cloud API を有効にします"](#)。これらの API は、コンソール エージェントとCloud Volumes ONTAP をデプロイするために必要です。

- クラウド デプロイメント マネージャー V2 API
- クラウドロギングAPI
- クラウド リソース マネージャー API
- コンピューティングエンジン API
- アイデンティティとアクセス管理 (IAM) API

6

コンソールを使用して**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

- ["コンソールエージェントの作成"](#)
- ["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 Google Cloud の権限で実行する処理"](#)

Google Cloud でCloud Volumes ONTAP構成を計画する

Google Cloud 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か、独自の構成を作成することができます。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 Google Cloud 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マシン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、いくつかのマシン タイプをサポートします。

["GCP でサポートされている 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。

["GCP の Cloud Volumes ONTAP のストレージ制限"](#)

GCP でシステムのサイズを決める

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。マシン タイプ、ディスク タイプ、ディスク サイズを選択するときは、いくつかの重要なポイントに注意する必要があります。

機械の種類

サポートされているマシンタイプについては、["Cloud Volumes ONTAP リリースノート"](#)次に、サポートされている各マシンタイプに関する Google の詳細を確認します。ワークロード要件を、マシンタイプの vCPU とメモリの数に合わせてください。各 CPU コアによってネットワーク パフォーマンスが向上することに注意してください。

詳細については、以下を参照してください。

- ["Google Cloud ドキュメント: N1 標準マシンタイプ"](#)
- ["Google Cloud ドキュメント: パフォーマンス"](#)

GCP のディスク タイプ

Cloud Volumes ONTAP のボリュームを作成するときは、Cloud Volumes ONTAP がディスクに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。ディスク タイプは次のいずれかになります。

- ゾーン SSD 永続ディスク: SSD 永続ディスクは、高レートのランダム IOPS を必要とするワークロードに最適です。
- ゾーンバランス永続ディスク: これらの SSD は、GB あたりの IOPS を低くすることで、パフォーマンスとコストのバランスをとります。
- ゾーン標準永続ディスク: 標準永続ディスクは経済的で、順次読み取り/書き込み操作を処理できます。

詳細については、"[Google Cloud ドキュメント: ゾーン永続ディスク（標準および SSD）](#)"。

GCP ディスクサイズ

Cloud Volumes ONTAPシステムをデプロイするときは、初期ディスク サイズを選択する必要があります。その後は、NetAppコンソールでシステムの容量を管理できるようになりますが、アグリゲートを自分で構築する場合は、次の点に注意してください。

- 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。
- パフォーマンスを考慮しながら、必要なスペースを決定します。
- 永続ディスクのパフォーマンスは、ディスク サイズとシステムで使用可能な vCPU の数に応じて自動的に調整されます。

詳細については、以下を参照してください。

- "[Google Cloud ドキュメント: ゾーン永続ディスク（標準および SSD）](#)"
- "[Google Cloud ドキュメント: 永続ディスクとローカル SSD のパフォーマンスの最適化](#)"

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。

- "[Google Cloud 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](#)"。
- "[Google Cloud ドキュメント: リソース割り当て](#)"

Google Cloud Compute Engine はリソース使用量に割り当て制限を適用するため、Cloud Volumes ONTAP をデプロイする前に制限に達していないことを確認する必要があります。



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

GCP 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。

単一ノードシステムのネットワーク情報

GCPの情報	あなたの価値
リージョン	

GCPの情報	あなたの価値
ゾーン	
VPCネットワーク	
サブネット	
ファイアウォール ポリシー（ 独自のものを使用している場合）	

複数のゾーンにあるHAペアのネットワーク情報

GCPの情報	あなたの価値
リージョン	
ノード1のゾーン	
ノード2のゾーン	
調停者のためのゾーン	
VPC-0とサブネット	
VPC-1とサブネット	
VPC-2とサブネット	
VPC-3とサブネット	
ファイアウォール ポリシー（ 独自のものを使用している場合）	

単一ゾーン内のHAペアのネットワーク情報

GCPの情報	あなたの価値
リージョン	
ゾーン	
VPC-0とサブネット	
VPC-1とサブネット	
VPC-2とサブネット	
VPC-3とサブネット	
ファイアウォール ポリシー（ 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

コンソールを使用すると、Google Cloud の高可用性（HA）ペアを除き、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"](#)

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用に Google Cloud ネットワークを設定する

NetAppコンソールは、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。

HAペアを導入する場合は、"[Google Cloud での HA ペアの仕組みを学ぶ](#)"。

Cloud Volumes ONTAPの要件

Google Cloud では次の要件を満たす必要があります。

単一ノードシステムに固有の要件

単一ノード システムを展開する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つのVPC

単一ノード システムには 1 つの仮想プライベート クラウド (VPC) が必要です。

プライベートIPアドレス

Google Cloud の単一ノード システムの場合、コンソールは次のものにプライベート IP アドレスを割り当てます。

- ノード
- クラスタ
- Storage VM
- データNAS LIF
- データ iSCSI LIF

API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```



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、ストレージ VM (SVM) 管理 LIF が必要です。

HAペア固有の要件

HA ペアを展開する場合は、ネットワークが次の要件を満たしていることを確認してください。

1つまたは複数のゾーン

複数のゾーンまたは単一のゾーンに HA 構成を展開することで、データの高可用性を確保できます。HA ペアを作成するときに、コンソールで複数のゾーンまたは単一のゾーンを選択するように求められます。

- 複数のゾーン（推奨）

3 つのゾーンにわたって HA 構成を展開すると、ゾーン内で障害が発生した場合でも継続的なデータ可用性が確保されます。書き込みパフォーマンスは単一ゾーンを使用する場合と比べてわずかに低下しますが、最小限であることに注意してください。

- 単一ゾーン

単一のゾーンにデプロイされる場合、Cloud Volumes ONTAP HA 構成では、スプレッド配置ポリシーが使用されます。このポリシーにより、障害の分離を実現するために個別のゾーンを使用する必要がなく、ゾーン内の単一障害点から HA 構成が保護されます。

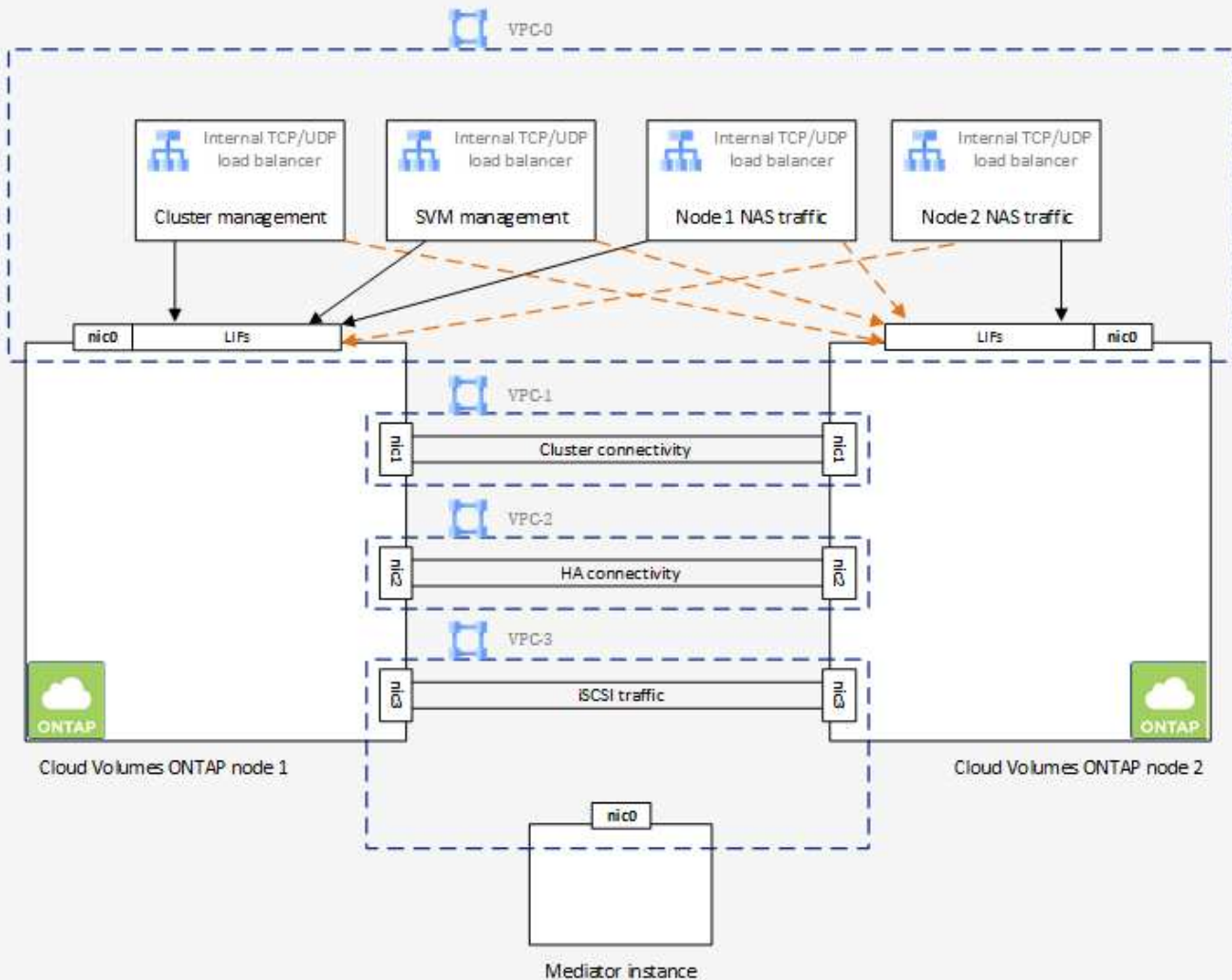
このデプロイメント モデルでは、ゾーン間のデータ送信料金が発生しないため、コストが削減されます。

4つの仮想プライベートクラウド

HA 構成には 4 つの仮想プライベート クラウド (VPC) が必要です。Google Cloud では各ネットワーク インターフェイスが個別の VPC ネットワークに存在する必要があるため、4 つの VPC が必要です。

HA ペアを作成するときに、コンソールで 4 つの VPC を選択するように求められます。

- データとノードへのインバウンド接続用の VPC-0
- ノードと HA メディエーター間の内部通信用の VPC-1、VPC-2、および VPC-3



サブネット

各 VPC にはプライベート サブネットが必要です。

コンソール エージェントを VPC-0 に配置する場合は、API にアクセスしてデータ階層化を有効にするために、サブネットでプライベート Google アクセスを有効にする必要があります。

これらの VPC 内のサブネットには、異なる CIDR 範囲が必要です。重複する CIDR 範囲を持つことはできません。

プライベート IP アドレス

コンソールは、Google Cloud 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 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 システムを展開するか、HA ペアを展開するかによって異なります。LIF は物理ポートに関連付けられた IP アドレスです。SnapCenter などの管理ツールには、SVM 管理 LIF が必要です。

- 単一ノード コンソールは単一ノード システムに 4 つの IP アドレスを割り当てます。

- ノード管理LIF
- クラスタ管理LIF
- iSCSI データ LIF



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。

- NAS LIF

API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```

- HA ペア コンソールは HA ペアに 12 ～ 13 個の IP アドレスを割り当てます。

- 2つのノード管理LIF (e0a)
- 1 クラスタ管理LIF (e0a)
- 2 つの iSCSI LIF (e0a)



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。

- 1 個または 2 個の NAS LIF (e0a)
- 2 つのクラスタ LIF (e0b)
- 2 つの HA 相互接続 IP アドレス (e0c)
- 2つのRSM iSCSI IPアドレス (e0d)

API を使用してCloud Volumes ONTAPをデプロイし、次のフラグを指定すると、ストレージ VM (SVM) 管理 LIF の作成をスキップできます。

```
skipSvmManagementLif: true
```

内部ロードバランサ

コンソールは、Cloud Volumes ONTAP HA ペアへの受信トラフィックを管理する 4 つの Google Cloud 内部ロードバランサ (TCP/UDP) を作成します。お客様側での設定は必要ありません。これを要件としてリストしたのは、ネットワーク トラフィックを通知し、セキュリティ上の懸念を軽減するためだけです。

1 つのロード バランサはクラスタ管理用、1 つはストレージ VM (SVM) 管理用、1 つはノード 1 への NAS トラフィック用、最後の 1 つはノード 2 への NAS トラフィック用です。

各ロードバランサーの設定は次のとおりです。

- 1つの共有プライベートIPアドレス
- グローバルな健康診断

デフォルトでは、ヘルスチェックで使用されるポートは 63001、63002、および 63003 です。

- 1つの地域TCPバックエンドサービス
- 1つの地域UDPバックエンドサービス
- 1つのTCP転送ルール
- 1つのUDP転送ルール
- グローバルアクセスが無効になっています

グローバル アクセスはデフォルトで無効になっていますが、デプロイ後に有効にすることはサポートされています。リージョン間のトラフィックのレイテンシが大幅に増加するため、これを無効にしました。誤ってリージョンをまたいでマウントすることによって、ネガティブな体験をすることがないようにしたいと考えました。このオプションを有効にするかどうかは、ビジネス ニーズによって異なります。

共有VPC

Cloud Volumes ONTAPとコンソール エージェントは、Google Cloud 共有 VPC とスタンドアロン VPC でもサポートされています。

単一ノード システムの場合、VPC は共有 VPC またはスタンドアロン VPC のいずれかになります。

HA ペアの場合、4 つの VPC が必要です。これらの各 VPC は、共有またはスタンドアロンのいずれかになります。たとえば、VPC-0 は共有 VPC であり、VPC-1、VPC-2、VPC-3 はスタンドアロン VPC である可能性があります。

共有 VPC を使用すると、複数のプロジェクトにわたって仮想ネットワークを構成し、一元管理できます。ホスト プロジェクト で共有 VPC ネットワークを設定し、サービス プロジェクト でコンソール エージェントとCloud Volumes ONTAP仮想マシン インスタンスをデプロイできます。

["Google Cloud ドキュメント: 共有 VPC の概要"](#)。

["コンソール エージェントのデプロイで説明されている必要な共有 VPC 権限を確認します。"](#)

VPC でのパケットミラーリング

["パケットミラーリング"](#)Cloud Volumes ONTAPをデプロイする Google Cloud サブネットが無効に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

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。セキュリティ要件が厳しい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	エンドポイントが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://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。

エンドポイント	適用対象	目的	展開モード	エンドポイントが利用できない場合の影響
https://www.googleapis.com/compute/v1/projects/ https://cloudresource-manager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deployment-manager/v2/projects https://compute.googleapis.com/compute/v1	Google Cloud（商用利用）。	Google Cloud 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、Google Cloud サービスと通信して、Google Cloud のコンソールの特定の操作を実行できません。

他のネットワーク内の**ONTAP**システムへの接続

Google Cloud 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、VPC 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。

["Google Cloud ドキュメント: Cloud VPN の概要"](#)。

ファイアウォールルール

コンソールは、Cloud Volumes ONTAP が正常に動作するために必要な受信ルールと送信ルールを含む Google Cloud ファイアウォール ルールを作成します。テスト目的の場合、または独自のファイアウォール ルールを使用する場合は、ポートを参照することをお勧めします。

Cloud Volumes ONTAPのファイアウォール ルールには、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。 HA 構成を展開する場合、これらは VPC-0 のCloud Volumes ONTAPのファイアウォール ルールです。

HA 構成には 2 セットのファイアウォール ルールが必要であることに注意してください。

- VPC-0 の HA コンポーネントに対する 1 セットのルール。これらのルールにより、Cloud Volumes ONTAPへのデータ アクセスが可能になります。
- VPC-1、VPC-2、VPC-3 の HA コンポーネントに対する別のルール セット。これらのルールは、HA コンポーネント間の受信および送信通信に対して有効です。 [詳細情報](#)。



コンソール エージェントに関する情報をお探しですか? ["コンソールエージェントのファイアウォールルールを表示する"](#)

インバウンドルール

Cloud Volumes ONTAPシステムを追加する場合、展開時に事前定義されたファイアウォール ポリシーのソース フィルターを選択できます。

- 選択した **VPC** のみ: 受信トラフィックのソース フィルターは、Cloud Volumes ONTAPシステムの VPC 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 VPC 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 **VPC**: 受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲です。

独自のファイアウォール ポリシーを使用する場合は、Cloud Volumes ONTAPと通信する必要があるすべてのネットワークを追加するだけでなく、内部 Google ロードバランサが正しく機能できるように両方のアドレス範囲も追加してください。これらのアドレスは 130.211.0.0/22 と 35.191.0.0/16 です。詳細については、["Google Cloud ドキュメント: ロードバランサのファイアウォール ルール"](#)。

プロトコル	ポート	目的
すべてのICMP	全て	インスタンスにpingを実行する
HTTP	80	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
HTTPS	443	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
SSH	22	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
TCP	111	NFS のリモート プロシージャ コール
TCP	139	CIFSのNetBIOSサービスセッション
TCP	161-162	簡易ネットワーク管理プロトコル
TCP	445	NetBIOS フレームを使用した TCP 経由の Microsoft SMB/CIFS
TCP	635	NFSマウント
TCP	749	Kerberos
TCP	2049	NFSサーバ デーモン
TCP	3260	iSCSI データ LIF を介した iSCSI アクセス
TCP	4045	NFSロック デーモン
TCP	4046	NFS のネットワーク ステータス モニター
TCP	10000	NDMPを使用したバックアップ
TCP	11104	SnapMirrorのクラスタ間通信セッションの管理
TCP	11105	クラスタ間LIFを使用したSnapMirrorデータ転送
TCP	63001-63050	どのノードが正常であるかを判断するためにプローブ ポートをロード バランシングします (HA ペアの場合のみ必要)

プロトコル	ポート	目的
UDP	111	NFS のリモート プロシージャ コール
UDP	161-162	簡易ネットワーク管理プロトコル
UDP	635	NFSマウント
UDP	2049	NFSサーバ デーモン
UDP	4045	NFSロック デーモン
UDP	4046	NFS のネットワーク ステータス モニター
UDP	4049	NFS rquotadプロトコル

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。

プロトコル	ポート	目的
すべてのICMP	全て	すべての送信トラフィック
すべてTCP	全て	すべての送信トラフィック
すべてUDP	全て	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。Cloud Volumes ONTAPクラスターは、ノード トラフィックを制御するために次のポートを使用します。



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

サービス	プロトコル	ポート	ソース	デスティネーション	目的
Active Directory	TCP	88	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
	UDP	137	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
	UDP	138	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
	TCP	139	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
	TCP とUDP	389	ノード管理LIF	アクティブディレクトリフォレスト	LDAP
	TCP	445	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
	TCP	464	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)
	UDP	464	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
	TCP	749	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)
	TCP	88	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
	UDP	137	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
	UDP	138	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
	TCP	139	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
	TCP とUDP	389	データ LIF (NFS、CIFS)	アクティブディレクトリフォレスト	LDAP
	TCP	445	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
	TCP	464	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)
	UDP	464	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
	TCP	749	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	プロトコル	ポート	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	UDP	68	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	UDP	67	ノード管理LIF	DHCP	DHCP サーバ
DNS	UDP	53	ノード管理LIFとデータLIF（NFS、CIFS）	DNS	DNS
NDMP	TCP	18600～18699	ノード管理LIF	宛先サーバー	NDMPコピー
SMTP	TCP	25	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	TCP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	161	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	TCP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
	UDP	162	ノード管理LIF	監視サーバー	SNMPトラップによる監視
SnapMirror	TCP	11104	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
	TCP	11105	クラスタ間LIF	ONTAPクラスタ間LIF	SnapMirrorデータ転送
syslog	UDP	514	ノード管理LIF	syslogサーバ	Syslog転送メッセージ

VPC-1、VPC-2、VPC-3のルール

Google Cloud では、HA 構成が 4 つの VPC にデプロイされます。VPC-0のHA構成に必要なファイアウォールルールは[Cloud Volumes ONTAPについては上記に記載されています](#)。

一方、VPC-1、VPC-2、VPC-3 のインスタンスに作成された定義済みのファイアウォール ルールにより、すべてのプロトコルとポートを介した受信通信が可能になります。これらのルールにより、HA ノード間の通信が可能になります。

HA ノードから HA メディエーターへの通信は、ポート 3260 (iSCSI) を介して行われます。



新しい Google Cloud HA ペアのデプロイメントで高速書き込みを有効にするには、VPC-1、VPC-2、VPC-3 に少なくとも 8,896 バイトの最大転送単位 (MTU) が必要です。既存の VPC-1、VPC-2、および VPC-3 を 8,896 バイトの MTU にアップグレードすることを選択した場合は、設定プロセス中にこれらの VPC を使用している既存の HA システムをすべてシャットダウンする必要があります。

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、ネットワーク要件を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"](#)
- ["Google Cloud のファイアウォール ルール"](#)

コンソールエージェントプロキシをサポートするためのネットワーク構成

コンソール エージェント用に設定されたプロキシ サーバーを使用して、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。コンソール エージェント管理者は、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 プロキシ経由で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、コンソール エージェント管理者は、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。

コンソールエージェントのプロキシサーバーの構成については、["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"](#)。

Google Cloud でCloud Volumes ONTAPのネットワーク タグを構成する

コンソール エージェントの透過プロキシ構成中に、管理者は Google Cloud のネットワーク タグを追加します。Cloud Volumes ONTAP構成に同じネットワーク タグを取得して手動で追加する必要があります。このタグは、プロキシ サーバーが正しく機能するために必要です。

1. Google Cloud コンソールで、Cloud Volumes ONTAPシステムを見つけます。
2. 詳細 > ネットワーク > ネットワーク タグ に移動します。
3. コンソール エージェントに使用するタグを追加し、構成を保存します。

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"](#)。

VPC Service Controls を設定して、**Google Cloud** に**Cloud Volumes ONTAP** をデプロイする

VPC Service Controls を使用して Google Cloud 環境をロックダウンする場合は、NetApp Console と Cloud Volumes ONTAP が Google Cloud API とどのようにやり取りするか、また Console と Cloud Volumes ONTAP をデプロイするためにサービス境界をどのように構成するかを理解する必要があります。

VPC Service Controls を使用すると、信頼できる境界外にある Google マネージド サービスへのアクセスを制御し、信頼できない場所からのデータアクセスをブロックし、不正なデータ転送のリスクを軽減できます。["Google Cloud VPC Service Controls の詳細"](#)。

NetAppサービスが **VPC Service Controls** と通信する方法

コンソールは Google Cloud API と直接通信します。これは、Google Cloud 外部の外部 IP アドレス (api.services.cloud.netapp.com など) からトリガーされるか、Google Cloud 内でコンソール エージェントに割り当てられた内部アドレスからトリガーされます。

コンソール エージェントの展開スタイルによっては、サービス境界に特定の例外を設ける必要がある場合があります。

イメージ

Cloud Volumes ONTAPとコンソールはどちらも、NetAppによって管理されている GCP 内のプロジェクトのイメージを使用します。組織内でホストされていないイメージの使用をブロックするポリシーが組織にある場合、これはコンソールエージェントとCloud Volumes ONTAPの展開に影響する可能性があります。

手動インストール方法を使用してコンソール エージェントを手動で展開できますが、Cloud Volumes ONTAPNetAppプロジェクトからイメージをプルする必要もあります。コンソール エージェントとCloud Volumes ONTAPをデプロイするには、許可リストを提供する必要があります。

コンソールエージェントの展開

コンソール エージェントを展開するユーザーは、プロジェクト ID *netapp-cloudmanager* およびプロジェクト番号 14190056516 でホストされているイメージを参照する必要があります。

Cloud Volumes ONTAPの導入

- コンソール サービス アカウントは、サービス プロジェクトのプロジェクト ID *netapp-cloudmanager* とプロジェクト番号 14190056516 でホストされているイメージを参照する必要があります。
- デフォルトの Google API サービス エージェントのサービス アカウントは、サービス プロジェクトのプロジェクト ID *netapp-cloudmanager* とプロジェクト番号 14190056516 でホストされているイメージを参照する必要があります。

VPC Service Controls を使用してこれらのイメージをプルするために必要なルールの例を以下に定義します。

VPC Service Controls 境界ポリシー

ポリシーにより、VPC Service Controls ルールセットの例外が許可されます。ポリシーの詳細については、["GCP VPC サービスコントロールポリシードキュメント"](#)。

コンソールに必要なポリシーを設定するには、組織内の VPC Service Controls 境界に移動し、次のポリシーを追加します。フィールドは、VPC Service Controls ポリシー ページで指定されたオプションと一致する必要があります。また、すべての*ルールが必須であり、ルール セットでは ***OR** パラメータを使用する必要があります。あることにも注意してください。

イングレスルール

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Service Project]
  Services =
    Service name: iam.googleapis.com
    Service methods: All actions
    Service name: compute.googleapis.com
    Service methods: All actions
```

または

```
From:
  Identities:
    [User Email Address]
  Source > All sources allowed
To:
  Projects =
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

または

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
  Source > All sources allowed
To:
  Projects =
    [Service Project]
    [Host Project]
  Services =
    Service name: compute.googleapis.com
    Service methods: All actions
```

出口ルール

```
From:
  Identities:
    [Service Project Number]@cloudservices.gserviceaccount.com
To:
  Projects =
    14190056516
  Service =
    Service name: compute.googleapis.com
    Service methods: All actions
```



上記のプロジェクト番号は、NetAppがコンソール エージェントとCloud Volumes ONTAP のイメージを保存するために使用するプロジェクト *netapp-cloudmanager* です。

Cloud Volumes ONTAP用の Google Cloud サービス アカウントを作成する

Cloud Volumes ONTAP、2つの目的で Google Cloud サービス アカウントが必要です。1つ目は、**"データ階層化"**コールドデータを Google Cloud の低コストのオブジェクト ストレージに階層化します。2つ目は、**"NetAppバックアップとリカバリ"**ボリュームを低コストのオブジェクト ストレージにバックアップします。

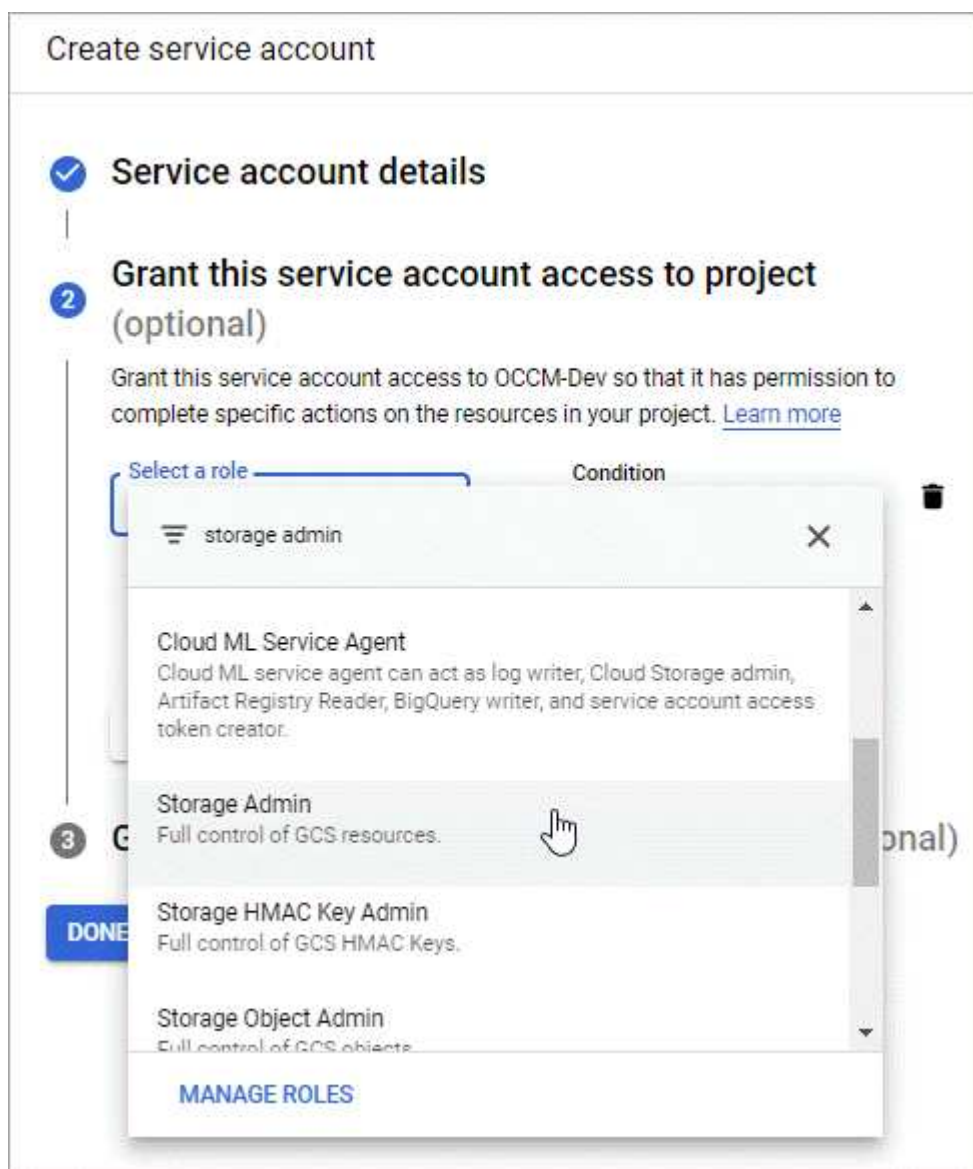
Cloud Volumes ONTAP は、サービス アカウントを使用して、階層化データ用の1つのバケットとバックアップ用の別のバケットにアクセスし、管理します。

1つのサービス アカウントを設定して、両方の目的に使用できます。サービス アカウントには **Storage Admin** ロールが必要です。

手順

1. Google Cloudコンソールでは、**"サービスアカウントページに移動します"**。
2. プロジェクトを選択してください。

3. サービス アカウントの作成 をクリックし、必要な情報を入力します。
 - a. サービス アカウントの詳細: 名前と説明を入力します。
 - b. このサービス アカウントにプロジェクトへのアクセス権を付与します: ストレージ管理者 ロールを選択します。



- c. ユーザーにこのサービス アカウントへのアクセスを許可: コンソール エージェント サービス アカウントを サービス アカウント ユーザー としてこの新しいサービス アカウントに追加します。

この手順は、データ階層化の場合にのみ必要です。バックアップとリカバリには必要ありません。

Create service account

✓ Service account details

✓ Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. [Learn more](#)

Service account users role

netapp-cloud-manager@iam.gserviceaccount.com

?

Grant users the permissions to deploy jobs and VMs with this service account

Service account admins role

?

Grant users the permission to administer this service account

DONE

CANCEL

次の手順

後でCloud Volumes ONTAPシステムを作成するときに、サービス アカウントを選択する必要があります。

Details and Credentials

default-project
Google Cloud Project

gcp-sub2
Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)
cloudvolumesontap

Service Account ⓘ

Service Account Name
account1

+ Add Labels

Optional Field | Up to four labels

Credentials

User Name
admin

Password

Confirm Password

Cloud Volumes ONTAPで顧客管理の暗号化キーを使用する

Google Cloud Storage では、データがディスクに書き込まれる前に常に暗号化されますが、API を使用して、顧客管理の暗号化キー を使用するCloud Volumes ONTAPシステムを作成できます。これらは、Cloud Key Management Service を使用して GCP で生成および管理するキーです。

手順

1. キーが保存されているプロジェクトにおいて、コンソール エージェント サービス アカウントにプロジェクト レベルでの適切な権限があることを確認します。

権限は、["デフォルトのサービスアカウント権限"](#)ただし、Cloud Key Management Service に代替プロジェクトを使用する場合は適用されない可能性があります。

権限は次のとおりです。

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

2. サービスアカウントが ["Google Compute Engine サービス エージェント"](#)キーに対する Cloud KMS 暗号化/復号化権限を持っています。

サービス アカウントの名前は、「service-[service_project_number]@compute-system.iam.gserviceaccount.com」という形式になります。

["Google Cloud ドキュメント: Cloud KMS での IAM の使用 - リソースに対するロールの付与"](#)

3. getコマンドを呼び出してキーの「ID」を取得します。 /gcp/vsa/metadata/gcp-encryption-keys API 呼び出し、または GCP コンソールのキーで「リソース名のコピー」を選択します。
4. 顧客管理の暗号化キーを使用し、データをオブジェクト ストレージに階層化する場合、NetAppコンソールは永続ディスクの暗号化に使用されるのと同じキーを利用しようとしています。ただし、まず Google Cloud Storage バケットがキーを使用できるようにする必要があります。
 - a. Google Cloud Storageサービスエージェントを見つけるには、["Google Cloud ドキュメント: Cloud Storage サービス エージェントの取得"](#)。
 - b. 暗号化キーに移動し、Google Cloud Storage サービス エージェントに Cloud KMS 暗号化/復号化権限を割り当てます。

詳細については、["Google Cloud ドキュメント: 顧客管理の暗号鍵の使用"](#)

5. システムを作成するときは、API リクエストで「GcpEncryption」パラメータを使用します。

例

```
"gcpEncryptionParameters": {  
  "key": "projects/project-1/locations/us-east4/keyRings/keyring-  
1/cryptoKeys/generatedkey1"  
}
```

参照 ["NetAppコンソール自動化ドキュメント"](#) 「GcpEncryption」パラメータの使用に関する詳細については、こちらをご覧ください。

Google Cloud 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

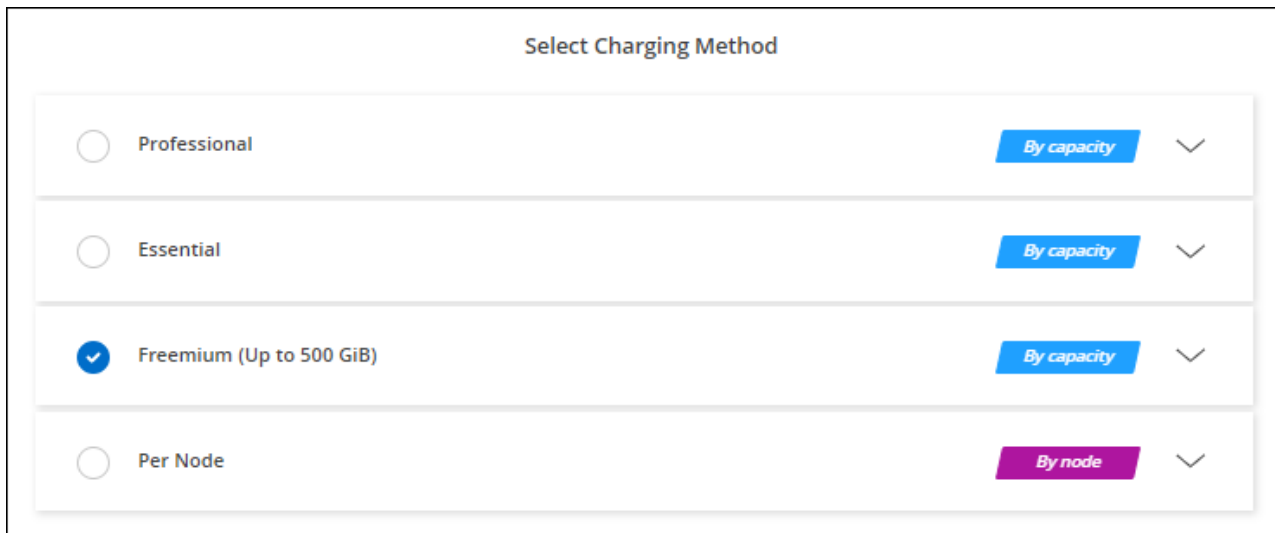
最大 500 GiB のプロビジョニング容量でCloud Volumes ONTAP を無料で使用するには、Freemium オフリングを選択してください。["フリーミアムプランの詳細"](#)。

手順

1. 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、NetAppコンソールの手順に従います。
 - a. [*詳細と認証情報*](#) ページで、[*認証情報の編集 > サブスクリプションの追加*](#) をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

プロビジョニングされた容量が500GiBを超えない限り、マーケットプレイ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"](#)。

- b. 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。



The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Freemium (Up to 500 GiB)' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for Professional, Essential, and Freemium are blue, while the button for Per Node is purple.

["Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください"](#)。

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、次の消費モデルで利用できます。

- NetAppから購入したライセンス（BYOL）
- Google Cloud 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NetApp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。エラーがなければ、コンソールはライセンスを追加します。

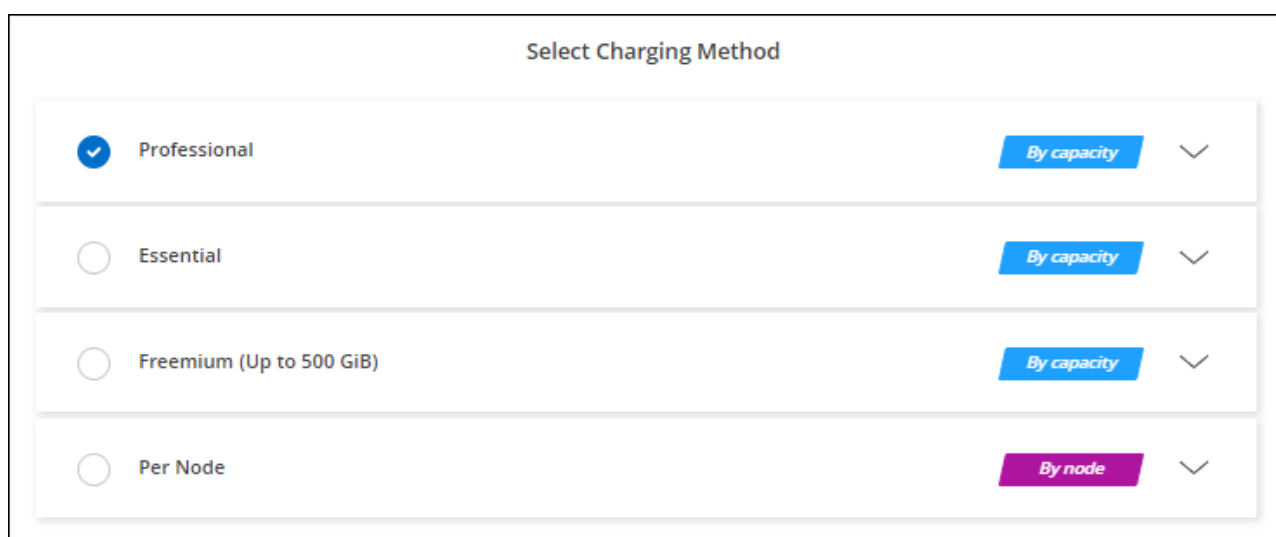
Cloud Volumes ONTAPでライセンスを使用するには、コンソールからライセンスを利用できる必要があります。必要であれば、"[コンソールにライセンスを手動で追加する](#)"。

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. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

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、マーケットプレースの時間単位料金で課金されます。

- 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。



The screenshot shows a 'Select Charging Method' dialog box with four radio button options. The 'Professional' option is selected, indicated by a blue checkmark. To the right of each option is a button labeled 'By capacity' (for Professional, Essential, and Freemium) or 'By node' (for Per Node), followed by a downward arrow. The buttons for 'By capacity' are blue, while the button for 'By node' is purple.

Charging Method	Button Label
☒ Professional	By capacity
☐ Essential	By capacity
☐ Freemium (Up to 500 GiB)	By capacity
☐ Per Node	By node

"[Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください](#)".

PAYGOサブスクリプション

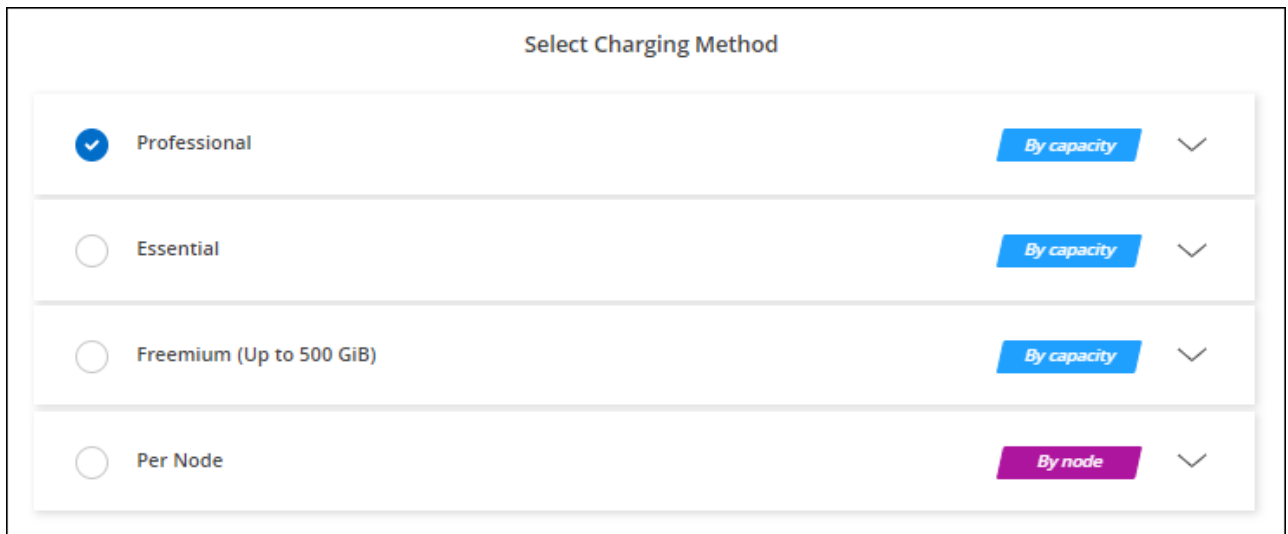
クラウド プロバイダーのマーケットプレースからのオファーをサブスクライブして、時間単位で支払います。

Cloud Volumes ONTAPシステムを作成すると、コンソールに、Google Cloud Marketplace で利用可能な契約に加入するように求めるメッセージが表示されます。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. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従ってGoogle Cloud Marketplaceの従量課金制オファーに登録します。

- 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	▼

"Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください"。



アカウントに関連付けられている Google Cloud Marketplace サブスクリプションは、[設定] > [認証情報] ページから管理できます。 ["Google Cloud の認証情報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。

この契約は、Google Cloud Marketplace でプライベート オファーとして入手できます。

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 Google Cloud Marketplace からサブスクリプションを選択できます。

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. *詳細と認証情報*ページで、*認証情報の編集 > サブスクリプションの追加*をクリックし、指示に従って Google Cloud Marketplace で年間プランを登録します。
 - b. Google Cloud で、アカウントと共有された年間プランを選択し、[登録] 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

▼

"[Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください](#)".

Keystoneサブスクリプション

Keystoneサブスクリプションは、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に問い合わせ](#) して、コンソール ユーザー アカウントに 1 つ以上のKeystoneサブスクリプションを承認します。
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

Storage management

Charged against your NetApp credit

Keystone Subscription

A-AMRITA1

By capacity

Professional

By capacity

Essential

By capacity

Freemium (Up to 500 GiB)

By capacity

Per Node

By node

["Google Cloud でCloud Volumes ONTAP を起動するための手順をご覧ください"](#)。

Google Cloud でCloud Volumes ONTAPを起動する

Cloud Volumes ONTAPは、単一ノード構成または Google Cloud の HA ペアとして起動できます。

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"。
 - コンソールエージェントに関連付けられたサービスアカウント "必要な権限を持っている必要があります"
- 使用する構成を理解すること。

構成を選択し、管理者から Google Cloud ネットワーク情報を取得して準備しておく必要があります。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"。

- Google Cloud APIは "[プロジェクトで有効化](#)":
 - クラウド デプロイメント マネージャー V2 API
 - クラウドログインAPI
 - クラウド リソース マネージャー API
 - コンピューティングエンジン API
 - アイデンティティとアクセス管理 (IAM) API

Google Cloud でシングルノード システムを起動する

NetAppコンソールでシステムを作成し、Google Cloud でCloud Volumes ONTAP を起動します。

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. 場所を選択: **Google Cloud** と * Cloud Volumes ONTAP* 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. 詳細と認証情報: プロジェクトを選択し、クラスター名を指定し、オプションでサービス アカウントを選択し、オプションでラベルを追加して、認証情報を指定します。

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 Google Cloud VM インスタンス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。
サービスアカウント名	使用予定の場合" データ階層化 "または " NetAppバックアップとリカバリ "Cloud Volumes ONTAPを使用する場合は、サービス アカウント を有効にし、事前定義されたストレージ管理者ロールを持つサービス アカウントを選択する必要があります。" サービスアカウントの作成方法を学ぶ "。
ラベルを追加する	ラベルは、Google Cloud リソースのメタデータです。コンソールは、Cloud Volumes ONTAPシステムと、システムに関連付けられた Google Cloud リソースにラベルを追加します。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 つのラベルを追加でき、作成後にさらにラベルを追加できます。システムを作成するときに、API ではラベルが 4 つに制限されないことに注意してください。ラベルの詳細については、 " Google Cloud ドキュメント: ラベル付けリソース "。
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。

フィールド	説明
プロジェクトを編集	Cloud Volumes ONTAPを配置するプロジェクトを選択します。デフォルトのプロジェクトは、コンソールがあるプロジェクトです。 ドロップダウン リストに追加のプロジェクトが表示されない場合は、サービス アカウントが他のプロジェクトにまだ関連付けられていません。Google Cloud コンソールに移動し、IAM サービスを開いて、プロジェクトを選択します。コンソールに使用するロールを持つサービス アカウントをそのプロジェクトに追加します。プロジェクトごとにこの手順を繰り返す必要があります。  これはコンソール用に設定したサービスアカウントです。"このページに記載されている通り"。 選択した資格情報をサブスクリプションに関連付けるには、「サブスクリプションの追加」をクリックします。 従量課金制のCloud Volumes ONTAPシステムを作成するには、Google Cloud マーケットプレイスからCloud Volumes ONTAPのサブスクリプションに関連付けられている Google Cloud プロジェクトを選択する必要があります。参照 "マーケットプレイスのサブスクリプションを Google Cloud 認証情報に関連付ける"。

6. サービス: このシステムで使用するサービスを選択します。バックアップとリカバリを選択するか、NetApp Cloud Tiering を使用するには、手順 3 でサービス アカウントを指定する必要があります。



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. 場所と接続: 場所を選択し、ファイアウォール ポリシーを選択して、データ階層化のための Google Cloud ストレージへのネットワーク接続を確認します。

次の表では、ガイダンスが必要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
接続検証	コールド データを Google Cloud Storage バケットに階層化するには、Cloud Volumes ONTAP が存在するサブネットをプライベート Google アクセス用に構成する必要があります。手順については、"Google Cloud ドキュメント: プライベート Google アクセスの設定"。
生成されたファイアウォールポリシー	コンソールでファイアウォール ポリシー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 VPC のみ を選択した場合、受信トラフィックのソース フィルターは、選択した VPC 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 VPC 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 VPC を選択した場合、受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲になります。

フィールド	説明
既存のファイアウォールポリシーを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。 "Cloud Volumes ONTAPのファイアウォールルールについて学ぶ"

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 サイトのアカウントを指定します。

- ["Cloud Volumes ONTAPのライセンスオプションについて学ぶ"](#)
- ["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: 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。

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、マシンタイプを選択します。



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. 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 (ディスク タイプと各ディスクのサイズ) を選択します。

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す。

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の選択については、以下を参照してください。["Google Cloud でシステムのサイズを決定する"](#)。

12. フラッシュキャッシュ、書き込み速度、**WORM**:

- a. 必要に応じて、フラッシュ キャッシュ を有効にします。



Cloud Volumes ONTAP 9.13.1 以降、*Flash Cache* は n2-standard-16、n2-standard-32、n2-standard-48、および n2-standard-64 インスタンス タイプでサポートされます。デプロイメント後に Flash Cache を無効にすることはできません。

- b. 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"](#)。



「高」書き込み速度オプションを選択すると、高速書き込み速度と、8,896 バイトの最大転送単位 (MTU) をさらに高めることができます。さらに、MTU が 8,896 と高いため、デプロイメントには VPC-1、VPC-2、VPC-3 を選択する必要があります。VPC-1、VPC-2、VPC-3の詳細については、以下を参照してください。"[VPC-1、VPC-2、VPC-3のルール](#)"。

- c. 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。

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。

13. **Google Cloud Platform** でのデータ階層化: 初期アグリゲートでデータ階層化を有効にするかどうかを選択し、階層化データのストレージ クラスを選択してから、定義済みのストレージ管理者ロールを持つサービス アカウントを選択するか (Cloud Volumes ONTAP 9.7 以降に必要)、Google Cloud アカウントを選択します (Cloud Volumes ONTAP 9.6 に必要)。

次の点に注意してください。

- コンソールは、Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービス アカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。コンソールエージェント サービス アカウントを階層化サービス アカウントのユーザーとして必ず追加してください。そうしないと、コンソールから選択できません。
- Google Cloud アカウントの追加に関するヘルプについては、以下を参照してください。"[9.6 でデータ階層化を行うための Google Cloud アカウントの設定と追加](#)"。
- 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、後続の集計で有効にすることはできますが、システムをオフにして、Google Cloud コンソールからサービス アカウントを追加する必要があります。

"[データ階層化の詳細](#)"。

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

"[サポートされ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。

フィールド	説明
権限とユーザー/グループ (CIFSのみ)	これらのフィールドを使用すると、ユーザ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 ⓘ

- 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。Google マネージド Active Directory を構成している場合、デフォルトでは 169.254.169.254 IP アドレスを使用して AD にアクセスできます。
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。Google Managed Microsoft AD 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=Computers,OU=Cloud と入力します。https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント: Google Managed Microsoft AD の組織単位"]
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。詳細については、 "NetAppコンソール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。

16. 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?"](#)

17. 確認と承認: 選択内容を確認して確定します。

- 構成の詳細を確認します。
- 詳細情報 をクリックすると、サポートと、コンソールで購入する Google Cloud リソースの詳細を確認できます。
- 理解しました... チェックボックスを選択します。
- [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。

Google Cloud で HA ペアを起動する

コンソールでシステムを作成し、Google Cloud でCloud Volumes ONTAP を起動します。

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、ストレージ > システム をクリックし、指示に従います。
3. 場所を選択: **Google Cloud** と * Cloud Volumes ONTAP HA* を選択します。
4. 詳細と認証情報: プロジェクトを選択し、クラスター名を指定し、オプションでサービス アカウントを選択し、オプションでラベルを追加して、認証情報を指定します。

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 Google Cloud VM インスタンス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。
サービスアカウント名	ご利用予定の場合は "NetAppクラウド階層化" または "バックアップとリカバリ" サービスでは、サービス アカウント スイッチを有効にして、定義済みのストレージ管理者ロールを持つサービス アカウントを選択する必要があります。
ラベルを追加する	ラベルは、Google Cloud リソースのメタデータです。コンソールは、Cloud Volumes ONTAPシステムと、システムに関連付けられた Google Cloud リソースにラベルを追加します。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 つのラベルを追加でき、作成後にさらにラベルを追加できます。システムを作成するときに、API ではラベルが 4 つに制限されないことに注意してください。ラベルの詳細については、 "Google Cloud ドキュメント: ラベル付けリソース" 。
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。

フィールド	説明
プロジェクトを編集	Cloud Volumes ONTAPを配置するプロジェクトを選択します。デフォルトのプロジェクトは、コンソールのプロジェクトです。 ド롭ダウン リストに追加のプロジェクトが表示されない場合は、サービス アカウントが他のプロジェクトにまだ関連付けられていません。Google Cloud コンソールに移動し、IAM サービスを開いて、プロジェクトを選択します。コンソールに使用するロールを持つサービス アカウントをそのプロジェクトに追加します。プロジェクトごとにこの手順を繰り返す必要があります。  これはコンソール用に設定したサービスアカウントです。"このページに記載されている通り"。 選択した資格情報をサブスクリプションに関連付けるには、「サブスクリプションの追加」をクリックします。 従量課金制の Cloud Volumes ONTAPシステムを作成するには、Google Cloud Marketplace からCloud Volumes ONTAPのサブスクリプションに関連付けられている Google Cloud プロジェクトを選択する必要があります。参照 "マーケットプレイスのサブスクリプションを Google Cloud 認証情報に関連付ける"。

5. サービス: このシステムで使用するサービスを選択します。バックアップとリカバリを選択するか、NetApp Cloud Tiering を使用するには、手順 3 でサービス アカウントを指定する必要があります。



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:** HA 構成に複数のゾーン (推奨) または単一のゾーンを選択します。次に、リージョンとゾーンを選択します。

["HA展開モデルの詳細"](#)。

7. 接続: HA 構成に 4 つの異なる VPC、各 VPC 内のサブネットを選択し、ファイアウォール ポリシーを選択します。

["ネットワーク要件の詳細"](#)。

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
生成されたポリシー	コンソールでファイアウォール ポリシー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 VPC のみ を選択した場合、受信トラフィックのソース フィルターは、選択した VPC 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 VPC 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 VPC を選択した場合、受信トラフィックのソース フィルターは 0.0.0.0/0 IP 範囲になります。
既存のものを使用する	既存のファイアウォール ポリシーを使用する場合は、必要なルールが含まれていることを確認してください。"Cloud Volumes ONTAPのファイアウォールルールについて学ぶ"。

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: 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。

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、マシンタイプを選択します。



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. 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 (ディスク タイプと各ディスクのサイズ) を選択します。

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の選択については、以下を参照してください。"[Google Cloud でシステムのサイズを決定する](#)"。

12. フラッシュキャッシュ、書き込み速度、**WORM**:

- a. 必要に応じて、フラッシュ キャッシュ を有効にします。



Cloud Volumes ONTAP 9.13.1 以降、*Flash Cache* は n2-standard-16、n2-standard-32、n2-standard-48、および n2-standard-64 インスタンス タイプでサポートされます。デプロイメント後に *Flash Cache* を無効にすることはできません。

- b. 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"](#)。



n2-standard-16、n2-standard-32、n2-standard-48、n2-standard-64 インスタンス タイプの 高 書き込み速度オプションでは、高速書き込み速度と 8,896 バイトの最大転送単位 (MTU) のより高い速度を利用できます。さらに、MTU が 8,896 と高いため、デプロイメントには VPC-1、VPC-2、VPC-3 を選択する必要があります。高速書き込み速度と 8,896 の MTU は機能に依存しており、構成されたインスタンス内で個別に無効にすることはできません。VPC-1、VPC-2、VPC-3の詳細については、以下を参照してください。 ["VPC-1、VPC-2、VPC-3のルール"](#)。

- c. 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。

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。

13. **Google Cloud** でのデータ階層化: 初期集約でデータ階層化を有効にするかどうかを選択し、階層化されたデータのストレージ クラスを選択してから、事前定義されたストレージ管理者のロールを持つサービス アカウントを選択します。

次の点に注意してください。

- コンソールは、Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービス アカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。コンソール エージェント サービス アカウントを階層化サービス アカウントのユーザーとして必ず追加してください。そうしないと、コンソールから選択できません。
- 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、後続の集計で有効にすることはできますが、システムをオフにして、Google Cloud コンソールからサービス アカウントを追加する必要があります。

["データ階層化の詳細"](#)。

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

["サポートされ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

ABDcv5689

Storage VM (SVM)

svm_CVO1

Volume Size

100

Unit

GiB

Snapshot Policy

default

default policy

15. **CIFS** セットアップ: CIFS プロトコルを選択した場合は、CIFS サーバ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。Google マネージド Active Directory を構成している場合、デフォルトでは 169.254.169.254 IP アドレスを使用して AD にアクセスできます。
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。Google Managed Microsoft AD 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=Computers,OU=Cloud と入力します。 https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units ["Google Cloud ドキュメント: Google Managed Microsoft AD の組織単位"]
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コンソール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を注意してください。CIFS サーバーを作成した後は構成できません。

16. 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?](#)"

17. 確認と承認: 選択内容を確認して確定します。

- 構成の詳細を確認します。
- 詳細情報をクリックすると、サポートと、コンソールで購入する Google Cloud リソースの詳細を確認できます。
- 理解しました... チェックボックスを選択します。
- [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。

Google Cloud Platform イメージ検証

Cloud Volumes ONTAPで Google Cloud イメージを検証する方法を学びます

Google Cloud 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。イメージを生成するスクリプトに変更が加えられ、このタスク専用生成された秘密鍵を使用して、途中でイメージに署名するようになりました。Google Cloud イメージの整合性は、Google Cloud の署名済みダイジェストと公開証明書を使用して検証できます。これらの証明書は、以下からダウンロードできます。"[NSS](#)"特定のリリース用。



Google Cloud イメージ検証は、Cloud Volumes ONTAPソフトウェア バージョン 9.13.0 以降でサポートされています。

Google Cloud イメージをCloud Volumes ONTAPの RAW 形式に変換する

新しいインスタンスやアップグレードを展開するために使用されているイメージ、または既存のイメージで使用されているイメージは、"[NetAppサポート サイト \(NSS\)](#)"。署名されたダイジェストと証明書は、NSS ポータルからダウンロードできます。NetApp サポートによって共有されたイメージに対応する適切なリリースのダイジェストと証明書をダウンロードしていることを確認してください。たとえば、9.13.0 イメージには、NSS で利用可能な 9.13.0 署名ダイジェストと証明書が含まれます。

このステップはなぜ必要なのでしょうか？

Google Cloud からのイメージを直接ダウンロードすることはできません。署名されたダイジェストと証明書に対してイメージを検証するには、2つのファイルを比較してイメージをダウンロードするメカニズムが必要です。これを行うには、イメージを disk.raw 形式にエクスポート/変換し、結果を Google Cloud のストレージバケットに保存する必要があります。このプロセスでは、disk.raw ファイルが tar 圧縮され、gzip 圧縮されます。

ユーザー/サービス アカウントには、次の操作を実行する権限が必要です。

- Google ストレージ バケットへのアクセス
- Google Storage バケットに書き込む

- クラウド ビルド ジョブを作成する (エクスポート プロセス中に使用)
- 希望の画像へのアクセス
- 画像のエクスポートタスクを作成する

イメージを検証するには、disk.raw 形式に変換してからダウンロードする必要があります。

Google Cloud コマンドラインを使用して **Google Cloud** イメージをエクスポートする

画像をクラウドストレージにエクスポートする推奨方法は、"[gcloud compute images エクスポートコマンド](#)"。このコマンドは、提供されたイメージを取得し、それを tar および gzip で圧縮された disk.raw ファイルに変換します。生成されたファイルは宛先 URL に保存され、検証のためにダウンロードできます。

この操作を実行するには、ユーザー/アカウントに、目的のバケットにアクセスして書き込む権限、イメージをエクスポートする権限、クラウド ビルド (Google がイメージをエクスポートするために使用) の権限が必要です。

gcloud を使用して **Google Cloud** イメージをエクスポートする

```
$ gcloud compute images export \
  --destination-uri DESTINATION_URI \
  --image IMAGE_NAME

# For our example:
$ gcloud compute images export \
  --destination-uri gs://vsa-dev-bucket1/example-user-exportimage-
gcp-demo \
  --image example-user-20230120115139

## DEMO ##
# Step 1 - Optional: Checking access and listing objects in the
destination bucket
$ gsutil ls gs://example-user-export-image-bucket/

# Step 2 - Exporting the desired image to the bucket
$ gcloud compute images export --image example-user-export-image-demo
--destination-uri gs://example-user-export-image-bucket/export-
demo.tar.gz
Created [https://cloudbuild.googleapis.com/v1/projects/example-demo-
project/locations/us-central1/builds/xxxxxxxxxxxxx].
Logs are available at [https://console.cloud.google.com/cloud-
build/builds;region=us-central1/xxxxxxxxxxxxx?project=xxxxxxxxxxxxx].
[image-export]: 2023-01-25T18:13:48Z Fetching image "example-user-
export-image-demo" from project "example-demo-project".
[image-export]: 2023-01-25T18:13:49Z Validating workflow
[image-export]: 2023-01-25T18:13:49Z Validating step "setup-disks"
[image-export]: 2023-01-25T18:13:49Z Validating step "image-export-
export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "setup-disks"
[image-export.image-export-export-disk]: 2023-01-25T18:13:49Z
Validating step "run-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "wait-for-inst-image-export-export-disk"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "copy-image-object"
[image-export.image-export-export-disk]: 2023-01-25T18:13:50Z
Validating step "delete-inst"
[image-export]: 2023-01-25T18:13:51Z Validation Complete
[image-export]: 2023-01-25T18:13:51Z Workflow Project: example-demo-
project
[image-export]: 2023-01-25T18:13:51Z Workflow Zone: us-central1-c
```

```

[image-export]: 2023-01-25T18:13:51Z Workflow GCSPath: gs://example-
demo-project-example-bkt-us/
[image-export]: 2023-01-25T18:13:51Z Example scratch path:
https://console.cloud.google.com/storage/browser/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px
[image-export]: 2023-01-25T18:13:51Z Uploading sources
[image-export]: 2023-01-25T18:13:51Z Running workflow
[image-export]: 2023-01-25T18:13:51Z Running step "setup-disks"
(CreateDisks)
[image-export.setup-disks]: 2023-01-25T18:13:51Z CreateDisks: Creating
disk "disk-image-export-image-export-r88px".
[image-export]: 2023-01-25T18:14:02Z Step "setup-disks" (CreateDisks)
successfully finished.
[image-export]: 2023-01-25T18:14:02Z Running step "image-export-export-
disk" (IncludeWorkflow)
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "setup-disks" (CreateDisks)
[image-export.image-export-export-disk.setup-disks]: 2023-01-
25T18:14:02Z CreateDisks: Creating disk "disk-image-export-export-disk-
image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Step
"setup-disks" (CreateDisks) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:14:02Z Running
step "run-image-export-export-disk" (CreateInstances)
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:02Z CreateInstances: Creating instance "inst-image-
export-export-disk-image-export-image-export--r88px".
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Step
"run-image-export-export-disk" (CreateInstances) successfully finished.
[image-export.image-export-export-disk.run-image-export-export-disk]:
2023-01-25T18:14:08Z CreateInstances: Streaming instance "inst-image-
export-export-disk-image-export-image-export--r88px" serial port 1
output to https://storage.cloud.google.com/example-demo-project-
example-bkt-us/example-image-export-20230125-18:13:49-r88px/logs/inst-
image-export-export-disk-image-export-image-export--r88px-serial-
port1.log
[image-export.image-export-export-disk]: 2023-01-25T18:14:08Z Running
step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal)
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:08Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
watching serial port 1, SuccessMatch: "ExportSuccess", FailureMatch:
["ExportFailed:"] (this is not an error), StatusMatch: "GCEExport:".
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":

```

```

StatusMatch found: "GCEExport: <serial-output key:'source-size-gb'
value:'10'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Running export tool."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Disk /dev/sdb is 10 GiB, compressed size
will most likely be much smaller."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Beginning export process..."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Copying \"/dev/sdb\" to gs://example-
demo-project-example-bkt-us/example-image-export-20230125-18:13:49-
r88px/outs/image-export-export-disk.tar.gz."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Using \"/root/upload\" as the buffer
prefix, 1.0 GiB as the buffer size, and 4 as the number of workers."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Creating gzipped image of \"/dev/sdb\"."
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:29Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 1.0 GiB of 10 GiB (212 MiB/sec),
total written size: 992 MiB (198 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:14:59Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Read 8.0 GiB of 10 GiB (237 MiB/sec),
total written size: 1.5 GiB (17 MiB/sec)"
[image-export.image-export-export-disk.wait-for-inst-image-export-
export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance
"inst-image-export-export-disk-image-export-image-export--r88px":
StatusMatch found: "GCEExport: Finished creating gzipped image of
\"/dev/sdb\" in 48.956433327s [213 MiB/s] with a compression ratio of
6."

```

```

[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: Finished export in 48.957347731s"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": StatusMatch found: "GCEExport: <serial-output key:'target-size-gb' value:'2'>"
[image-export.image-export-export-disk.wait-for-inst-image-export-export-disk]: 2023-01-25T18:15:19Z WaitForInstancesSignal: Instance "inst-image-export-export-disk-image-export-image-export--r88px": SuccessMatch found "ExportSuccess"
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "wait-for-inst-image-export-export-disk" (WaitForInstancesSignal) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "copy-image-object" (CopyGCSObjects)
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Running step "delete-inst" (DeleteResources)
[image-export.image-export-export-disk.delete-inst]: 2023-01-25T18:15:19Z DeleteResources: Deleting instance "inst-image-export-export-disk".
[image-export.image-export-export-disk]: 2023-01-25T18:15:19Z Step "copy-image-object" (CopyGCSObjects) successfully finished.
[image-export.image-export-export-disk]: 2023-01-25T18:15:34Z Step "delete-inst" (DeleteResources) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Step "image-export-export-disk" (IncludeWorkflow) successfully finished.
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> source-size-gb:10
[image-export]: 2023-01-25T18:15:34Z Serial-output value -> target-size-gb:2
[image-export]: 2023-01-25T18:15:34Z Workflow "image-export" cleaning up (this may take up to 2 minutes).
[image-export]: 2023-01-25T18:15:35Z Workflow "image-export" finished cleanup.

# Step 3 - Validating the image was successfully exported
$ gsutil ls gs://example-user-export-image-bucket/
gs://example-user-export-image-bucket/export-demo.tar.gz

# Step 4 - Download the exported image
$ gcloud storage cp gs://BUCKET_NAME/OBJECT_NAME SAVE_TO_LOCATION

```

```
$ gcloud storage cp gs://example-user-export-image-bucket/export-  
demo.tar.gz CVO_GCP_Signed_Digest.tar.gz  
Copying gs://example-user-export-image-bucket/export-demo.tar.gz to  
file://CVO_GCP_Signed_Digest.tar.gz  
Completed files 1/1 | 1.5GiB/1.5GiB | 185.0MiB/s
```

```
Average throughput: 213.3MiB/s
```

```
$ ls -l  
total 1565036  
-rw-r--r-- 1 example-user example-user 1602589949 Jan 25 18:44  
CVO_GCP_Signed_Digest.tar.gz
```

圧縮ファイルを解凍

```
# Extracting files from the digest  
$ tar -xf CVO_GCP_Signed_Digest.tar.gz
```



Google Cloud経由で画像をエクスポートする方法の詳細については、["画像のエクスポートに関する Google Cloud ドキュメント"](#)。

画像署名検証

Cloud Volumes ONTAPの Google Cloud イメージ署名検証

エクスポートされた Google Cloud 署名付きイメージを検証するには、NSS からイメージ ダイジェスト ファイルをダウンロードして、disk.raw ファイルとダイジェスト ファイルの内容を検証する必要があります。

署名画像検証ワークフローの概要

以下は、Google Cloud 署名付きイメージ検証ワークフロー プロセスの概要です。

- から **"NSS"**次のファイルを含む Google Cloud アーカイブをダウンロードします。
 - 署名付きダイジェスト (.sig)
 - 公開鍵を含む証明書 (.pem)
 - 証明書チェーン (.pem)

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

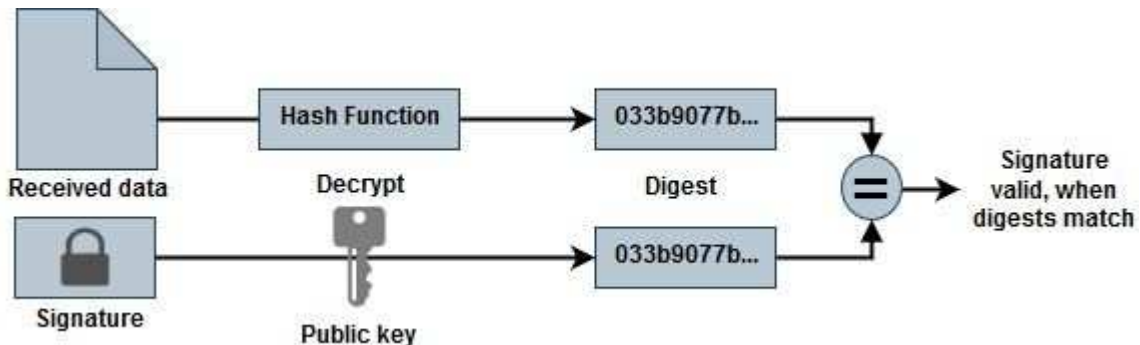
DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

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

[View and download checksums](#)

- 変換されたdisk.rawファイルをダウンロードする
- 証明書チェーンを使用して証明書を検証する
- 公開鍵を含む証明書を使用して署名されたダイジェストを検証する
 - 公開鍵を使用して署名されたダイジェストを復号化し、画像ファイルのダイジェストを抽出します。
 - ダウンロードしたdisk.rawファイルのダイジェストを作成する
 - 検証のために2つのダイジェストファイルを比較する



OpenSSL を使用してCloud Volumes ONTAPの Google Cloud イメージの disk.raw ファイルを確認する

Google Cloudでダウンロードしたdisk.rawファイルを、以下のダイジェストファイルの内容と比較することができます。 "NSS" OpenSSL を使用します。



イメージを検証するための OpenSSL コマンドは、Linux、macOS、および Windows マシンと互換性があります。

手順

1. OpenSSL を使用して証明書を検証します。

```
# Step 1 - Optional, but recommended: Verify the certificate using
OpenSSL

# Step 1.1 - Copy the Certificate and certificate chain to a
directory
$ openssl version
LibreSSL 3.3.6
$ ls -l
total 48
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.pem

# Step 1.2 - Get the OSCP URL
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in <Certificate-
Chain.pem>)
$ oscp_url=$(openssl x509 -noout -ocsp_uri -in Certificate-Chain-
GCP-CVO-20230119-0XXXXXX.pem)
$ echo $oscp_url
http://ocsp.entrust.net

# Step 1.3 - Generate an OSCP request for the certificate
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -reqout <request.der>
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXXX.pem -reqout req.der

# Step 1.4 - Optional: Check the new file "req.der" has been
generated
$ ls -l
total 56
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der

# Step 1.5 - Connect to the OSCP Manager using openssl to send the
OCSP request
$ openssl ocsp -issuer <Certificate-Chain.pem> -CAfile <Certificate-
Chain.pem> -cert <Certificate.pem> -url ${oscp_url} -resp_text
-respout <response.der>
```

```
$ openssl ocsp -issuer Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem
-CAfile Certificate-Chain-GCP-CVO-20230119-0XXXXX.pem -cert
Certificate-GCP-CVO-20230119-0XXXXX.pem -url ${ocsp_url} -resp_text
-respout resp.der
```

OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2

Produced At: Jan 19 15:14:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 5994B3D01D26D594BD1D0FA7098C6FF5

Cert Status: good

This Update: Jan 19 15:00:00 2023 GMT

Next Update: Jan 26 14:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

0b:b6:61:e4:03:5f:98:6f:10:1c:9a:f7:5f:6f:c7:e3:f4:72:
f2:30:f4:86:88:9a:b9:ba:1e:d6:f6:47:af:dc:ea:e4:cd:31:
af:e3:7a:20:35:9e:60:db:28:9c:7f:2e:17:7b:a5:11:40:4f:
1e:72:f7:f8:ef:e3:23:43:1b:bb:28:1a:6f:c6:9c:c5:0c:14:
d3:5d:bd:9b:6b:28:fb:94:5e:8a:ef:40:20:72:a4:41:df:55:
cf:f3:db:1b:39:e0:30:63:c9:c7:1f:38:7e:7f:ec:f4:25:7b:
1e:95:4c:70:6c:83:17:c3:db:b2:47:e1:38:53:ee:0a:55:c0:
15:6a:82:20:b2:ea:59:eb:9c:ea:7e:97:aa:50:d7:bc:28:60:
8c:d4:21:92:1c:13:19:b4:e0:66:cb:59:ed:2e:f8:dc:7b:49:
e3:40:f2:b6:dc:d7:2d:2e:dd:21:82:07:bb:3a:55:99:f7:59:
5d:4a:4d:ca:e7:8f:1c:d3:9a:3f:17:7b:7a:c4:57:b2:57:a8:
b4:c0:a5:02:bd:59:9c:50:32:ff:16:b1:65:3a:9c:8c:70:3b:
9e:be:bc:4f:f9:86:97:b1:62:3c:b2:a9:46:08:be:6b:1b:3c:
24:14:59:28:c6:ae:e8:d5:64:b2:f8:cc:28:24:5c:b2:c8:d8:
5a:af:9d:55:48:96:f6:3e:c6:bf:a6:0c:a4:c0:ab:d6:57:03:
2b:72:43:b0:6a:9f:52:ef:43:bb:14:6a:ce:66:cc:6c:4e:66:
17:20:a3:64:e0:c6:d1:82:0a:d7:41:8a:cc:17:fd:21:b5:c6:
d2:3a:af:55:2e:2a:b8:c7:21:41:69:e1:44:ab:a1:dd:df:6d:
15:99:90:cc:a0:74:1e:e5:2e:07:3f:50:e6:72:a6:b9:ae:fc:
44:15:eb:81:3d:1a:f8:17:b6:0b:ff:05:76:9d:30:06:40:72:
cf:d5:c4:6f:8b:c9:14:76:09:6b:3d:6a:70:2c:5a:c4:51:92:
e5:cd:84:b6:f9:d9:d5:bc:8d:72:b7:7c:13:9c:41:89:a8:97:
6f:4a:11:5f:8f:b6:c9:b5:df:00:7e:97:20:e7:29:2e:2b:12:
77:dc:e2:63:48:87:42:49:1d:fc:d0:94:a8:8d:18:f9:07:85:

```

e4:d0:3e:9a:4a:d7:d5:d0:02:51:c3:51:1c:73:12:96:2d:75:
22:83:a6:70:5a:4a:2b:f2:98:d9:ae:1b:57:53:3d:3b:58:82:
38:fc:fa:cb:57:43:3f:3e:7e:e0:6d:5b:d6:fc:67:7e:07:7e:
fb:a3:76:43:26:8f:d1:42:d6:a6:33:4e:9e:e0:a0:51:b4:c4:
bc:e3:10:0d:bf:23:6c:4b
WARNING: no nonce in response
Response Verify OK
Certificate-GCP-CVO-20230119-0XXXXX.pem: good
  This Update: Jan 19 15:00:00 2023 GMT
  Next Update: Jan 26 14:59:59 2023 GMT

# Step 1.5 - Optional: Check the response file "response.der" has
been generated. Verify its contents.
$ ls -l
total 64
-rw-r--r--@ 1 example-user  engr  8537 Jan 19 15:42 Certificate-
Chain-GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  engr  2365 Jan 19 15:42 Certificate-GCP-
CVO-20230119-0XXXXX.pem
-rw-r--r--  1 example-user  engr   120 Jan 19 16:50 req.der
-rw-r--r--  1 example-user  engr   806 Jan 19 16:51 resp.der

# Step 1.6 - Verify the chain of trust and expiration dates against
the local host
$ openssl version -d
OPENSSLDIR: "/private/etc/ssl"
$ OPENSSLDIR=$(openssl version -d | cut -d '"' -f2)
$ echo $OPENSSLDIR
/private/etc/ssl

$ openssl verify -untrusted <Certificate-Chain.pem> -CApath <OpenSSL
dir> <Certificate.pem>
$ openssl verify -untrusted Certificate-Chain-GCP-CVO-20230119-
0XXXXX.pem -CApath ${OPENSSLDIR} Certificate-GCP-CVO-20230119-
0XXXXX.pem
Certificate-GCP-CVO-20230119-0XXXXX.pem: OK

```

2. ダウンロードした disk.raw ファイル、署名、および証明書をディレクトリに配置します。
3. OpenSSL を使用して証明書から公開鍵を抽出します。
4. 抽出した公開キーを使用して署名を復号化し、ダウンロードした disk.raw ファイルの内容を確認します。

```
# Step 1 - Place the downloaded disk.raw, the signature and the
certificates in a directory
$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 2 - Extract the public key from the certificate
$ openssl x509 -pubkey -noout -in (certificate.pem) >
(public_key.pem)
$ openssl x509 -pubkey -noout -in Certificate-GCP-CVO-20230119-
0XXXXX.pem > CVO-GCP-pubkey.pem

$ ls -l
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-Chain-
GCP-CVO-20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 Certificate-GCP-CVO-
20230119-0XXXXX.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 17:02 CVO-GCP-pubkey.pem
-rw-r--r--@ 1 example-user  staff  Jan 19 15:42 GCP_CVO_20230119-
XXXXXX_digest.sig
-rw-r--r--@ 1 example-user  staff  Jan 19 16:39 disk.raw

# Step 3 - Decrypt the signature using the extracted public key and
verify the contents of the downloaded disk.raw
$ openssl dgst -verify (public_key) -keyform PEM -sha256 -signature
(signed digest) -binary (downloaded or obtained disk.raw)
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary disk.raw
Verified OK

# A failed response would look like this
$ openssl dgst -verify CVO-GCP-pubkey.pem -keyform PEM -sha256
-signature GCP_CVO_20230119-XXXXXX_digest.sig -binary
../sample_file.txt
Verification Failure
```

Cloud Volumes ONTAPを使用する

ライセンス管理

Cloud Volumes ONTAPの容量ベースのライセンスを管理する

NetAppコンソールから容量ベースのライセンスを管理して、NetAppアカウントにCloud Volumes ONTAPシステムに十分な容量があることを確認します。

容量ベースのライセンスを使用すると、容量 1 TiB ごとにCloud Volumes ONTAPの料金を支払うことができます。

NetAppコンソールから容量ベースのCloud Volumes ONTAPライセンスを管理できます。



コンソールで管理される製品とサービスの実際の使用量と計測値は常に GiB と TiB で計算されますが、GB/GiB と TB/TiB という用語は同じ意味で使用されます。これは、クラウドマーケットプレイスのリスト、価格見積もり、リストの説明、およびその他のサポートドキュメントに反映されます。

["Cloud Volumes ONTAPライセンスの詳細"](#)。

NetAppコンソールにライセンスを追加する方法

NetApp の営業担当者からライセンスを購入すると、NetAppシリアル番号と追加のライセンス詳細が記載されたメールが送信されます。

その間、コンソールは自動的に NetApp のライセンス サービスにクエリを実行し、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。エラーがなければ、ライセンスが追加されます。

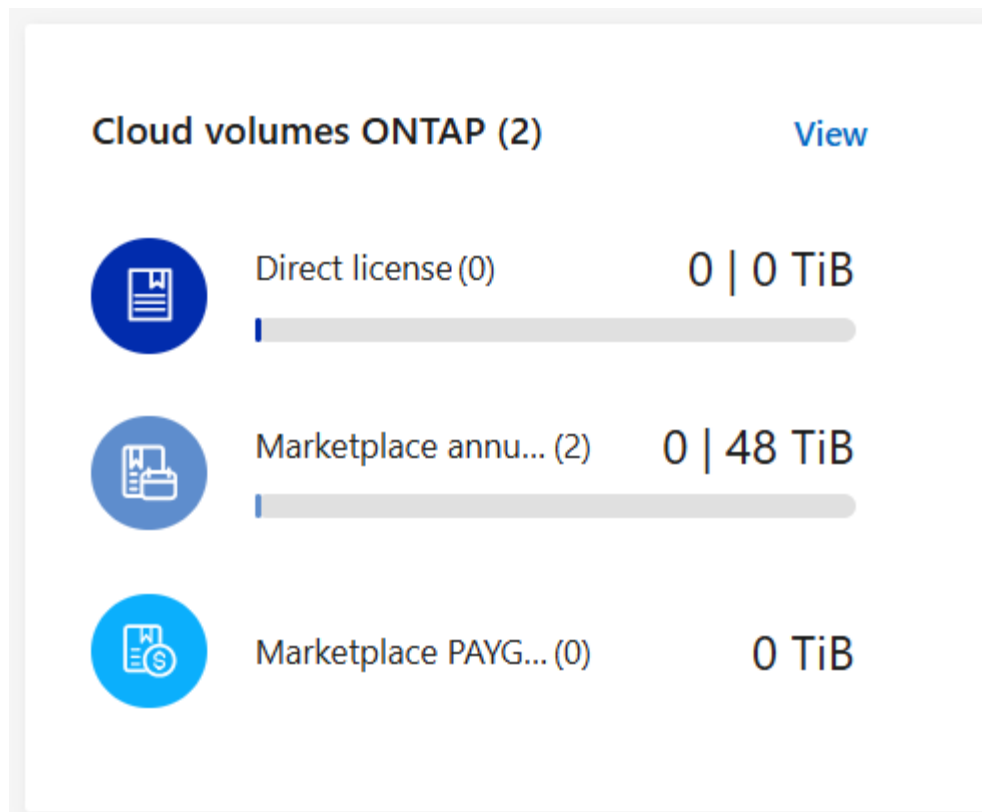
コンソールでライセンスを追加できない場合は、手動で追加する必要があります。たとえば、コンソールエージェントがインターネットにアクセスできない場所にインストールされている場合は、ライセンスを自分で追加する必要があります。 ["購入したライセンスをアカウントに追加する方法を学びます"](#)。

アカウントで消費された容量を表示する

コンソールには、アカウント内の消費済み容量の合計と、ライセンス パッケージ別の消費済み容量が表示されます。これにより、料金がどのように請求されるか、追加の容量を購入する必要があるかどうかを把握できます。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要* タブのCloud Volumes ONTAPタイルには、アカウントにプロビジョニングされている現在の容量が表示されます。



- 直接ライセンス は、NetAppアカウント内のすべてのCloud Volumes ONTAPシステムのプロビジョニングされた合計容量です。課金は、ボリューム内のローカル、使用済み、保存済み、または有効なスペースに関係なく、各ボリュームのプロビジョニングされたサイズに基づいて行われます。
- 年間契約 は、NetAppから購入したライセンス容量 (ライセンス持ち込み (BYOL) またはマーケットプレイス契約) の合計です。
- PAYGO は、クラウド マーケットプレイスのサブスクリプションを使用してプロビジョニングされた合計容量です。PAYGO による課金は、消費容量がライセンス容量よりも大きい場合、またはコンソールで利用できる BYOL ライセンスがない場合にのみ使用されます。

3. 各ライセンス パッケージの消費容量を確認するには、[表示] を選択します。
4. 購入した各パッケージ ライセンスの詳細を表示するには、[ライセンス] タブを選択します。

Essentials パッケージに表示される容量をよりよく理解するには、充電の仕組みを理解しておく必要があります。"[Essentials パッケージの料金について](#)"。

5. ライセンス消費モデル別に消費された容量を確認するには、「サブスクリプション」タブを選択します。このタブには、PAYGO ライセンスと年間契約ライセンスの両方が含まれます。

現在表示している組織に関連付けられているサブスクリプションのみが表示されます。

6. サブスクリプションに関する情報を表示しながら、テーブル内の詳細を操作できます。詳細を表示するには行を展開します。
 - 選択  テーブルに表示する列を選択します。期間と自動更新の列はデフォルトでは表示されないことに注意してください。「自動更新」列には、Azure 契約の更新情報のみが表示されます。

パッケージの詳細を表示する

Cloud Volumes ONTAPページでレガシー モードに切り替えると、パッケージごとに使用されている容量の詳細を表示できます。

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブのCloud Volumes ONTAPタイルには、アカウントにプロビジョニングされている現在の容量が表示されます。
3. 各ライセンス パッケージのプロビジョニングされた容量を確認するには、[表示] を選択します。
4. *詳細表示に切り替える*を選択します。

Overview > Cloud Volumes ONTAP

Cloud Volumes ONTAP

[Usage report](#) [Switch to advanced View](#)

Marketplace annual con... (2) 0 | 48 TiB

Marketplace PAYGO (0) 0 TiB

Direct license (0) 0 | 0 TiB

[Subscriptions \(2\)](#) [Licenses \(0\)](#)

Cloud Volumes ONTAP subscriptions (2) [Search](#) [Download](#)

Provider	Name	Type	Start date	End date	Status	
	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed	...
	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed	...

5. 確認したいパッケージの詳細を表示します。

Overview > Cloud Volumes ONTAP

Cloud Volumes ONTAP

[Switch to standard View](#)

Cloud Volumes ONTAP Packages Summary [Usage report](#)

0 TiB
Total consumed capacity

48 TiB
Total precommitted capacity

0 TiB
Total PAYGO

Essentials Secondary Single Node

0 TiB
Consumed Capacity

6 TiB
Precommitted capacity

0 TiB
PAYGO

BYOL 0 TiB

Marketplace Contracts 6 TiB

Professional

0 TiB
Consumed Capacity

6 TiB
Precommitted capacity

0 TiB
PAYGO

BYOL 0 TiB

Marketplace Contracts 6 TiB

充電方法を変更する

容量ベースのライセンスは、_パッケージ_の形式で利用できます。Cloud Volumes ONTAPシステムを作成するときは、ビジネス ニーズに応じて複数のライセンス パッケージから選択できます。システムを作成した後にニーズが変化した場合は、いつでもパッケージを変更できます。たとえば、Essentials パッケージから Professional パッケージに変更する場合があります。

"容量ベースのライセンスパッケージの詳細"。

タスク概要

- 課金方法を変更しても、NetAppから購入したライセンス (BYOL) を通じて課金されるか、クラウド プロバイダーのマーケットプレイスの従量課金制 (PAYGO) サブスクリプションを通じて課金されるかには影響しません。

コンソールは常に最初にライセンスに対して課金を試みます。ライセンスが利用できない場合は、マーケットプレイスのサブスクリプションに対して料金が請求されます。BYOL サブスクリプションをマーケットプレイス サブスクリプションに変換したり、その逆を行ったりする必要はありません。

- クラウド プロバイダーのマーケットプレイスからプライベート オファーまたは契約を結んでいる場合、契約に含まれていない課金方法に変更すると、BYOL (NetAppからライセンスを購入した場合) または PAYGO に対して課金されることになります。

手順

- 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
- *概要*タブを選択します。
- Cloud Volumes ONTAPタイルで、[表示] を選択します。
- *詳細表示に切り替える*を選択します。

Overview > Cloud Volumes ONTAP

Cloud Volumes ONTAP

Usage report ⓘ Switch to advanced View

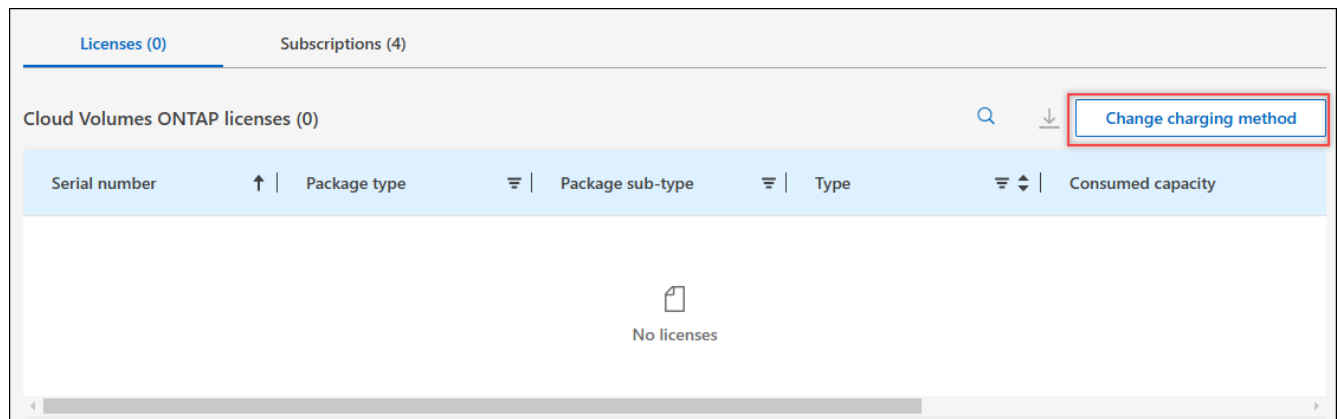
Marketplace annual con... (2) 0 | 48 TiB Marketplace PAYGO (0) 0 TiB Direct license (0) 0 | 0 TiB

Subscriptions (2) Licenses (0)

Cloud Volumes ONTAP subscriptions (2)

Provider	Name	Type	Start date	End date	Status	
	DWdemoAnnualSmall123	Annual Contract	Jan 22, 2025	Jan 21, 2026	Subscribed	⋮ ▼
	cvo_team_bycap_bynode_annual	Annual Contract	Mar 12, 2025	Mar 11, 2026	Subscribed	⋮ ▼

- *容量ベースのライセンス*テーブルまで下にスクロールし、*課金方法の変更*を選択します。



6. *課金方法の変更*ポップアップで、Cloud Volumes ONTAPシステムを選択し、新しい課金方法を選択して、パッケージ タイプを変更するとサービス料金に影響することを理解していることを確認します。
7. *充電方法の変更*を選択します。

使用状況レポートをダウンロードする

コンソールから 4 つの使用状況レポートをダウンロードできます。これらの使用状況レポートには、サブスクリプションの容量の詳細が提供され、Cloud Volumes ONTAPサブスクリプション内のリソースに対してどのように課金されるかが示されます。ダウンロード可能なレポートでは、ある時点でのデータが取得され、他のユーザーと簡単に共有できます。



以下のレポートをダウンロードできます。表示される容量値は TiB 単位です。

- 高レベルの使用状況: このレポートには次の情報が含まれます。
 - 総消費容量
 - 事前コミット済み容量合計
 - 合計BYOL容量
 - マーケットプレイス契約総容量
 - 総PAYGO容量
- * Cloud Volumes ONTAPパッケージの使用状況*: このレポートには、各パッケージに関する次の情報が含まれます。
 - 総消費容量
 - 事前コミット済み容量合計
 - 合計BYOL容量
 - マーケットプレイス契約総容量
 - 総PAYGO容量

- ストレージ **VM** の使用状況: このレポートには、課金された容量がCloud Volumes ONTAPシステムとストレージ仮想マシン (SVM) 全体でどのように内訳されているかが表示されます。この情報はレポートでのみ利用可能です。次の情報が含まれています。
 - システムIDと名前（UUIDとして表示されます）
 - クラウド
 - NetAppアカウントID
 - システム設定
 - SVM名
 - プロビジョニング済み容量
 - 充電容量のまとめ
 - マーケットプレースの請求期間
 - Cloud Volumes ONTAPパッケージまたは機能
 - 課金SaaSマーケットプレースのサブスクリプション名
 - 課金SaaSマーケットプレースサブスクリプションID
 - ワークロードの種類
- ボリュームの使用状況: このレポートには、Cloud Volumes ONTAPシステム内のボリュームごとに課金容量がどのように内訳されているかが表示されます。この情報はコンソールのどの画面でも表示されません。以下の情報が含まれます。
 - システムIDと名前（UUIDとして表示されます）
 - SVN name
 - ボリューム ID
 - ボリューム タイプ
 - ボリュームプロビジョニング容量



FlexCloneボリュームは料金が発生しないため、このレポートには含まれません。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブで、Cloud Volumes ONTAPタイルから*表示*を選択します。
3. *使用状況レポート*を選択します。

使用状況レポートがダウンロードされます。

4. レポートにアクセスするには、ダウンロードしたファイルを開きます。

NetAppコンソールからCloud Volumes ONTAPのKeystoneサブスクリプションを管理する

Cloud Volumes ONTAPでできるようにサブスクリプションを有効にし、サブスクリプションのサービス レベルのコミット済み容量の変更を要求することで、BlueXP digital

walletからKeystoneサブスクリプションを管理します。サービス レベルの追加容量を要求すると、オンプレミスのONTAPクラスターまたはCloud Volumes ONTAPシステムにさらに多くのストレージが提供されます。

NetApp Keystone は、CapEx やリースよりも OpEx を好む顧客にハイブリッド クラウド エクスペリエンスを提供する、成長に合わせて拡張できる柔軟なサブスクリプションベースのサービスです。

["Keystoneについて詳しくはこちら"](#)

アカウントを承認する

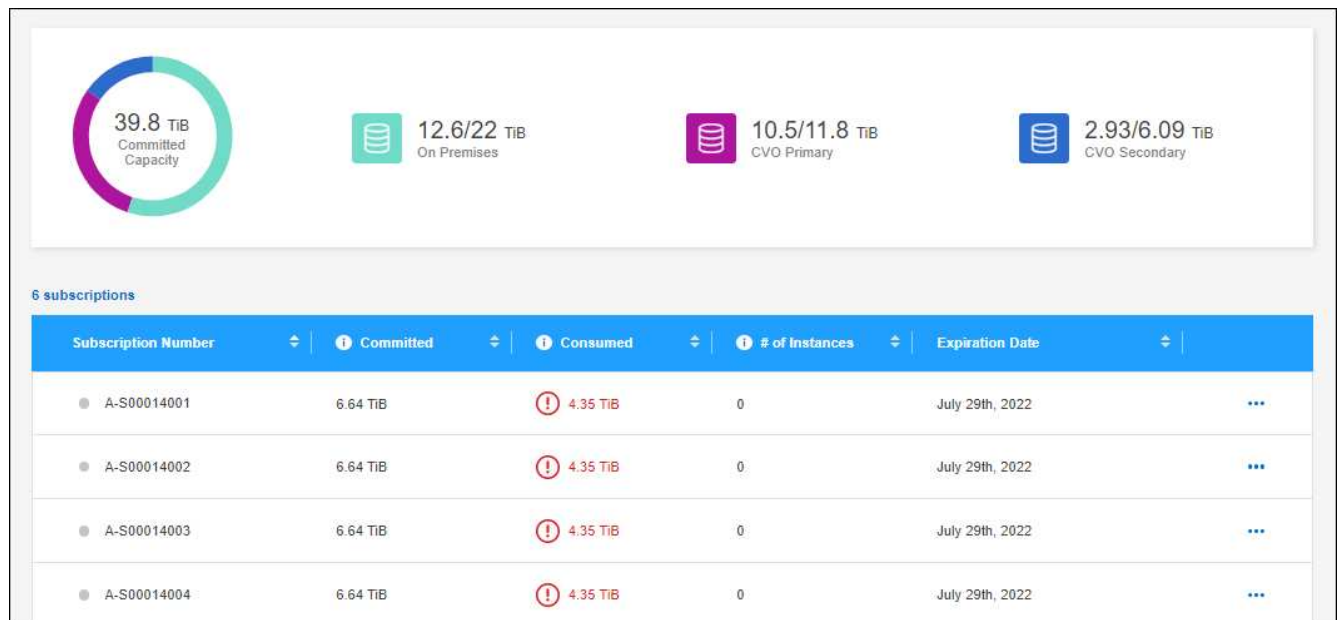
BlueXPでKeystoneサブスクリプションを使用および管理する前に、NetAppに連絡して、BlueXPユーザー アカウントにKeystoneサブスクリプションを承認してもらう必要があります。

手順

1. BlueXPナビゲーション メニューから、ガバナンス > デジタル ウォレット を選択します。
2. * Keystoneサブスクリプション* を選択します。
3. **Welcome to NetApp Keystone** ページが表示された場合は、ページに記載されているアドレスに電子メールを送信します。

NetApp の担当者が、ユーザー アカウントにサブスクリプションへのアクセスを許可して、リクエストを処理します。

4. サブスクリプションを表示するには、* Keystoneサブスクリプション* タブに戻ってください。



サブスクリプションをリンクする

NetApp がアカウントを承認すると、KeystoneサブスクリプションをCloud Volumes ONTAPで使用するためにリンクできるようになります。このアクションにより、ユーザーは新しいCloud Volumes ONTAPシステムの課金方法としてサブスクリプションを選択できるようになります。

手順

1. BlueXPナビゲーション メニューから、ガバナンス > デジタル ウォレット を選択します。
2. * Keystoneサブスクリプション* を選択します。
3. リンクしたいサブスクリプションについては、... *リンク*を選択します。

Subscription Number	Committed	Consumed	# of Instances	Expiration Date	
A-S00014001	6.64 TiB	4.35 TiB	0	July 29th, 2022	...
A-S00014002	6.64 TiB	4.35 TiB	0	July 29th, 2022	View detail and edit
A-S00014003	6.64 TiB	4.35 TiB	0	July 29th, 2022	Link

結果

サブスクリプションはBlueXP組織またはアカウントにリンクされ、Cloud Volumes ONTAP作業環境を作成するときに選択できるようになります。

コミットされた容量の増減を要求する

サブスクリプションのサービス レベルのコミット容量を変更する場合は、BlueXPから直接NetAppにリクエストを送信できます。サービス レベルの追加容量を要求すると、オンプレミスのクラスターまたはCloud Volumes ONTAPシステムにさらに多くのストレージが提供されます。

手順

1. BlueXPナビゲーション メニューから、ガバナンス > デジタル ウォレット を選択します。
2. * Keystoneサブスクリプション* を選択します。
3. 容量を調整したいサブスクリプションについては、... [詳細を表示して編集]を選択します。
4. 1 つ以上のサブスクリプションに対して要求されたコミット容量を入力します。

Subscription Modification for A-S00014001

Service Level	Current Committed Capacity	Current Consumed Capacity	Requested Committed Capacity
Extreme	0.977 TiB	0.293 TiB	Enter amount TiB
Premium	0.977 TiB	0.488 TiB	Enter amount TiB
Performance	0 TiB	0 TiB	Enter amount TiB
Standard	0.732 TiB	0.439 TiB	Enter amount TiB
Value	0.977 TiB	 0.879 TiB	Enter amount TiB
Data Tiering	0 TiB	0 TiB	Enter amount TiB
CVO Primary	1.96 TiB	 1.76 TiB	3 TiB
CVO Secondary	1.02 TiB	0.488 TiB	Enter amount TiB

Additional Information

Is there anything else we should know about your request?
Please be as descriptive as possible.

Enter your notes here

Submit Cancel

5. 下にスクロールして、リクエストの追加詳細を入力し、[送信] をクリックします。

結果

リクエストにより、NetApp のシステムに処理用のチケットが作成されます。

使用状況を監視する

BlueXP digital advisorダッシュボードを使用すると、Keystoneサブスクリプションの使用状況を監視し、レポートを生成できます。

"サブスクリプションの使用状況の監視について詳しくは、こちらをご覧ください。"

サブスクリプションのリンクを解除する

BlueXPでKeystoneサブスクリプションを使用しなくなった場合は、サブスクリプションのリンクを解除できます。既存のCloud Volumes ONTAPサブスクリプションに接続されていないサブスクリプションのみをリンク解除できることに注意してください。

手順

1. BlueXPナビゲーションメニューから、ガバナンス > デジタルウォレットを選択します。
2. * Keystone*を選択します。
3. リンクを解除したいサブスクリプションについては、... *リンク解除*を選択します。

結果

サブスクリプションはBlueXP組織またはアカウントからリンク解除され、Cloud Volumes ONTAP作業環境を作成するときに選択できなくなります。

Cloud Volumes ONTAPのノードベースのライセンスを管理する

NetAppコンソールでノードベースのライセンスを管理して、各Cloud Volumes ONTAPシステムに必要な容量を持つ有効なライセンスがあることを確認します。

ノードベースのライセンスは、以前の世代のライセンスモデルです (新規顧客には利用できません)。

- NetAppから購入したライセンスを持参 (BYOL)
- クラウド プロバイダーのマーケットプレイスから時間単位の従量課金制 (PAYGO) サブスクリプションを購入する

NetAppコンソールからノードベースのCloud Volumes ONTAPライセンスを管理できます。

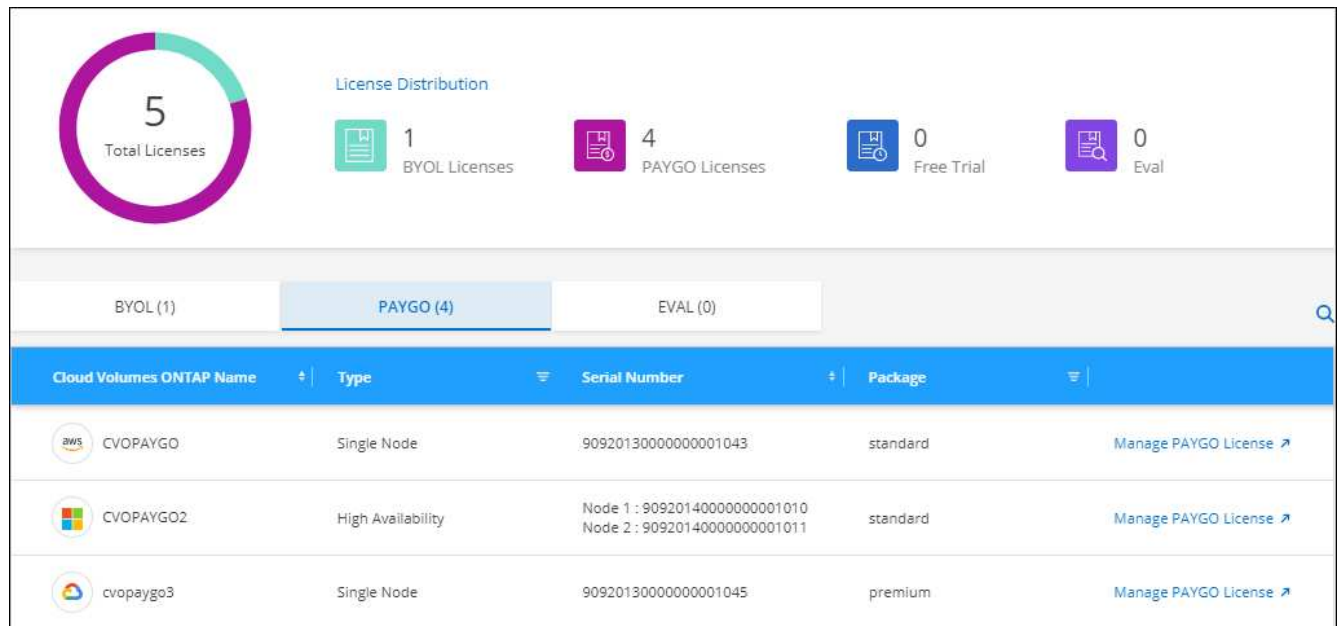
["Cloud Volumes ONTAPライセンスの詳細"](#)。

PAYGOライセンスの管理

「ライセンスとサブスクリプション」メニューでは、シリアル番号や PAYGO ライセンスの種類など、各 PAYGO Cloud Volumes ONTAPシステムの詳細を表示できます。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブを選択します。
3. Cloud Volumes ONTAPタイルで、[表示] を選択します。
4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. [PAYGO]をクリックします。
6. 各 PAYGO ライセンスの詳細を表で表示します。



- 必要に応じて、「**PAYGO** ライセンスの管理」をクリックして、PAYGO ライセンスを変更するか、インスタンス タイプを変更します。

BYOLライセンスの管理

システム ライセンスと追加容量ライセンスを追加および削除することで、NetAppから直接購入したライセンスを管理します。



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"](#)。

割り当てられていないライセンスを追加する

新しいCloud Volumes ONTAPシステムを作成するときにライセンスを選択できるように、ノードベースのライセンスをコンソールに追加します。コンソールはこれらのライセンスを「未割り当て」として識別します。

手順

- 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
- *概要*タブを選択します。
- Cloud Volumes ONTAPタイルで、[表示] を選択します。
- ドロップダウンから*ノードベースのライセンス*を選択します。
- *未割り当て*をクリックします。
- *未割り当てのライセンスの追加*をクリックします。
- ライセンスのシリアル番号を入力するか、ライセンス ファイルをアップロードします。

ライセンス ファイルをまだお持ちでない場合は、以下のセクションを参照してください。

- *ライセンスの追加*をクリックします。

結果

コンソールがライセンスを追加します。ライセンスは、新しいCloud Volumes ONTAPシステムに関連付けるまで、未割り当てとして識別されます。その後、ライセンスは **ライセンスとサブスクリプション** の **BYOL** タブに移動します。

Exchangeの未割り当てノードベースライセンス

使用していないCloud Volumes ONTAPの未割り当てのノードベース ライセンスがある場合は、そのライセンスをNetApp Backup and Recovery ライセンス、 NetApp Data Classification ライセンス、またはNetApp Cloud Tiering ライセンスに変換して交換できます。

ライセンスを交換すると、 Cloud Volumes ONTAPライセンスが取り消され、サービスに対してドル相当のライセンスが作成されます。

- Cloud Volumes ONTAP HAペアのライセンスは51 TiBの直接ライセンスに変換されます
- Cloud Volumes ONTAPシングルノードのライセンスは 32 TiB の直接ライセンスに変換されます

変換されたライセンスの有効期限は、 Cloud Volumes ONTAPライセンスと同じになります。

"ノードベースのライセンスを交換する方法のチュートリアルを表示します。"

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブを選択します。
3. Cloud Volumes ONTAPタイルで、[表示] を選択します。
4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. *未割り当て*をクリックします。
6. *ライセンスの交換*をクリックします。

BYOL (14)		Eval (2)		Unassigned (3)		PAYGO (6)			
Serial Number		Type		Cloud Provider		License Expiry		Status	
012345678901234567890		Single Node		All Providers		April 20, 2022		Unassigned	
012345678901234567891		Single Node		Azure		April 20, 2022		Unassigned	
012345678901234567892		Single Node		AWS		January 1, 2022		Exchanged to Cloud Tiering on August 1, 2021	

7. ライセンスを交換するサービスを選択します。
8. プロンプトが表示されたら、HA ペアの追加ライセンスを選択します。
9. 法的同意書を読み、「同意する」をクリックします。

結果

コンソールは、割り当てられていないライセンスを選択したサービスに変換します。新しいライセンスは、[データ サービス ライセンス] タブで確認できます。

システムライセンスファイルを取得する

ほとんどの場合、コンソールはNetAppサポート サイトのアカウントを使用してライセンス ファイルを自動的に取得できます。ただし、それができない場合は、ライセンス ファイルを手動でアップロードする必要があります。ライセンス ファイルがない場合は、netapp.com から取得できます。

手順

1. に行く ["NetApp License File Generator"](#) NetAppサポート サイトの認証情報を使用してログインします。
2. パスワードを入力し、製品を選択し、シリアル番号を入力し、プライバシー ポリシーを読んで同意したことを確認してから、[送信] をクリックします。

例

License Generator

The following fields are pre-populated based on the NetApp SSO login provided.
To download the corresponding NetApp license file, re-enter your SSO password along with the correct Product Line and Product Serial number.

First Name: Ben

Last Name:

Company: Network Appliance, Inc

Email Address:

Username:

Product Line*

- ONTAP Select - Standard
- ONTAP Select - Premium
- ONTAP Select - Premium XL
- Cloud Volumes ONTAP for AWS (single node)
- Cloud Volumes ONTAP for AWS (HA)
- Cloud Volumes ONTAP for GCP (single node or HA)
- Cloud Volumes ONTAP for Microsoft Azure (single node)
- Cloud Volumes ONTAP for Microsoft Azure (HA)
- Service Level Manager - SLO Advanced
- StorageGRID Webscale
- StorageGRID WhiteBox
- SnapCenter Standard (capacity-based)

☐ I have read NetApp's new **Global Data Privacy Policy** and I agree to the terms.

3. serialnumber.NLF JSON ファイルを電子メールで受け取るか、直接ダウンロードするかを選択します。

システムライセンスを更新する

NetApp の担当者に連絡して BYOL サブスクリプションを更新すると、コンソールはNetAppから新しいライセンスを自動的に取得し、Cloud Volumes ONTAPシステムにインストールします。コンソールが安全なインターネット接続を介してライセンス ファイルにアクセスできない場合は、自分でファイルを取得し、手動でファイルをアップロードすることができます。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要* タブを選択します。

3. Cloud Volumes ONTAPタイルで、[表示] を選択します。
4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. **BYOL** タブで、Cloud Volumes ONTAPシステムの詳細を展開します。
6. システム ライセンスの横にあるアクション メニューをクリックし、*ライセンスの更新*を選択します。
7. ライセンス ファイル (HA ペアがある場合は複数のファイル) をアップロードします。
8. *ライセンスの更新*をクリックします。

結果

コンソールは、Cloud Volumes ONTAPシステムのライセンスを更新します。

追加容量ライセンスの管理

Cloud Volumes ONTAP BYOL システムの追加容量ライセンスを購入して、BYOL システム ライセンスで提供される 368 TiB を超える容量を割り当てることができます。たとえば、最大 736 TiB の容量をCloud Volumes ONTAPに割り当てるために、追加のライセンス容量を 1 つ購入することができます。または、最大 1.4 PiB を得るために、追加容量ライセンスを 3 つ購入することもできます。

単一ノードシステムまたはHAペアに対して購入できるライセンスの数に制限はありません。

容量ライセンスを追加する

コンソールの右下にあるチャット アイコンからお問い合わせいただき、追加容量ライセンスを購入してください。ライセンスを購入したら、それをCloud Volumes ONTAPシステムに適用できます。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブを選択します。
3. Cloud Volumes ONTAPタイルで、[表示] を選択します。
4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. **BYOL** タブで、Cloud Volumes ONTAPシステムの詳細を展開します。
6. *容量ライセンスの追加*をクリックします。
7. シリアル番号を入力するか、ライセンス ファイル (HA ペアがある場合は複数のファイル) をアップロードします。
8. *容量ライセンスの追加*をクリックします。

容量ライセンスの更新

追加容量ライセンスの期間を延長した場合は、コンソールでライセンスを更新する必要があります。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブを選択します。
3. Cloud Volumes ONTAPタイルで、[表示] を選択します。

4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. **BYOL** タブで、Cloud Volumes ONTAPシステムの詳細を展開します。
6. 容量ライセンスの横にあるアクション メニューをクリックし、[ライセンスの更新] を選択します。
7. ライセンス ファイル (HA ペアがある場合は複数のファイル) をアップロードします。
8. *ライセンスの更新*をクリックします。

容量ライセンスを削除する

追加容量ライセンスの有効期限が切れて使用されなくなった場合は、いつでも削除できます。

手順

1. 左側のナビゲーション ペインから、管理 > ライセンスとサブスクリプション を選択します。
2. *概要*タブを選択します。
3. Cloud Volumes ONTAPタイルで、[表示] を選択します。
4. ドロップダウンから*ノードベースのライセンス*を選択します。
5. **BYOL** タブで、Cloud Volumes ONTAPシステムの詳細を展開します。
6. 容量ライセンスの横にあるアクション メニューをクリックし、[ライセンスの削除] を選択します。
7. *削除*をクリックします。

PAYGOとBYOL間の変更

システムを PAYGO ノード単位ライセンスから BYOL ノード単位ライセンス (およびその逆) に変換することはサポートされていません。従量課金制サブスクリプションと BYOL サブスクリプションを切り替える場合は、新しいシステムをデプロイし、既存のシステムから新しいシステムにデータを複製する必要があります。

手順

1. 新しいCloud Volumes ONTAPシステムを作成します。
2. 複製する必要があるボリュームごとに、システム間で 1 回限りのデータ レプリケーションを設定します。

["システム間でデータを複製する方法を学ぶ"](#)

3. 元のシステムを削除して、不要になったCloud Volumes ONTAPシステムを終了します。

["Cloud Volumes ONTAPシステムを削除する方法を学ぶ"](#)。

関連リンク

リンク: ["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"](#)

ボリュームとLUNの管理

Cloud Volumes ONTAPシステムにFlexVol volumeを作成する

最初のCloud Volumes ONTAPシステムを起動した後にさらにストレージが必要な場合は、NetAppコンソールから NFS、CIFS、または iSCSI 用の新しいFlexVolボリュームを作成できます。

新しいボリュームを作成するには、いくつかの方法があります。

- 新しいボリュームの詳細を指定し、基礎となるデータ集計をコンソールで処理できるようにします。 [詳細情報](#)
- 選択したデータ アグリゲート上にボリュームを作成します。 [詳細情報](#)
- HA 構成の 2 番目のノードにボリュームを作成します。 [詳細情報](#)

開始する前に

ボリュームのプロビジョニングに関する注意事項:

- 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り、管理の手間がかかりません。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](#)"。
- ONTAP System Manager またはONTAP CLI から追加の LUN を作成できます。
- AWS で CIFS を使用する場合は、DNS と Active Directory を設定する必要があります。詳細については、"[Cloud Volumes ONTAP for AWS のネットワーク要件](#)"。
- Cloud Volumes ONTAP構成がAmazon EBS Elastic Volumes機能をサポートしている場合は、"[ボリュームを作成すると何が起こるかについて詳しく知る](#)"。

ボリュームの作成

ボリュームを作成する最も一般的な方法は、必要なボリュームの種類を指定し、コンソールにディスクの割り当てを処理させることです。ただし、ボリュームを作成する特定のアグリゲートを選択することもできます。

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、FlexVol volumeをプロビジョニングするCloud Volumes ONTAPシステムの名前をダブルクリックします。

コンソールでディスク割り当てを処理させてボリュームを作成することも、ボリュームの特定のアグリゲートを選択することもできます。Cloud Volumes ONTAPシステム上のデータ アグリゲートについて十分に理解している場合にのみ、特定のアグリゲートを選択することをお勧めします。

あらゆる集合体

特定の骨材

- a. *集計*タブで、必要な集計に移動し、...アイコン。
- b. *ボリュームの追加*を選択します。

Aggregate (1)

The screenshot shows the 'Aggregate (1)' interface. At the top, there is a header bar with a purple icon, the name 'aggr1', a green 'Online' status indicator, and a three-dot menu icon. Below the header is a table with aggregate details. The table has two main sections: 'INFO' and 'Capacity'. The 'INFO' section includes 'Disk Type' (Premium SSD v2), 'Disks' (1), 'Volumes' (2), and 'Blob Tiering' (Enabled). The 'Capacity' section includes 'Provisioned', 'Disk Used', and 'Blob Used'. A context menu is open over the 'Add Volume' option, showing options: 'View aggregate details', 'Add Volume', 'Add Azure Disks', and 'Delete'.

INFO		Capacity	
Disk Type	Premium SSD v2	Provisioned	
Disks	1	Disk Used	
Volumes	2	Blob Used	
Blob Tiering	Enabled		

3. ウィザードの手順に従ってボリュームを作成します。

- a. 詳細、保護、タグ: ボリュームに関する基本的な詳細を入力し、スナップショット ポリシーを選択します。

このページの一部のフィールドは説明不要です。次のリストでは、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
ボリューム名	新しいボリュームに入力できる識別可能な名前。
ボリューム サイズ	入力できる最大サイズは、シン プロビジョニングを有効にするかどうかによって大きく異なります。シン プロビジョニングを有効にすると、現在使用可能な物理ストレージよりも大きなボリュームを作成できます。
ストレージ VM (SVM)	ストレージ VM は、ONTAP内で実行され、クライアントにストレージおよびデータ サービスを提供する仮想マシンです。これは SVM または vserver として知られているかもしれません。Cloud Volumes ONTAPはデフォルトで1つのストレージ VM で構成されていますが、一部の構成では追加のストレージ VM がサポートされます。新しいボリュームのストレージ VM を指定できます。

フィールド	説明
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)。

- b. プロトコル: ボリュームのプロトコル (NFS、CIFS、または iSCSI) を選択し、必要な情報を入力します。

CIFS を選択し、サーバーが設定されていない場合は、次へ をクリックした後に、コンソールで CIFS 接続を設定するように求められます。

["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"](#)。

次のセクションでは、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。説明はプロトコル別にまとめられています。

NFS

アクセス制御

ボリュームをクライアントが利用できるようにするには、カスタム エクスポート ポリシーを選択します。

エクスポート ポリシー

ボリュームにアクセスできるサブネット内のクライアントを定義します。デフォルトでは、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。

CIFS

権限とユーザー/グループ

ユーザーおよびグループの SMB 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。

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。

Google Managed Active Directory を構成している場合、デフォルトでは 169.254.169.254 IP アドレスを使用して AD にアクセスできます。

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。

- AWS Managed Microsoft AD をCloud Volumes ONTAPの AD サーバーとして設定するには、このフィールドに **OU=Computers,OU=corp** と入力します。
- 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** と入力します。 <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"]
- Google Managed Microsoft AD 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=Computers,OU=Cloud** と入力します。 https://cloud.google.com/managed-microsoft-ad/docs/manage-active-directory-objects#organizational_units["Google Cloud ドキュメント: Google Managed Microsoft AD の"]

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。詳細については、"[NetAppコンソール自動化ドキュメント](#)"。

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。

iSCSI

LUN

iSCSI ストレージ ターゲットは LUN (論理ユニット) と呼ばれ、標準のブロック デバイスとしてホストに提供されます。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り、管理の手間がかかりません。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](#)"。

イニシエーターグループ

イニシエーター グループ (igroup) は、ストレージ システム上の指定された LUN にアクセスできるホストを指定します。

ホストイニシエーター (IQN)

iSCSIターゲットは、標準のイーサネット ネットワーク アダプタ (NIC) 、ソフトウェア イニシエータを搭載した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 (CNA) 、または専用のホスト バス アダプタ (HBA) を介してネットワークに接続し、iSCSI修飾名 (IQN) で識別されます。

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

- "[AWS でのシステムのサイズ設定](#)"
- "[Azure でのシステムのサイズ設定](#)"
- "[Google Cloud でのシステムのサイズ設定](#)"

4. 使用プロファイルと階層化ポリシー: ボリュームのストレージ効率機能を有効にするか無効にするかを選択し、"[ボリューム階層化ポリシー](#)"。

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。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。

5. 確認: ボリュームの詳細を確認し、[追加] をクリックします。

結果

コンソールは、Cloud Volumes ONTAPシステムにボリュームを作成します。

HA構成の2番目のノードにボリュームを作成する

デフォルトでは、コンソールは HA 構成の最初のノードにボリュームを作成します。両方のノードがクライアントにデータを提供するアクティブ/アクティブ構成が必要な場合は、2 番目のノードにアグリゲートとボリュームを作成する必要があります。

手順

1. 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、アグリゲートを管理するCloud Volumes ONTAPシステムの名前をダブルクリックします。
3. 「集計」タブで、「集計の追加」をクリックし、集計を作成します。

Aggregates Summary

1 Total Aggregates

1 Aggregates with Tiering

0 Aggregates without Tiering

1 Allocated Disks

Aggregate (1)

aggr1 Online

INFO		Capacity	
Disk Type	Premium SSD v2	Provisioned size	907.18 GiB
Disks	1	Disk Used	1.15 GiB
Volumes	2	Blob Used	0 GiB
Blob Tiering	Enabled		

Add Aggregate

4. ホーム ノードでは、HA ペアの 2 番目のノードを選択します。
5. コンソールがアグリゲートを作成したら、それを選択し、「ボリュームの作成」をクリックします。
6. 新しいボリュームの詳細を入力し、「作成」をクリックします。

結果

コンソールは、HA ペアの 2 番目のノードにボリュームを作成します。



複数の AWS アベイラビリティゾーンにデプロイされた HA ペアの場合、ボリュームが存在するノードのフローティング IP アドレスを使用して、ボリュームをクライアントにマウントする必要があります。

ボリュームを作成した後

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、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 を使用する必要があります。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。

Cloud Volumes ONTAPシステム上のボリュームを管理する

NetAppコンソールでボリュームと CIFS サーバーを管理できます。容量の問題を回避するためにボリュームを移動することもできます。

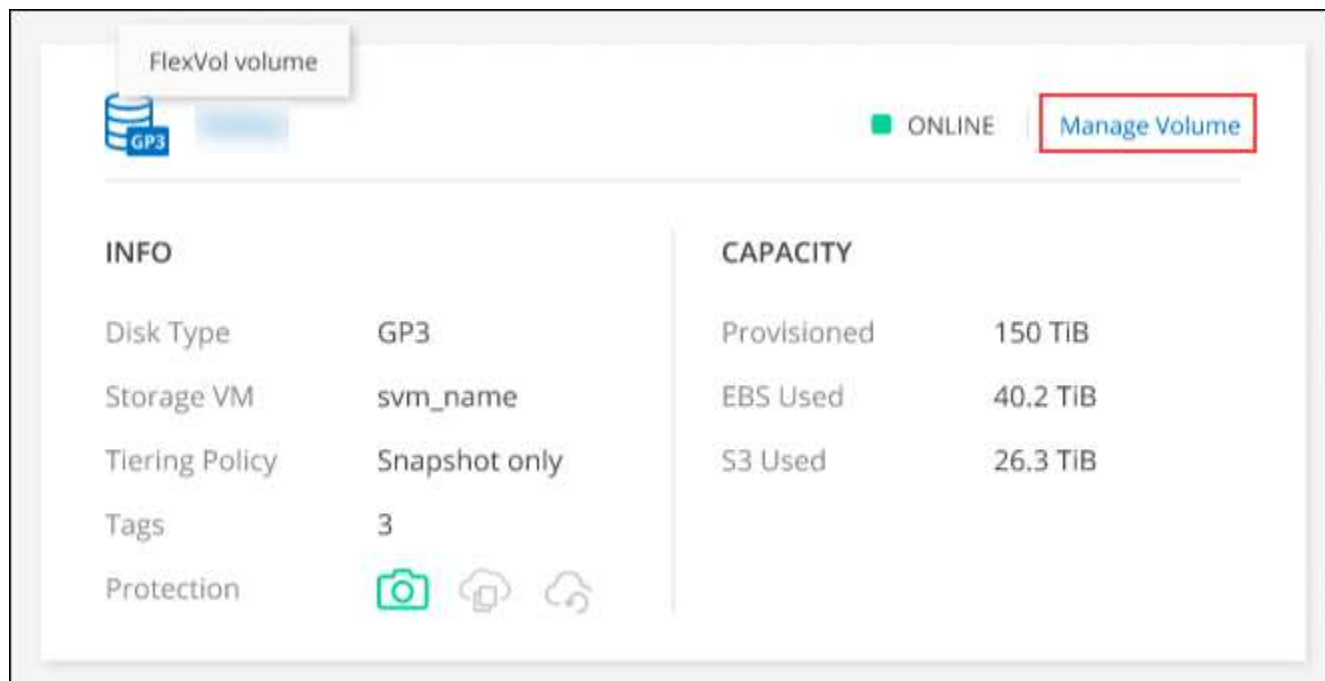
ボリュームは、NetAppコンソールの標準ビューで管理することも、コンソールに組み込まれているONTAP System Manager を使用して管理し、高度なボリューム管理を行うこともできます。標準ビューでは、ボリュームを変更するためのオプションが限定的に提供されます。System Manager は、クローン作成、サイズ変更、ランサムウェア対策、分析、保護、アクティビティ追跡の設定変更、階層間でのボリュームの移動など、高度なレベルの管理機能を提供します。詳細については、"[System Manager を使用してCloud Volumes ONTAPを管理する](#)"。

ボリュームを管理する

コンソールの標準ビューを使用すると、ストレージのニーズに応じてボリュームを管理できます。ボリュームを表示、編集、複製、復元、削除できます。

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、ボリュームを管理するCloud Volumes ONTAPシステムをダブルクリックします。
3. *ボリューム*タブを選択します。



4. 必要なボリューム タイルで、[ボリュームの管理] をクリックします。

Task	アクション
ボリュームに関する情報を表示する	ボリュームの管理パネルのボリュームアクションで、*ボリュームの詳細の表示*をクリックします。
NFSマウントコマンドを取得する	a. ボリュームの管理パネルのボリュームアクションで、*マウントコマンド*をクリックします。 b. *コピー*をクリックします。
ボリュームをクローニングする	a. ボリュームの管理パネルのボリュームアクションで、*ボリュームの複製*をクリックします。 b. 必要に応じてクローン名を変更し、「クローン」をクリックします。 このプロセスにより、FlexCloneボリュームが作成されます。FlexCloneボリュームは、メタデータに少量のスペースを使用し、データが変更または追加された場合にのみ追加のスペースを消費するため、スペース効率に優れた書き込み可能なポイントインタイム コピーです。 FlexCloneボリュームの詳細については、 "ONTAP 9 論理ストレージ管理ガイド" 。

Task	アクション
ボリュームを編集する（読み取り/書き込みボリュームのみ）	a. ボリューム管理パネルのボリュームアクションで、*ボリューム設定の編集*をクリックします。 b. ボリュームのスナップショット ポリシー、NFS プロトコル バージョン、NFS アクセス制御リスト (エクスポート ポリシー)、または共有アクセス許可を変更し、[適用] をクリックします。  カスタム スナップショット ポリシーが必要な場合は、ONTAP System Manager を使用して作成できます。
ボリュームを削除する	a. ボリュームの管理パネルのボリュームアクションで、*ボリュームの削除*をクリックします。 b. 「ボリュームの削除」ウィンドウで、削除するボリュームの名前を入力します。 c. もう一度「削除」をクリックして確認します。
オンデマンドでスナップショットコピーを作成する	a. [ボリュームの管理] パネルの [保護アクション] で、[スナップショット コピーの作成] をクリックします。 b. 必要に応じて名前を変更し、「作成」をクリックします。
スナップショットコピーから新しいボリュームにデータを復元する	a. [ボリュームの管理] パネルの [保護アクション] で、[スナップショット コピーからの復元] をクリックします。 b. スナップショット コピーを選択し、新しいボリュームの名前を入力して、[復元] をクリックします。
基盤となるディスクの種類を変更する	a. 「ボリュームの管理」パネルの「詳細アクション」で、「ディスク タイプの変更」をクリックします。 b. ディスクの種類を選択し、[変更] をクリックします。  コンソールは、選択したディスク タイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。
階層化ポリシーを変更する	a. 「ボリュームの管理」パネルの「詳細アクション」で、「階層化ポリシーの変更」をクリックします。 b. 別のポリシーを選択し、「変更」をクリックします。  コンソールは、階層化されている選択されたディスク タイプを使用する既存のアグリゲートにボリュームを移動するか、ボリュームの新しいアグリゲートを作成します。

Task	アクション
ボリュームを削除する	a. ボリュームを選択し、「削除」をクリックします。 b. ダイアログにボリュームの名前を入力します。 c. もう一度「削除」をクリックして確認します。

ボリュームのサイズを変更する

デフォルトでは、ボリュームの容量が不足すると、ボリュームは自動的に最大サイズまで拡張されます。デフォルト値は 1,000 です。つまり、ボリュームのサイズは 11 倍まで拡張できます。この値は、コンソールエージェントの設定で構成できます。

ボリュームのサイズを変更する必要がある場合は、コンソールのONTAP System Manager から変更できます。

手順

1. ONTAP System Manager を通じてボリュームのサイズを変更するには、System Manager ビューをクリックします。。 ["始め方"](#)。
2. 左側のナビゲーション メニューから、*ストレージ> ボリューム*を選択します。
3. ボリュームのリストから、サイズを変更するボリュームを特定します。
4. オプションアイコンをクリックします .
5. *サイズ変更*を選択します。
6. *ボリュームのサイズ変更*画面で、必要に応じて容量とスナップショット予約率を編集します。既存の使用可能なスペースと変更された容量を比較できます。
7. *保存*をクリックします。

×

Resize volume

CAPACITY

25

GiB

SNAPSHOT RESERVE %

1

Existing

DATA SPACE

20 GiB

SNAPSHOT RESERVE

0 Bytes

New

DATA SPACE

24.75 GiB

SNAPSHOT RESERVE

256 MiB

Cancel

Save

ボリュームのサイズを変更するときは、システムの容量制限を必ず考慮してください。に行く ["Cloud Volumes ONTAPリリースノート"](#)詳細についてはこちらをご覧ください。

CIFSサーバーを変更する

DNS サーバーまたは Active Directory ドメインを変更する場合は、クライアントにストレージを引き続き提供できるように、Cloud Volumes ONTAPの CIFS サーバーを変更する必要があります。

手順

- Cloud Volumes ONTAPシステムの 概要 タブで、右側のパネルの下にある 機能 タブをクリックします。
- CIFS セットアップ フィールドの下にある 鉛筆アイコン をクリックして、CIFS セットアップ ウィンドウを表示します。
- CIFS サーバーの設定を指定します。

Task	アクション
ストレージVM（SVM）を選択	Cloud Volume ONTAPストレージ仮想マシン (SVM) を選択すると、設定されている CIFS 情報が表示されます。
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。

Task	アクション
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。リストされている DNS サーバーには、CIFS サーバーが参加するドメインの Active Directory LDAP サーバーとドメイン 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。ifdef::gcp[] Google マネージド Active Directory を設定している場合、AD にはデフォルトで 169.254.169.254 の IP アドレスでアクセスできます。endif::gcp[]
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。
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。 • AWS Managed Microsoft AD をCloud Volumes ONTAPの AD サーバーとして設定するには、このフィールドに OU=Computers,OU=corp と入力します。 • 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 と入力します。"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" • Google Managed Microsoft AD 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=Computers,OU=Cloud と入力します。"Google Cloud ドキュメント: Google Managed Microsoft AD の組織単位"

4. *設定*をクリックします。

結果

Cloud Volumes ONTAP は、変更内容に応じて CIFS サーバーを更新します。

ボリュームの移動

容量使用率、パフォーマンス向上、およびサービス レベル アグリーメントの達成のためにボリュームを移動します。

ONTAP System Manager でボリュームを移動するには、ボリュームと移動先のアグリゲートを選択し、ボリューム移動操作を開始し、オプションでボリューム移動ジョブを監視します。System Manager を使用すると、ボリューム移動操作は自動的に終了します。

手順

1. ONTAP System Manager またはONTAP CLI を使用して、ボリュームをアグリゲートに移動します。

ほとんどの場合、System Manager を使用してボリュームを移動できます。

手順については、["ONTAP 9 ボリューム移動エクスペスガイド"](#)。

コンソールに「アクションが必要です」というメッセージが表示されたらボリュームを移動します

コンソールには、容量の問題を回避するためにボリュームの移動が必要であるが、問題を自分で修正する必要があることを示すアクションが必要なメッセージが表示される場合があります。このような場合は、問題を修正する方法を特定し、1 つ以上のボリュームを移動する必要があります。



アグリゲートの使用容量が 90% に達すると、コンソールにこれらのアクションが必要なメッセージが表示されます。データ階層化が有効になっている場合、アグリゲートの使用容量が 80% に達するとメッセージが表示されます。デフォルトでは、データ階層化用に 10% の空き領域が予約されています。["データ階層化の空き領域比率について詳しく見る"](#)。

手順

1. [\[容量の問題を修正する方法を特定する\]](#)。
2. 分析に基づいて、容量の問題を回避するためにボリュームを移動します。
 - [\[容量の問題を回避するためにボリュームを別のシステムに移動する\]](#)。
 - [\[容量の問題を回避するためにボリュームを別のアグリゲートに移動する\]](#)。

容量の問題を修正する方法を特定する

コンソールが容量の問題を回避するためにボリュームを移動するための推奨事項を提供できない場合は、移動する必要があるボリュームを特定し、それらを同じシステム上の別のアグリゲートに移動するべきか、別のシステムに移動するべきかを識別する必要があります。

手順

1. 容量制限に達したアグリゲートを識別するには、「アクションが必要」メッセージの詳細情報を表示します。

たとえば、詳細情報には次のような内容が表示されます: アグリゲート aggr1 が容量制限に達しました。
2. アグリゲートから移動する 1 つ以上のボリュームを特定します。
 - a. Cloud Volumes ONTAPシステムで、*Aggregates タブ*をクリックします。
 - b. 集計タイルで、...アイコンをクリックし、[集計の詳細を表示] をクリックします。
 - c. *アグリゲートの詳細*画面の*概要*タブで、各ボリュームのサイズを確認し、アグリゲートから移動する 1 つ以上のボリュームを選択します。

将来的に追加の容量の問題を回避するために、アグリゲート内のスペースを解放するのに十分な大きさのボリュームを選択する必要があります。

Aggregate Details	
aggr1	
Overview	Capacity Allocation
State	online
Home Node	storage01
Encryption Type	cloudEncrypted
Volumes	2 ^
	new_storage01 (1 GiB)
	storage01 (500 GiB)

3. システムがディスク制限に達していない場合は、ボリュームを同じシステム上の既存のアグリゲートまたは新しいアグリゲートに移動する必要があります。

詳細については、[容量の問題を回避するためにボリュームを別のアグリゲートに移動する](#)。

4. システムがディスク制限に達した場合は、次のいずれかを実行します。

- 未使用のボリュームを削除します。
- ボリュームを再配置してアグリゲート上のスペースを解放します。

詳細については、[容量の問題を回避するためにボリュームを別のアグリゲートに移動する](#)。

- 2 つ以上のボリュームを、スペースのある別のシステムに移動します。

詳細については、[容量の問題を回避するためにボリュームを別のアグリゲートに移動する](#)。

容量の問題を回避するためにボリュームを別のシステムに移動する

容量の問題を回避するために、1 つ以上のボリュームを別のCloud Volumes ONTAPシステムに移動できます。システムがディスク制限に達した場合は、これを実行する必要があるかもしれません。

タスク概要

次の「アクションが必要」メッセージを修正するには、このタスクの手順に従います。

容量の問題を回避するにはボリュームを移動する必要がありますが、システムがディスク制限に達したため、コンソールはこのアクションを実行できません。

手順

1. 使用可能な容量を持つCloud Volumes ONTAPシステムを特定するか、新しいシステムを展開します。
2. ソース システムをターゲット システムにドラッグ アンド ドロップして、ボリュームの 1 回限りのデータ レプリケーションを実行します。

詳細については、["システム間でのデータの複製"](#)。

3. 「レプリケーション ステータス」 ページに移動し、 SnapMirror関係を解除して、複製されたボリューム をデータ保護ボリュームから読み取り/書き込みボリュームに変換します。

詳細については、["データ複製スケジュールと関係の管理"](#)。

4. データ アクセス用にボリュームを構成します。

データアクセス用の宛先ボリュームの設定については、["ONTAP 9 ボリューム ディザスタ リカバリ エク スプレス ガイド"](#)。

5. 元のボリュームを削除します。

詳細については、["ボリュームを管理する"](#)。

容量の問題を回避するためにボリュームを別のアグリゲートに移動する

容量の問題を回避するために、1 つ以上のボリュームを別のアグリゲートに移動できます。

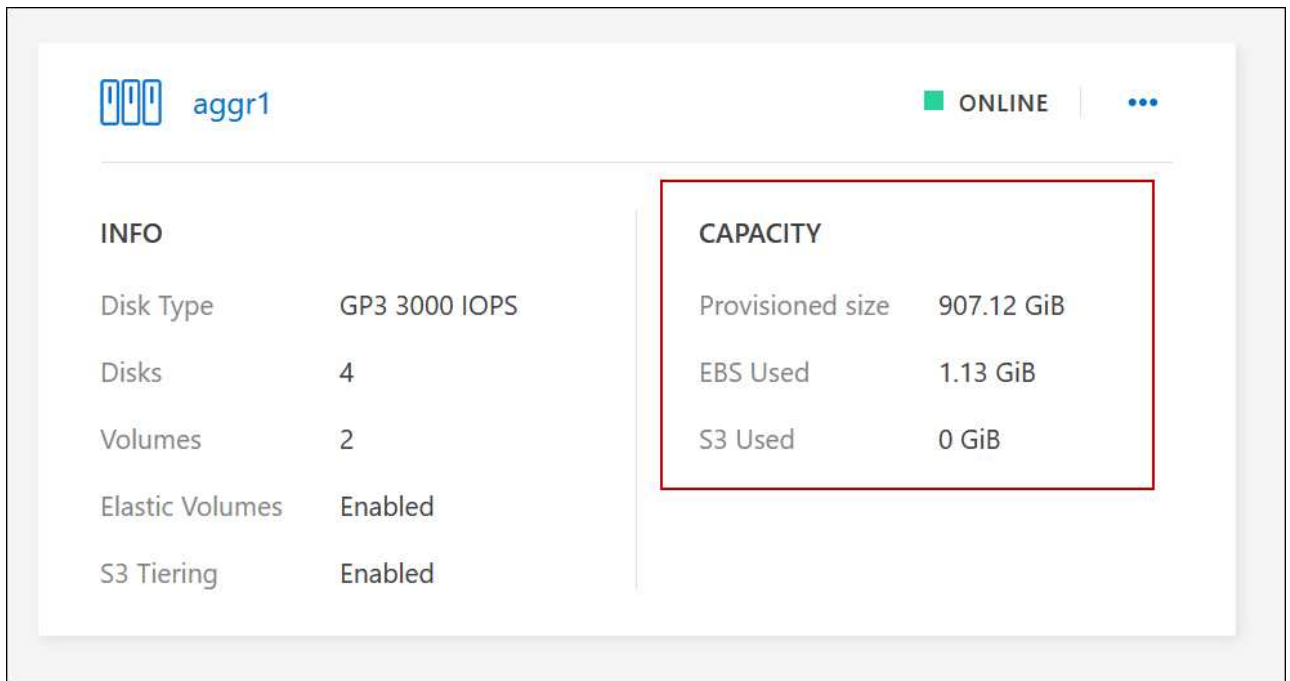
タスク概要

次の「アクションが必要」メッセージを修正するには、このタスクの手順に従います。

容量の問題を回避するには 2 つ以上のボリュームを移動する必要がありますが、コンソールではこのアクションを自動的に実行することはできません。

手順

1. 既存のアグリゲートに、移動する必要があるボリュームに使用可能な容量があるかどうかを確認します。
 - a. Cloud Volumes ONTAPシステムで、***Aggregates タブ***をクリックします。
 - b. 必要な集計タイルで、**...**アイコンをクリックし、次に***集計の詳細を表示***をクリックして、使用可能な容量（プロビジョニングされたサイズから使用された集計容量を差し引いたもの）を表示します。



2. 必要に応じて、既存のアグリゲートにディスクを追加します。
 - a. 集計を選択し、...アイコン > ディスクの追加。
 - b. 追加するディスクの数を選択し、「追加」をクリックします。
3. 使用可能な容量を持つアグリゲートがない場合は、新しいアグリゲートを作成します。

詳細については、["集計の作成"](#)。

4. ONTAP System Manager または ONTAP CLI を使用して、ボリュームをアグリゲートに移動します。
5. ほとんどの場合、System Manager を使用してボリュームを移動できます。

手順については、["ONTAP 9 ボリューム移動エクスペスガイド"](#)。

ボリューム移動が遅くなる理由

Cloud Volumes ONTAPに次のいずれかの条件が当てはまる場合、ボリュームの移動に予想よりも時間がかかることがあります。

- ボリュームはクローンです。
- ボリュームはクロンの親です。
- ソースまたは宛先アグリゲートには、単一のスループット最適化 HDD (st1) ディスクがあります。
- 集約の 1 つは、オブジェクトに古い命名スキームを使用します。両方の集約は同じ名前形式を使用する必要があります。

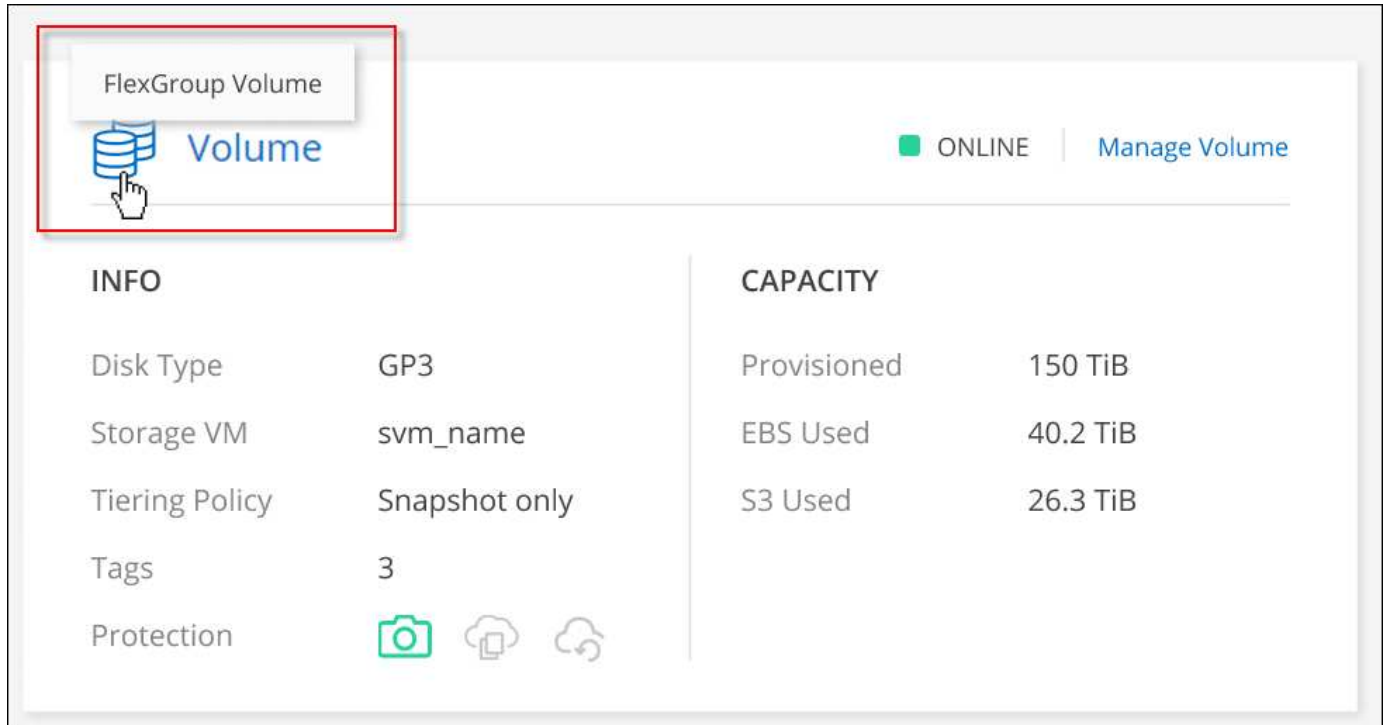
9.4 リリース以前でアグリゲートに対してデータ階層化が有効になっている場合は、古い命名スキームが使用されます。

- 暗号化設定がソース集約と宛先集約で一致していないか、キー再生成が進行中です。
- 階層化ポリシーを変更するために、ボリューム移動時に `-tiering-policy` オプションが指定されました。

- ボリューム移動時に `-generate-destination-key` オプションが指定されました。

FlexGroupボリュームを表示

ONTAP System Manager またはONTAP CLI を通じて作成されたFlexGroupボリュームは、コンソールの [ボリューム] タブから直接表示できます。専用の「ボリューム」タイルから FlexGroup ボリュームの詳細情報を確認できます。ここでは、アイコンのホバー テキストから各FlexGroupボリューム グループを識別できます。さらに、ボリューム リスト ビューの「ボリューム スタイル」列でFlexGroupボリュームを識別および並べ替えることもできます。



INFO		CAPACITY	
Disk Type	GP3	Provisioned	150 TiB
Storage VM	svm_name	EBS Used	40.2 TiB
Tiering Policy	Snapshot only	S3 Used	26.3 TiB
Tags	3		
Protection	  		



現在、コンソールでは既存のFlexGroupボリュームのみを表示できます。コンソールでFlexGroupボリュームを作成することはできません。

非アクティブなCloud Volumes ONTAPデータを低コストのオブジェクトストレージに階層化します

ホット データ用の SSD または HDD パフォーマンス層と非アクティブ データ用のオブジェクト ストレージ容量層を組み合わせることで、Cloud Volumes ONTAPのストレージコストを削減できます。データ階層化はFabricPoolテクノロジーによって実現されます。概要については、以下を参照してください。"[データ階層化の概要](#)"。

データ階層化を設定するには、次の手順を実行する必要があります。

1

サポートされている構成を選択してください

ほとんどの構成がサポートされています。最新バージョンを実行しているCloud Volumes ONTAPシステムをお持ちの場合は、そのままご利用いただけます。"[詳細情報](#)"。

2

Cloud Volumes ONTAPとオブジェクトストレージ間の接続を確保する

- AWS の場合、S3 への VPC エンドポイントが必要になります。[詳細情報](#)。
- Azure の場合、NetAppコンソールに必要な権限がある限り、何もする必要はありません。[詳細情報](#)。
- Google Cloud の場合、プライベート Google アクセスのサブネットを構成し、サービス アカウントを設定する必要があります。[詳細情報](#)。

3

階層化が有効になっているアグリゲートがあることを確認します

ボリューム上でデータ階層化を有効にするには、アグリゲート上でデータ階層化を有効にする必要があります。新しいボリュームと既存のボリュームの要件を認識しておく必要があります。[詳細情報](#)。

4

ボリュームを作成、変更、または複製するときに階層化ポリシーを選択します

NetAppコンソールでは、ボリュームを作成、変更、または複製するときに階層化ポリシーを選択するように求められます。

- "読み書きボリュームからの階層データ"
- "データ保護ボリュームからの階層データ"

データ階層化に必須ではないものは何ですか？

- データ階層化を有効にするために機能ライセンスをインストールする必要はありません。
- 容量層用のオブジェクト ストアを作成する必要はありません。コンソールがそれを実行します。
- システム レベルでデータ階層化を有効にする必要はありません。



コンソールはシステムを作成するときにコールドデータ用のオブジェクトストアを作成します。[接続や権限の問題がない限り](#)。その後は、ボリューム上のデータ階層化を有効にするだけです（場合によっては、[骨材について](#)）。

データ階層化をサポートする構成

特定の構成と機能を使用する場合、データ階層化を有効にすることができます。

AWSでのサポート

- データ階層化は、Cloud Volumes ONTAP 9.2 以降で AWS でサポートされます。
- パフォーマンス層は、汎用 SSD (gp3 または gp2) またはプロビジョニングされた IOPS SSD (io1) にすることができます。



スループット最適化 HDD (st1) を使用する場合は、オブジェクト ストレージにデータを階層化することはお勧めしません。

- 非アクティブなデータは Amazon S3 バケットに階層化されます。他のプロバイダーへの階層化はサポートされていません。

Azureでのサポート

- Azure では、データ階層化は次のようにサポートされています。
 - シングルノードシステムのバージョン9.4
 - HAペア付きバージョン9.6
- パフォーマンス レベルは、Premium SSD マネージド ディスク、Standard SSD マネージド ディスク、または Standard HDD マネージド ディスクになります。
- 非アクティブなデータは Microsoft Azure Blob に階層化されます。他のプロバイダーへの階層化はサポートされていません。

Google Cloud のサポート

- データ階層化は、Cloud Volumes ONTAP 9.6 以降、Google Cloud でサポートされます。
- パフォーマンス レベルは、SSD 永続ディスク、バランス永続ディスク、標準永続ディスクのいずれかになります。
- 非アクティブなデータは Google Cloud Storage に階層化されます。他のプロバイダーへの階層化はサポートされていません。

機能の相互運用性

- データ階層化は暗号化テクノロジーによってサポートされます。
- ボリューム上でシンプロビジョニングを有効にする必要があります。

要件

クラウド プロバイダーによっては、Cloud Volumes ONTAP がコールド データをオブジェクト ストレージに階層化できるように、特定の接続とアクセス許可を設定する必要があります。

コールドデータをAWS S3に階層化するための要件

Cloud Volumes ONTAP がS3 に接続されていることを確認します。この接続を提供する最善の方法は、S3 サービスへの VPC エンドポイントを作成することです。手順については、["AWS ドキュメント: ゲートウェイ エンドポイントの作成"](#)。

VPC エンドポイントを作成するときは、Cloud Volumes ONTAPインスタンスに対応するリージョン、VPC、ルートテーブルを選択してください。また、セキュリティ グループを変更して、S3 エンドポイントへのトラフィックを有効にする送信 HTTPS ルールを追加する必要があります。そうしないと、Cloud Volumes ONTAP はS3 サービスに接続できません。

問題が発生した場合は、["AWS サポート ナレッジセンター: ゲートウェイ VPC エンドポイントを使用して S3 バケットに接続できないのはなぜですか?"](#)。

コールドデータをAzure Blobストレージに階層化するための要件

コンソールに必要な権限がある限り、パフォーマンス層と容量層の間に接続を設定する必要はありません。コンソール エージェントのカスタム ロールに次の権限がある場合、コンソールは VNet サービス エンドポイントを有効にします。


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

カスタム ロールには、デフォルトで権限が含まれます。 ["コンソール エージェントの Azure 権限を表示する"](#)

コールドデータを **Google Cloud Storage** バケットに階層化するための要件

- Cloud Volumes ONTAPが存在するサブネットは、プライベート Google アクセス用に構成する必要があります。手順については、["Google Cloud ドキュメント: プライベート Google アクセスの設定"](#)。
- サービス アカウントをCloud Volumes ONTAPに接続する必要があります。

["このサービスアカウントの設定方法を学ぶ"](#)。

Cloud Volumes ONTAPシステムを作成するときに、このサービス アカウントを選択するように求められます。

デプロイ中にサービス アカウントを選択しない場合は、Cloud Volumes ONTAPをシャットダウンし、Google Cloud コンソールに移動して、サービス アカウントをCloud Volumes ONTAPインスタンスに接続する必要があります。次のセクションで説明するように、データ階層化を有効にできます。

- 顧客管理の暗号鍵を使用してバケットを暗号化するには、Google Cloud ストレージ バケットで鍵の使用を有効にします。

["Cloud Volumes ONTAPで顧客管理の暗号化キーを使用する方法を学びます"](#)。

要件を実装した後、データ階層化を有効にする

接続性や権限の問題がない限り、コンソールはシステムの作成時にコールド データ用のオブジェクト ストアを作成します。システムの作成後まで上記の要件を実装しなかった場合は、オブジェクト ストアを作成する API またはONTAP System Manager を使用して階層化を手動で有効にする必要があります。



コンソールを通じて階層化を有効にする機能は、将来のCloud Volumes ONTAPリリースで利用できるようになります。

アグリゲートで階層化が有効になっていることを確認する

ボリューム上でデータ階層化を有効にするには、アグリゲート上でデータ階層化を有効にする必要があります。新しいボリュームと既存のボリュームの要件を認識しておく必要があります。

- 新刊

新しいボリュームでデータ階層化を有効にする場合は、アグリゲートでデータ階層化を有効にすることについて心配する必要はありません。コンソールは、階層化が有効になっている既存のアグリゲート上にボリュームを作成するか、データ階層化が有効になっているアグリゲートがまだ存在しない場合は、ボリュームの新しいアグリゲートを作成します。

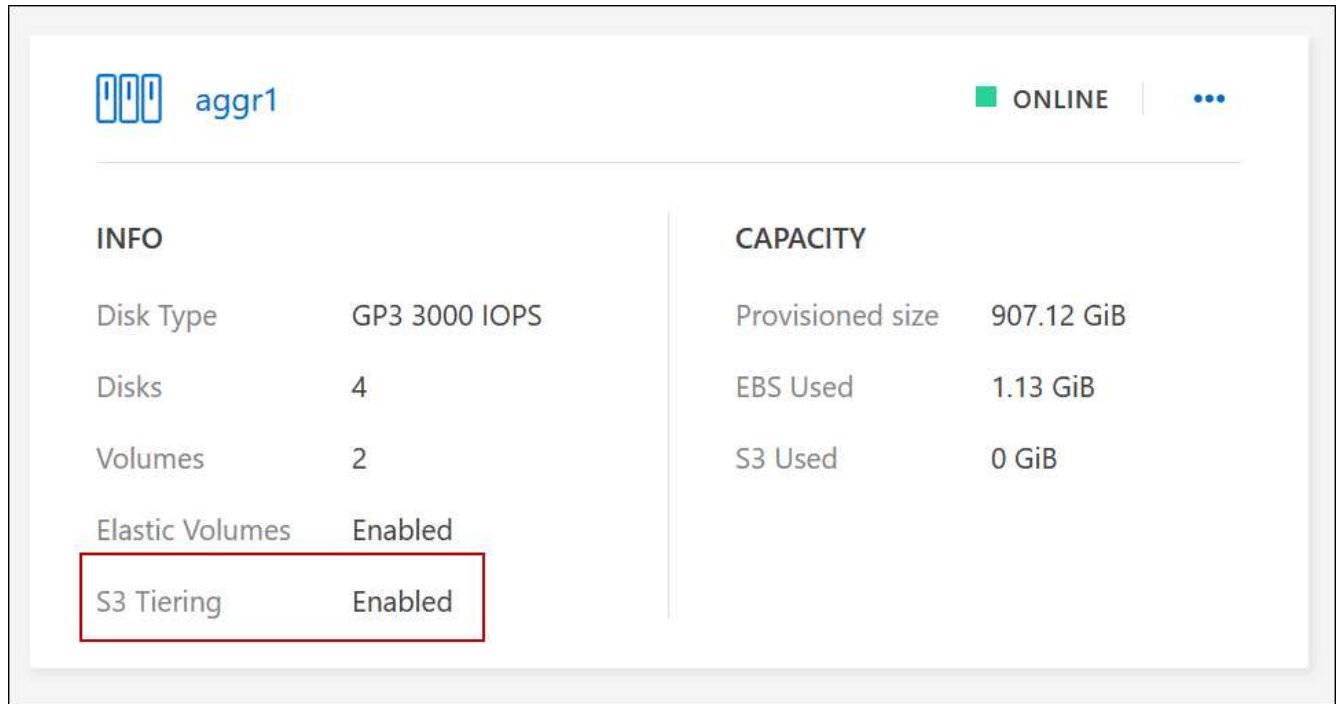
- 既存の巻

既存のボリュームでデータ階層化を有効にするには、基礎となるアグリゲートでそれが有効になっていることを確認します。既存のアグリゲートでデータ階層化が有効になっていない場合は、ONTAP System

Manager を使用して既存のアグリゲートをオブジェクトストアに接続する必要があります。

アグリゲートで階層化が有効になっているかどうかを確認する手順

1. 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. Cloud Volumes ONTAPシステムを開きます。
3. **Aggregates** タブを選択し、アグリゲートで階層化が有効になっているか無効になっているかを確認します。



INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

アグリゲート上で階層化を有効にする手順

1. ONTAP System Manager で、ストレージ > 階層 をクリックします。
2. アグリゲートのアクションメニューをクリックし、*クラウドティアの接続*を選択します。
3. アタッチするクラウド層を選択し、「保存」をクリックします。

次の手順

次のセクションで説明するように、新規および既存のボリュームでデータ階層化を有効にできるようになりました。

読み書きボリュームからの階層データ

Cloud Volumes ONTAP は、読み取り/書き込みボリューム上の非アクティブなデータをコスト効率の高いオブジェクトストレージに階層化し、パフォーマンス層をホット データ用に解放します。

手順

1. システムの「ボリューム」タブで、新しいボリュームを作成するか、既存のボリュームの階層を変更します。

Task	アクション
新しいボリュームを作成	*新しいボリュームの追加*をクリックします。
既存のボリュームの変更	目的のボリューム タイルを選択し、ボリュームの管理 をクリックしてボリュームの管理の右側のパネルにアクセスし、右側のパネルの下にある詳細アクション と 階層化ポリシーの変更 をクリックします。

2. 階層化ポリシーを選択します。

これらのポリシーの説明については、"[データ階層化の概要](#)"。

例

Change Tiering Policy

Volume_1

Tiering Policy

☒

Auto - Tiers cold Snapshot copies and cold user data from the active file system to object storage.
Minimum cooling days: 31 (2-183)

☐

All - Immediately tiers all data (not including metadata) to object storage.

☐

Snapshot Only - Tiers cold Snapshot copies to object storage.

☐

None - Data tiering is disabled.

S3 Storage classes

Standard-Infrequent Access

S3 Storage Encryption Key

aws/s3

データ階層化対応のアグリゲートがまだ存在しない場合、コンソールはボリュームの新しいアグリゲートを作成します。

データ保護ボリュームからの階層データ

Cloud Volumes ONTAP は、データ保護ボリュームから容量層にデータを階層化できます。宛先ボリュームをアクティブ化すると、データは読み取られるにつれて徐々にパフォーマンス層に移動します。

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、ソースボリュームを含むCloud Volumes ONTAPシステムを選択し、ボリュームを複製するシステムにドラッグします。
3. 階層化ページに到達するまでプロンプトに従い、オブジェクト ストレージへのデータ階層化を有効にします。

例

 **S3 Tiering** What are storage tiers?

☒ **Enabled** ☐ **Disabled**

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

データの複製に関するヘルプについては、以下を参照してください。 ["クラウドとの間でデータを複製する"](#)。

階層化データのストレージクラスを変更する

Cloud Volumes ONTAPを導入した後、30 日間アクセスされていない非アクティブなデータのストレージ クラスを変更することで、ストレージ コストを削減できます。データにアクセスする場合、アクセス コストが高くなるため、ストレージ クラスを変更する前にその点を考慮する必要があります。

階層化データのストレージ クラスはシステム全体にわたっており、ボリュームごとではありません。

サポートされているストレージクラスの詳細については、["データ階層化の概要"](#)。

手順

1. Cloud Volumes ONTAPシステムで、メニュー アイコンをクリックし、ストレージ クラス または **Blob** ストレージ階層化 をクリックします。
2. ストレージ クラスを選択し、[保存] をクリックします。

データ階層化の空き領域比率を変更する

データ階層化の空き領域比率は、データをオブジェクト ストレージに階層化するときに、Cloud Volumes ONTAP SSD/HDD に必要な空き領域の量を定義します。デフォルト設定は 10% の空き領域ですが、要件に応じて設定を微調整できます。

たとえば、購入した容量を確実に活用するには、空き領域を 10% 未満に選択する場合があります。追加の容量が必要になったときに、コンソールは追加のディスクを購入できます (アグリゲートのディスク制限に達するまで)。



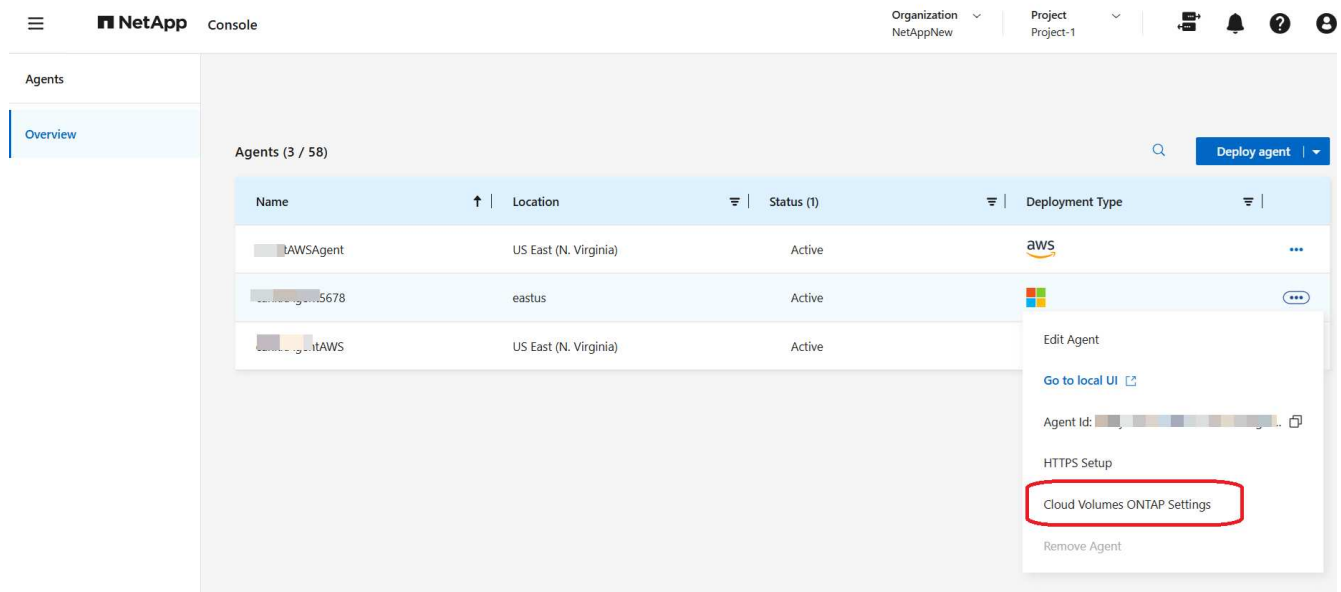
十分なスペースがない場合、Cloud Volumes ONTAP はデータを移動できず、パフォーマンスが低下する可能性があります。いかなる変更も慎重に行う必要があります。不明な場合は、NetAppサポートに問い合わせるガイダンスを受けてください。

この比率は、オブジェクト ストアからデータが読み取られると、Cloud Volumes ONTAP がデータを SSD/HDD に移動してパフォーマンスを向上させるため、災害復旧シナリオにとって重要です。十分なスペースがない場合、Cloud Volumes ONTAP はデータを移動できません。ビジネス要件を満たすことができるよう

に比率を変更するときは、この点を考慮してください。

手順

1. 左側のナビゲーション ペインから、管理 > エージェント に移動します。
2. クリック ...Cloud Volumes ONTAPシステムを管理するコンソール エージェントのアイコン。
3. * Cloud Volumes ONTAP設定*を選択します。



4. *容量*の下で、*総容量しきい値 - データ階層化の空き領域比率*をクリックします。

Edit Cloud Volumes ONTAP settings

Capacity

Capacity Management Mode	Automatic Mode	▼
Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

General

Automatic Cloud Volumes ONTAP update during deployment	On	▼

Azure

Azure CIFS locks for Azure HA systems	Off	▼
Use Azure Private Link	On	▼

5. 要件に応じて空き領域の比率を変更し、「保存」をクリックします。

自動階層化ポリシーの冷却期間を変更する

auto 階層化ポリシーを使用してCloud Volumes ONTAPボリュームでデータ階層化を有効にした場合は、ビジネス ニーズに基づいてデフォルトの冷却期間を調整できます。このアクションは、ONTAP CLI および API のみを使用してサポートされます。

冷却期間とは、ボリューム内のユーザー データが「コールド」であるとみなされてオブジェクト ストレージに移動されるまでに非アクティブのままでないなければならない日数です。

自動階層化ポリシーのデフォルトの冷却期間は 31 日です。冷却期間は次のように変更できます。

- 9.8以降: 2日から183日
- 9.7以前: 2日から63日

手順

1. ボリュームを作成するとき、または既存のボリュームを変更するときは、API リクエストで *minimumCoolingDays* パラメータを使用します。

システムの廃止時にS3バケットを削除する

環境を廃止するときに、Cloud Volumes ONTAPシステムから階層化されたデータを含む S3 バケットを削除

できます。

S3 バケットを削除できるのは、次の場合のみです。

- Cloud Volume ONTAPシステムがコンソールから削除されます。
- すべてのオブジェクトがバケットから削除され、S3 バケットは空になります。

Cloud Volumes ONTAPシステムを廃止しても、その環境用に作成された S3 バケットは自動的に削除されません。代わりに、偶発的なデータ損失を防ぐために孤立状態のままになります。バケット内のオブジェクトを削除してから、S3 バケット自体を削除するか、後で使用するために保持することができます。参照 ["ONTAP CLI: vservers object-store-server バケット削除"](#)。

ホストシステムからCloud Volumes ONTAP上のLUNに接続する

iSCSI ボリュームを作成すると、NetApp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り、管理の手間がかかりません。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。

次の点に注意してください。

- コンソールの自動容量管理は LUN には適用されません。LUN を作成すると、自動拡張機能が無効になります。
- ONTAP System Manager またはONTAP CLI から追加の LUN を作成できます。

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、ボリュームを管理するCloud Volumes ONTAPシステムをダブルクリックします。
3. システムで、[ボリューム] タブを選択します。
4. 必要なボリューム タイルに移動し、ボリュームの管理 を選択して、右側のボリュームの管理パネルにアクセスします。
5. ターゲット **iQN** をクリックします。
6. コピー をクリックして iQN 名をコピーします。
7. ホストから LUN への iSCSI 接続を設定します。
 - ["Red Hat Enterprise Linux 用ONTAP 9 iSCSI 高速構成: ターゲットとの iSCSI セッションの開始"](#)
 - ["Windows用ONTAP 9 iSCSIエクスプレス構成：ターゲットとのiSCSIセッションの開始"](#)
 - ["ONTAP SAN Host Configuration"](#)

Cloud Volumes ONTAPシステム上のFlexCacheボリュームを使用してデータ アクセスを高速化します

FlexCacheボリュームは、元のボリューム (またはソース ボリューム) からの SMB および NFS 読み取りデータをキャッシュするストレージ ボリュームです。キャッシュされたデータへの後続の読み取りにより、そのデータへのアクセスが高速化されます。

FlexCacheボリュームを使用すると、データへのアクセスを高速化したり、頻繁にアクセスされるボリューム

のトラフィックをオフロードしたりできます。FlexCacheボリュームを使用すると、元のボリュームにアクセスせずに直接データを使用できるため、特にクライアントが同じデータに繰り返しアクセスする場合に読み取りパフォーマンスが向上します。FlexCacheボリュームは、読み取り集中型のシステム ワークロードに適しています。

NetAppコンソールはFlexCacheボリュームの管理を"[NetAppボリューム キャッシング](#)"。

ONTAP CLI またはONTAP System Manager を使用してFlexCacheボリュームを作成および管理することもできます。

- "[FlexCacheボリュームによるデータアクセス高速化のパワーガイド](#)"
- "[System ManagerでFlexCacheボリュームを作成する](#)"



オリジンが暗号化されている場合に**FlexCache**を使用する

元のボリュームが暗号化されているCloud Volumes ONTAPシステムでFlexCache を構成する場合は、FlexCacheボリュームが暗号化されたデータに適切にアクセスしてキャッシュできるようにするために、追加の手順が必要です。

開始する前に

1. 暗号化の設定: ソース ボリュームが完全に暗号化され、動作可能であることを確認します。Cloud Volumes ONTAPシステムの場合、これにはクラウド固有のキー管理サービスとの統合が含まれます。

AWS の場合、これは通常、AWS Key Management Service (KMS) を使用することを意味します。詳細については、"[AWS Key Management Service でキーを管理する](#)"。

Azure の場合、NetApp Volume Encryption (NVE) 用に Azure Key Vault を設定する必要があります。詳細については、"[Azure Key Vault でキーを管理する](#)"。

Google Cloud の場合は、Google Cloud Key Management Service です。詳細については、"[Google の Cloud Key Management Service で鍵を管理する](#)"。

1. キー管理サービス: FlexCacheボリュームを作成する前に、Cloud Volumes ONTAPシステムでキー管理サービスが正しく設定されていることを確認します。この構成は、FlexCacheボリュームが元のボリュームからのデータを復号化するために不可欠です。
2. ライセンス: 有効なFlexCacheライセンスがCloud Volumes ONTAPシステムで使用可能であり、アクティブ化されていることを確認します。
3. * ONTAPバージョン*: Cloud Volumes ONTAPシステムのONTAPバージョンが、暗号化されたボリュームを持つFlexCacheをサポートしていることを確認します。最新の "[ONTAPリリースノート](#)" 詳細については、または[互換性マトリックス](#)を参照してください。
4. ネットワーク構成: ネットワーク構成によって、元のボリュームとFlexCacheボリューム間のシームレスな通信が可能であることを確認します。これには、クラウド環境での適切なルーティングと DNS 解決が含まれます。

手順

暗号化されたソース ボリュームを使用して、Cloud Volumes ONTAPシステムにFlexCacheボリュームを作成します。詳細な手順と追加の考慮事項については、次のセクションを参照してください。

- "[FlexCacheボリュームによるデータアクセス高速化のパワーガイド](#)"
- "[System ManagerでFlexCacheボリュームを作成する](#)"

集計管理

Cloud Volumes ONTAPシステムのアグリゲートを作成する

アグリゲートは自分で作成することも、ボリュームの作成時にNetAppコンソールに作成させることもできます。アグリゲートを自分で作成する利点は、基盤となるディスク サイズを選択できるため、必要な容量やパフォーマンスに合わせてアグリゲートのサイズを設定できることです。



すべてのディスクとアグリゲートは、コンソールから直接作成および削除する必要があります。これらのアクションを別の管理ツールから実行しないでください。そうすると、システムの安定性に影響が及び、将来的にディスクを追加する能力が妨げられ、クラウド プロバイダーの料金が重複して発生する可能性があります。

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、アグリゲートを管理するCloud Volumes ONTAPシステムの名前をダブルクリックします。
3. 「集計」タブで、「集計の追加」をクリックし、集計の詳細を指定します。

AWS

- ° ディスクの種類とサイズを選択するように求められた場合は、["AWS でCloud Volumes ONTAP構成を計画する"](#)。
- ° アグリゲートの容量サイズを入力するように求められた場合は、Amazon EBS Elastic Volumes 機能をサポートする構成でアグリゲートを作成していることになります。次のスクリーンショットは、gp3 ディスクで構成された新しいアグリゲートの例を示しています。

1 Disk Type 2 Aggregate details 3 Tiering Data 4 Review

Select Disk Type

Disk Type

GP3 - General Purpose SSD Dynamic Performance

 **General Purpose SSD (gp3) Disk Properties**

Description: General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)

IOPS Value		Throughput MB/s	
12000		250	

["エラスティックボリュームのサポートについて詳しくはこちら"](#)。

Azure

ディスクの種類とディスクサイズに関するヘルプについては、["AzureでCloud Volumes ONTAPの構成を計画する"](#)。

Google Cloud

ディスクの種類とディスクサイズに関するヘルプについては、["Google Cloud でCloud Volumes ONTAP構成を計画する"](#)。

4. *追加*をクリックし、*承認して購入*をクリックします。

Cloud Volumes ONTAP クラスターのアグリゲートを管理する

ディスクを追加したり、アグリゲートの情報を表示したり、アグリゲートを削除したりして、アグリゲートを自分で管理します。



すべてのディスクとアグリゲートは、NetAppコンソールから直接作成および削除する必要があります。これらのアクションを別の管理ツールから実行しないでください。そうすると、システムの安定性に影響が及び、将来的にディスクを追加する能力が妨げられ、クラウドプロバイダーの料金が重複して発生する可能性があります。

開始する前に

アグリゲートを削除する場合は、まずアグリゲート内のボリュームを削除しておく必要があります。

タスク概要

アグリゲートのスペースが不足している場合は、ONTAP System Manager を使用してボリュームを別のアグリゲートに移動できます。

手順

1. 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、アグリゲートを管理するCloud Volumes ONTAPシステムをダブルクリックします。
3. システムの詳細から、[集計] タブをクリックします。
4. 必要な集計については、...管理アクションのアイコン。

INFO		CAPACITY	
Disk Type	GP3 3000 IOPS	Provisioned size	907.12 GiB
Disks	4	EBS Used	1.13 GiB
Volumes	2	S3 Used	0 GiB
Elastic Volumes	Enabled		
S3 Tiering	Enabled		

5. 利用可能なオプションから集計を管理します ...メニュー。



アグリゲートにディスクを追加する場合、アグリゲート内のすべてのディスクのサイズが同じである必要があります。

AWS の場合、Amazon EBS Elastic Volumes をサポートするアグリゲートの容量を増やすことができます。

1. の下で ...メニューで、[容量を増やす] をクリックします。
2. 追加したい容量を入力し、「増加」をクリックします。

アグリゲートの容量を少なくとも 256 GiB、またはアグリゲートのサイズの 10% 増やす必要があることに注意してください。たとえば、1.77 TiB の集約がある場合、10% は 181 GiB になります。これは 256 GiB より小さいため、集計のサイズを最小値の 256 GiB だけ増やす必要があります。

コンソールエージェントでCloud Volumes ONTAPアグリゲート容量を管理する

各コンソール エージェントには、Cloud Volumes ONTAPの総容量を管理する方法を決定する設定があります。

これらの設定は、コンソール エージェントによって管理されるすべてのCloud Volumes ONTAPシステムに影響します。別のコンソール エージェントがある場合は、別の方法で構成できます。

必要な権限

Cloud Volumes ONTAP設定を変更するには、NetAppコンソールの組織またはアカウントの管理者権限が必要です。

手順

1. 左側のナビゲーション ペインから、管理 > エージェント に移動します。
2. クリック ...Cloud Volumes ONTAPシステムを管理するコンソール エージェントのアイコン。
3. * Cloud Volumes ONTAP設定*を選択します。

The screenshot shows the NetApp Console interface. On the left, the 'Agents' section is active. The main area displays a table of agents. The first agent, 'AWSAgent', is selected, and a context menu is open over it. The menu includes options like 'Edit Agent', 'Go to local UI', 'Agent Id', 'HTTPS Setup', 'Cloud Volumes ONTAP Settings' (which is highlighted with a red rectangle), and 'Remove Agent'.

Name	Location	Status (1)	Deployment Type
AWSAgent	US East (N. Virginia)	Active	aws
5678	eastus	Active	
itAWS	US East (N. Virginia)	Active	

4. *容量*の下で、次のいずれかの設定を変更します。

Edit Cloud Volumes ONTAP settings

Capacity

 Capacity Management Mode	Automatic Mode	▼
 Aggregate Capacity Thresholds - Free Space Ratio	10%	▼
 Aggregate Capacity Thresholds - Free Space Ratio for Data Tiering	10%	▼
 Volume Autosize - Additional Size in Percentage to Which Volumes Can Grow	1000%	▼

General

 Automatic Cloud Volumes ONTAP update during deployment	On	▼

Azure

 Azure CIFS locks for Azure HA systems	Off	▼
 Use Azure Private Link	On	▼

容量管理モード

コンソールでストレージ容量の決定を通知するか、容量要件を自動的に管理するかを選択します。

["容量管理モードの仕組みを学ぶ"](#)。

総容量しきい値 - 空き容量比率

この比率は容量管理の決定における重要なパラメータであり、容量管理の自動モードと手動モードのどちらであっても、その影響を理解することは不可欠です。リソース使用率とコストのバランスを維持するために、特定のストレージ ニーズと予想される増加を考慮してこのしきい値を設定することをお勧めします。

手動モードでは、アグリゲートの空き領域率が指定されたしきい値を下回ると、通知がトリガーされ、空き領域率の低下に対処するためのアクションを実行する必要があることが警告されます。サービスの中断を回避し、最適なパフォーマンスを確保するには、これらの通知を監視し、総容量を手動で管理することが重要です。

空き容量比率は次のように計算されます: $(\text{総容量} - \text{総使用容量}) / \text{総容量}$

参照["自動容量管理"](#)Cloud Volumes ONTAPで容量が自動的に管理されるようになりました。

総容量しきい値 - データ階層化の空き領域比率

データを容量層 (オブジェクト ストレージ) に階層化するとき、パフォーマンス層 (ディスク) に必要な空き領域の量を定義します。

この比率は災害復旧シナリオにとって重要です。データが容量層から読み取られると、Cloud Volumes ONTAP はデータをパフォーマンス層に移動して、パフォーマンスを向上させます。十分なスペースがない場合、Cloud Volumes ONTAP はデータを移動できません。

5. *保存*をクリックします。

ストレージVM管理

Cloud Volumes ONTAPのストレージVMを管理する

ストレージ VM は、ONTAP内で実行され、クライアントにストレージおよびデータ サービスを提供する仮想マシンです。以前は「SVM」または「Vserver」と呼んでいました。Cloud Volumes ONTAPはデフォルトで 1つのストレージ VM で構成されていますが、一部の構成では追加のストレージ VM がサポートされます。

サポートされるストレージVMの数

特定の構成では複数のストレージ VM がサポートされます。に行く ["Cloud Volumes ONTAPリリースノート"](#) お使いのCloud Volumes ONTAPのバージョンでサポートされているストレージ VM の数を確認します。

複数のストレージVMを操作する

NetAppコンソールは、ONTAP System Manager またはONTAP CLI から作成した追加のストレージ VM をサポートします。

たとえば、次の図は、ボリュームを作成するときにストレージ VM を選択する方法を示しています。

Details & Protection

Storage VM Name ⓘ

svm_name1 ▼

Volume Name

Size (GiB) ⓘ

Volume size

Snapshot Policy

default ▼

ⓘ Default Policy

次の図は、ボリュームを別のシステムに複製するときにストレージ VM を選択する方法を示しています。

The screenshot shows a configuration form with three fields:

- Destination Volume Name:** A text input field containing the value "volume_copy".
- Destination Storage VM Name:** A dropdown menu with "svm_name1" selected.
- Destination Aggregate:** A dropdown menu with "Automatically select the best aggregate" selected.

デフォルトのストレージ**VM**の名前を変更する

コンソールは、Cloud Volumes ONTAP用に作成する単一のストレージ VM に自動的に名前を付けます。厳密な命名規則がある場合は、ONTAP System Manager、ONTAP CLI、または API からストレージ VM の名前を変更できます。たとえば、名前をONTAPクラスターのストレージ VM の名前と一致させたい場合があります。

AWS でCloud Volumes ONTAPのデータサービス ストレージ VM を管理する

ストレージ VM は、ONTAP内で実行され、クライアントにストレージおよびデータ サービスを提供する仮想マシンです。以前は「SVM」または「Vserver」と呼んでいました。Cloud Volumes ONTAPはデフォルトで 1 つのストレージ VM で構成されていますが、一部の構成では追加のストレージ VM がサポートされます。

追加のデータ提供ストレージ VM を作成するには、AWS で IP アドレスを割り当て、Cloud Volumes ONTAP 構成に基づいてONTAPコマンドを実行する必要があります。

サポートされるストレージ**VM**の数

9.7 リリース以降、特定のCloud Volumes ONTAP構成では複数のストレージ VM がサポートされます。に行く ["Cloud Volumes ONTAPリリースノート"](#)お使いのCloud Volumes ONTAPのバージョンでサポートされているストレージ VM の数を確認します。

その他のすべてのCloud Volumes ONTAP構成では、1 つのデータ提供ストレージ VM と、災害復旧に使用される 1 つの宛先ストレージ VM がサポートされます。ソース ストレージ VM に障害が発生した場合、データ アクセス用に宛先ストレージ VM をアクティブ化できます。

構成の制限を確認する

各 EC2 インスタンスは、ネットワーク インターフェイスごとに最大数のプライベート IPv4 アドレスをサポートします。新しいストレージ VM に AWS で IP アドレスを割り当てる前に、制限を確認する必要があります。

す。

手順

1. 行く ["Cloud Volumes ONTAPリリースノートのストレージ制限セクション"](#)。
2. インスタンス タイプごとのインターフェースあたりの IP アドレスの最大数を特定します。
3. この番号は、次のセクションで AWS で IP アドレスを割り当てるときに必要なになるので、メモしておいてください。

AWSでIPアドレスを割り当てる

新しいストレージ VM の LIF を作成する前に、AWS のポート e0a にプライベート IPv4 アドレスを割り当てる必要があります。

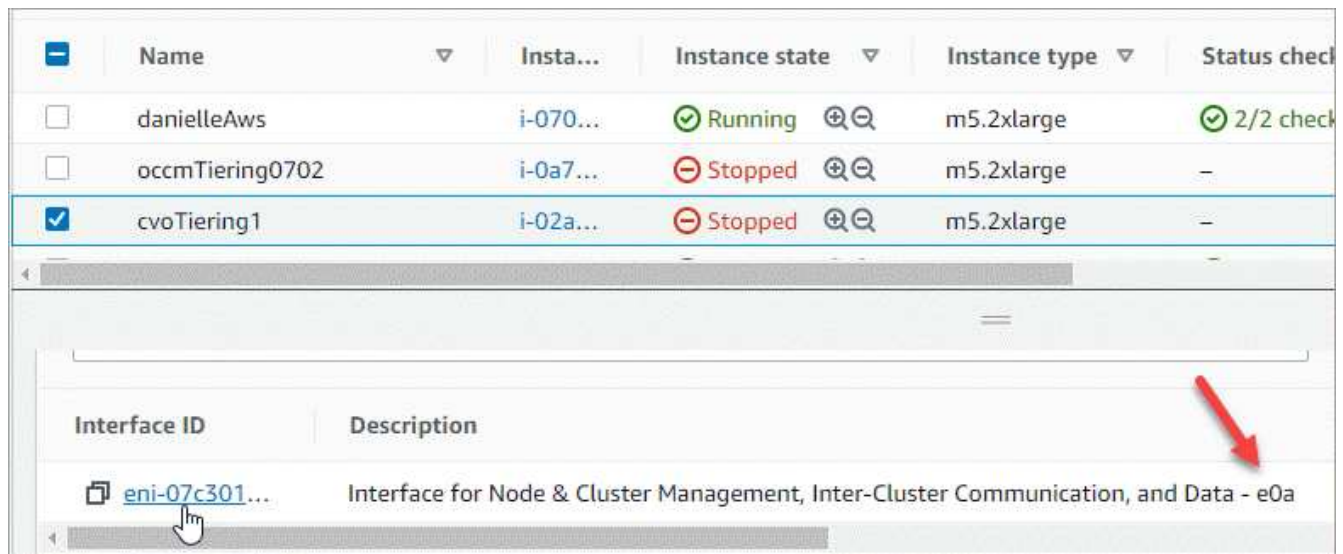
ストレージ VM のオプションの管理 LIF には、単一ノード システム上および単一 AZ 内の HA ペア上のプライベート IP アドレスが必要であることに注意してください。この管理 LIF は、SnapCenterなどの管理ツールへの接続を提供します。

手順

1. AWS にログインし、EC2 サービスを開きます。
2. Cloud Volumes ONTAPインスタンスを選択し、**[Networking]** をクリックします。

HA ペアでストレージ VM を作成する場合は、ノード 1 を選択します。

3. ネットワーク インターフェース まで下にスクロールし、ポート e0a の インターフェース ID をクリックします。



4. ネットワーク インターフェースを選択し、**[アクション] > [IP アドレスの管理]** をクリックします。
5. e0a の IP アドレスのリストを展開します。
6. IP アドレスを確認します。
 - a. 割り当てられた IP アドレスの数を数えて、ポートに追加の IP を割り当てる余裕があることを確認します。

このページの前のセクションで、インターフェースごとにサポートされる IP アドレスの最大数を特定しておく必要があります。

- b. オプション: Cloud Volumes ONTAPのONTAP CLI に移動し、**network interface show** を実行して、これらの各 IP アドレスが使用中であることを確認します。

IP アドレスが使用されていない場合は、新しいストレージ VM で使用できます。

7. AWS コンソールに戻り、[新しい IP アドレスの割り当て] をクリックして、新しいストレージ VM に必要な量に基づいて追加の IP アドレスを割り当てます。

- 単一ノード システム: 未使用のセカンダリ プライベート IP が 1 つ必要です。

ストレージ VM 上に管理 LIF を作成する場合は、オプションのセカンダリ プライベート IP が必要です。

- 単一 AZ 内の HA ペア: ノード 1 に未使用のセカンダリ プライベート IP が 1 つ必要です。

ストレージ VM 上に管理 LIF を作成する場合は、オプションのセカンダリ プライベート IP が必要です。

- 複数の AZ の HA ペア: 各ノードに未使用のセカンダリ プライベート IP が 1 つ必要です。

8. 単一の AZ 内の HA ペアで IP アドレスを割り当てる場合は、セカンダリ プライベート **IPv4** アドレスの再割り当てを許可する を有効にします。

9. *保存*をクリックします。

10. 複数の AZ に HA ペアがある場合は、ノード 2 に対してこれらの手順を繰り返す必要があります。

単一ノードシステム上にストレージVMを作成する

これらの手順では、単一ノード システムに新しいストレージ VM を作成します。NAS LIF を作成するには 1 つのプライベート IP アドレスが必要であり、管理 LIF を作成する場合は、オプションで別のプライベート IP アドレスが必要になります。

手順

1. ストレージ VM とストレージ VM へのルートを作成します。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. NAS LIF を作成します。


```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-data-files -home-port e0a -address private_ip_x -netmask
node1Mask -lif ip_nas_2 -home-node cvo-node
```

ここで、*private_ip_x* は e0a 上の未使用のセカンダリ プライベート IP です。

3. オプション: ストレージ VM 管理 LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service
-policy default-management -home-port e0a -address private_ip_y -netmask
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node
```

ここで、*private_ip_y* は e0a 上の別の未使用のセカンダリ プライベート IP です。

4. 1 つ以上のアグリゲートをストレージ VM に割り当てます。

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

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

単一の AZ 内の HA ペアにストレージ VM を作成する

これらの手順では、単一の AZ 内の HA ペアに新しいストレージ VM を作成します。NAS LIF を作成するには 1 つのプライベート IP アドレスが必要であり、管理 LIF を作成する場合は、オプションで別のプライベート IP アドレスが必要になります。

これらの LIF は両方ともノード 1 に割り当てられます。障害が発生した場合、プライベート IP アドレスはノード間で移動できます。

手順

1. ストレージ VM とストレージ VM へのルートを作成します。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway
subnet_gateway
```

2. ノード 1 に NAS LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address private_ip_x -netmask  
node1Mask -lif ip_nas_2 -home-node cvo-node1
```

ここで、*private_ip_x* は cvo-node1 の e0a 上の未使用のセカンダリ プライベート IP です。サービス ポリシー default-data-files では IP がパートナー ノードに移行できることが示されているため、テイクオーバーの際にこの IP アドレスは cvo-node2 の e0a に再配置できます。

3. オプション: ノード 1 にストレージ VM 管理 LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address private_ip_y -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

ここで、*private_ip_y* は e0a 上の別の未使用のセカンダリ プライベート IP です。

4. 1 つ以上のアグリゲートをストレージ VM に割り当てます。

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

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

5. Cloud Volumes ONTAP 9.11.1 以降を実行している場合は、ストレージ VM のネットワーク サービス ポリシーを変更します。

Cloud Volumes ONTAP がアウトバウンド管理接続に iSCSI LIF を使用できるようにするため、サービスを変更する必要があります。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

複数の AZ の HA ペアにストレージ VM を作成する

これらの手順では、複数の AZ の HA ペアに新しいストレージ VM を作成します。

フローティング IP アドレスは NAS LIF には必須ですが、管理 LIF にはオプションです。これらのフローティング IP アドレスでは、AWS でプライベート IP を割り当てる必要はありません。代わりに、フローティング IP は、同じ VPC 内の特定のノードの ENI を指すように AWS ルートテーブルで自動的に構成されます。

フローティング IP を ONTAP で動作させるには、各ノード上のすべてのストレージ VM にプライベート IP アドレスを設定する必要があります。これは、iSCSI LIF がノード 1 とノード 2 に作成される以下の手順に反映されています。

手順

1. ストレージ VM とストレージ VM へのルートを作成します。

```
vserver create -rootvolume-security-style unix -rootvolume root_svm_2  
-snapshot-policy default -vserver svm_2 -aggregate aggr1
```

```
network route create -destination 0.0.0.0/0 -vserver svm_2 -gateway  
subnet_gateway
```

2. ノード 1 に NAS LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-data-files -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_nas_floating_2 -home-node cvo-node1
```

- フローティング IP アドレスは、HA 構成を展開する AWS リージョン内のすべての VPC の CIDR ブロックの外側にある必要があります。192.168.209.27 はフローティング IP アドレスの例です。["フローティングIPアドレスの選択について詳しくはこちら"](#)。
- `-service-policy default-data-files` IP がパートナー ノードに移行できることを示します。

3. オプション: ノード 1 にストレージ VM 管理 LIF を作成します。

```
network interface create -auto-revert true -vserver svm_2 -service  
-policy default-management -home-port e0a -address floating_ip -netmask  
node1Mask -lif ip_svm_mgmt_2 -home-node cvo-node1
```

4. ノード 1 に iSCSI LIF を作成します。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmask node1Mask -lif  
ip_node1_iscsi_2 -home-node cvo-node1
```

- この iSCSI LIF は、ストレージ VM 内のフローティング IP の LIF 移行をサポートするために必要です。iSCSI LIF である必要はありませんが、ノード間で移行するように構成することはできません。
- `-service-policy default-data-block` IP アドレスがノード間で移行されないことを示します。
- `private_ip` は、`cvo_node1` の `eth0 (e0a)` 上の未使用のセカンダリプライベート IP アドレスです。

5. ノード 2 に iSCSI LIF を作成します。

```
network interface create -vserver svm_2 -service-policy default-data-  
blocks -home-port e0a -address private_ip -netmaskNode2Mask -lif  
ip_node2_iscsi_2 -home-node cvo-node2
```

- この iSCSI LIF は、ストレージ VM 内のフローティング IP の LIF 移行をサポートするために必要です。iSCSI LIF である必要はありませんが、ノード間で移行するように構成することはできません。
- `-service-policy default-data-block`IP` アドレスがノード間で移行されないことを示します。
- `private_ip` は、`cvo_node2` の `eth0 (e0a)` 上の未使用のセカンダリプライベート IP アドレスです。

6. 1 つ以上のアグリゲートをストレージ VM に割り当てます。

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

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

7. Cloud Volumes ONTAP 9.11.1 以降を実行している場合は、ストレージ VM のネットワーク サービス ポリシーを変更します。

Cloud Volumes ONTAP がアウトバウンド管理接続に iSCSI LIF を使用できるようにするため、サービスを変更する必要があります。

```

network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service data-fpolicy-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ad-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-dns-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-ldap-client
network interface service-policy remove-service -vserver <svm-name>
-policy default-data-files -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-blocks -service management-nis-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service data-fpolicy-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ad-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-dns-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-ldap-client
network interface service-policy add-service -vserver <svm-name> -policy
default-data-iscsi -service management-nis-client

```

Azure でCloud Volumes ONTAPのデータサービス ストレージ VM を管理する

ストレージ VM は、ONTAP内で実行され、クライアントにストレージおよびデータ サービスを提供する仮想マシンです。以前は「SVM」または「Vserver」と呼んでいました。Cloud Volumes ONTAP はデフォルトで 1 つのストレージ VM で構成されていますが、Azure でCloud Volumes ONTAP を実行するときに追加のストレージ VM を作成できます。

Azure で追加のデータ サービス ストレージ VM を作成および管理するには、API を使用する必要があります。これは、API がストレージ VM を作成し、必要なネットワーク インターフェイスを構成するプロセスを自動化するためです。ストレージ VM を作成するときに、NetAppコンソールは必要な LIF サービスと、ストレージ VM からの送信 SMB/CIFS 通信に必要な iSCSI LIF を構成します。

Cloud Volumes ONTAP API呼び出しの実行については、以下を参照してください。 ["最初のAPI呼び出し"](#)。

サポートされるストレージVMの数

Cloud Volumes ONTAP 9.9.0 以降では、ライセンスに基づいて、特定の構成で複数のストレージ VM がサポートされるようになりました。参照 ["Cloud Volumes ONTAPリリースノート"](#)お使いのCloud Volumes ONTAPのバージョンでサポートされているストレージ VM の数を確認します。

Cloud Volumes ONTAP 9.9.0 より前のすべてのバージョンでは、災害復旧に使用される 1 つのデータ提供ストレージ VM と 1 つの宛先ストレージ VM がサポートされます。ソース ストレージ VM に障害が発生した場合、データ アクセス用に宛先ストレージ VM をアクティブ化できます。

ストレージVMを作成する

構成とライセンスの種類に基づいて、NetAppコンソールの API を使用して、単一ノード システムまたは高可用性 (HA) 構成で複数のストレージ VM を作成できます。

タスク概要

APIを使用してストレージVMを作成すると、必要なネットワークインターフェースの設定とともに、コンソールは `default-data-files` NAS データ LIF から次のサービスを削除し、アウトバウンド管理接続に使用される iSCSI データ LIF に追加することで、データ ストレージ VM のポリシーを変更します。

- data-fpolicy-client
- management-ad-client
- management-dns-client
- management-ldap-client
- management-nis-client

開始する前に

コンソール エージェントには、Cloud Volumes ONTAPのストレージ VM を作成するための特定の権限が必要です。必要な権限は以下に記載されています ["NetAppが提供するポリシー"](#)。

シングルノードシステム

次の API 呼び出しを使用して、単一ノード システムにストレージ VM を作成します。

POST /azure/vsa/working-environments/{workingEnvironmentId}/svm

リクエスト本文に次のパラメータを含めます。

```
{ "svmName": "myNewSvm1"
  "svmPassword": "optional, the API takes the cluster password if not
provided"
  "mgmtLif": "optional, to create an additional management LIF, if you
want to use the storage VM for management purposes"}
```

HAペア

HA ペア上にストレージ VM を作成するには、次の API 呼び出しを使用します。

POST /azure/ha/working-environments/{workingEnvironmentId}/svm

リクエスト本文に次のパラメータを含めます。

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

単一ノードシステムおよびHAペア上のストレージVMを管理する

APIを使用すると、単一ノード構成とHA構成の両方でストレージVMの名前を変更したり、削除したりできます。

開始する前に

コンソール エージェントには、Cloud Volumes ONTAPのストレージVMを管理するために特定の権限が必要です。必要な権限は以下に記載されています ["NetAppが提供するポリシー"](#)。

ストレージVMの名前を変更する

ストレージVMの名前を変更するには、既存のストレージVMと新しいストレージVMの名前をパラメーターとして指定する必要があります。

手順

- 単一ノード システム上のストレージVMの名前を変更するには、次のAPI呼び出しを使用します。

PUT /azure/vsa/working-environments/{workingEnvironmentId}/svm

リクエスト本文に次のパラメータを含めます。

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- HA ペア上のストレージVMの名前を変更するには、次のAPI呼び出しを使用します。

PUT /azure/ha/working-environments/{workingEnvironmentId}/svm

リクエスト本文に次のパラメータを含めます。


```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

ストレージVMを削除する

単一ノードまたは HA 構成では、アクティブなボリュームがない場合、ストレージ VM を削除できます。

手順

- 単一ノード システム上のストレージ VM を削除するには、次の API 呼び出しを使用します。

```
DELETE /azure/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- HA ペア上のストレージ VM を削除するには、次の API 呼び出しを使用します。

```
DELETE /azure/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

関連情報

- ["APIを使用する準備"](#)
- ["Cloud Volumes ONTAPワークフロー"](#)
- ["必要な識別子を取得する"](#)
- ["NetAppコンソールのREST APIを使用する"](#)

Google Cloud でCloud Volumes ONTAPのデータ提供ストレージ VM を管理する

ストレージ VM は、ONTAP内で実行され、クライアントにストレージおよびデータ サービスを提供する仮想マシンです。以前は「SVM」または「Vserver」と呼んでいました。Cloud Volumes ONTAPはデフォルトで 1 つのストレージ VM で構成されていますが、一部の構成では追加のストレージ VM がサポートされます。

Google Cloud で追加のデータ提供ストレージ VM を作成して管理するには、API を使用する必要があります。これは、API がストレージ VM を作成し、必要なネットワーク インターフェイスを構成するプロセスを自動化するためです。ストレージ VM を作成するときに、NetAppコンソールは必要な LIF サービスと、ストレージ VM からの送信 SMB/CIFS 通信に必要な iSCSI LIF を構成します。

Cloud Volumes ONTAP API呼び出しの実行については、以下を参照してください。 ["最初のAPI呼び出し"](#)。

サポートされるストレージVMの数

Cloud Volumes ONTAP 9.11.1 以降では、ライセンスに基づいて、特定の構成で複数のストレージ VM がサポートされるようになりました。参照 ["Cloud Volumes ONTAPリリースノート"](#)お使いのCloud Volumes ONTAP のバージョンでサポートされているストレージ VM の数を確認します。

Cloud Volumes ONTAP 9.11.1 より前のすべてのバージョンでは、災害復旧に使用される 1 つのデータ提供ストレージ VM と 1 つの宛先ストレージ VM がサポートされます。ソース ストレージ VM に障害が発生した場

合、データ アクセス用に宛先ストレージ VM をアクティブ化できます。

ストレージVMを作成する

構成とライセンスの種類に基づいて、API を使用して、単一ノード システムまたは高可用性 (HA) 構成で複数のストレージ VM を作成できます。

タスク概要

APIを使用してストレージVMを作成すると、必要なネットワークインターフェースの設定とともに、コンソールは `default-data-files` NAS データ LIF から次のサービスを削除し、アウトバウンド管理接続に使用される iSCSI データ LIF に追加することで、データ ストレージ VM のポリシーを変更します。

- data-fpolicy-client
- management-ad-client
- management-dns-client
- management-ldap-client
- management-nis-client

開始する前に

コンソール エージェントには、Cloud Volumes ONTAP HA ペアのストレージ VM を作成するための特定の権限が必要です。必要な権限は以下に記載されています ["NetAppが提供するポリシー"](#)。

シングルノードシステム

次の API 呼び出しを使用して、単一ノード システムにストレージ VM を作成します。

POST /gcp/vsa/working-environments/{workingEnvironmentId}/svm

リクエスト本文に次のパラメータを含めます。

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
  "mgmtLif": "optional value, to create an additional management LIF, if
you want to use the storage VM for management purposes"}
```

HAペア

HA ペア上にストレージ VM を作成するには、次の API 呼び出しを使用します。

POST /gcp/ha/working-environments/{workingEnvironmentId}/svm/

リクエスト本文に次のパラメータを含めます。

```
{ "svmName": "NewSvmName"
  "svmPassword": "optional value, the API takes the cluster password if
not provided"
}
```

ストレージVMの管理

API を使用すると、単一ノード構成と HA 構成の両方でストレージ VM の名前を変更したり、削除したりできます。

開始する前に

コンソール エージェントには、Cloud Volumes ONTAP HA ペアのストレージ VM を管理するために特定の権限が必要です。必要な権限は以下に記載されています ["NetAppが提供するポリシー"](#)。

ストレージVMの名前を変更する

ストレージ VM の名前を変更するには、既存のストレージ VM と新しいストレージ VM の名前をパラメーターとして指定する必要があります。

手順

- 単一ノード システム上のストレージ VM の名前を変更するには、次の API 呼び出しを使用します。

```
PUT /gcp/vsa/working-environments/{workingEnvironmentId}/svm
```

リクエスト本文に次のパラメータを含めます。

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

- HA ペア上のストレージ VM の名前を変更するには、次の API 呼び出しを使用します。

```
PUT /gcp/ha/working-environments/{workingEnvironmentId}/svm
```

リクエスト本文に次のパラメータを含めます。

```
{
  "svmNewName": "NewSvmName",
  "svmName": "OldSvmName"
}
```

ストレージVMを削除する

単一ノードまたは HA 構成では、アクティブなボリュームがない場合、ストレージ VM を削除できます。

手順

- 単一ノード システム上のストレージ VM を削除するには、次の API 呼び出しを使用します。

```
DELETE /gcp/vsa/working-environments/{workingEnvironmentId}/svm/{svmName}
```

- HA ペア上のストレージ VM を削除するには、次の API 呼び出しを使用します。

```
DELETE /gcp/ha/working-environments/{workingEnvironmentId}/svm/{svmName}
```

関連情報

- ["APIを使用する準備"](#)
- ["Cloud Volumes ONTAPワークフロー"](#)
- ["必要な識別子を取得する"](#)
- ["NetAppコンソールのREST APIを使用する"](#)

Cloud Volumes ONTAPのストレージ VM 災害復旧を設定する

NetAppコンソールは、ストレージ VM (SVM) 災害復旧のセットアップやオーケストレーションのサポートを提供しません。これらのタスクを実行するには、ONTAP System Manager またはONTAP CLI を使用します。

2 つのCloud Volumes ONTAPシステム間でSnapMirror SVM レプリケーションを設定する場合、レプリケーションは 2 つの HA ペア システム間または 2 つの単一ノード システム間で実行する必要があります。HA ペアと単一ノード システム間でSnapMirror SVM レプリケーションを設定することはできません。

ONTAP CLI の手順については、次のドキュメントを参照してください。

- ["SVM Disaster Recovery Preparation Express Guide"](#)
- ["SVM Disaster Recovery Express Guide"](#)

セキュリティとデータ暗号化

NetApp暗号化ソリューションを使用して**Cloud Volumes ONTAP**上のボリュームを暗号化する

Cloud Volumes ONTAP は、NetApp Volume Encryption (NVE) とNetApp Aggregate Encryption (NAE) をサポートしています。NVE と NAE は、ボリュームの FIPS 140-2 準拠の保存データ暗号化を可能にするソフトウェア ベースのソリューションです。["これらの暗号化ソリューションについて詳しく見る"](#)。

NVE と NAE はどちらも外部キー マネージャーでサポートされます。

```
] endif::aws[] ifdef::azure[] endif::azure[] ifdef::gcp[] endif::gcp[] ifdef::aws[] endif::aws[] ifdef::azure[]  
endif::azure[] ifdef::gcp[] endif::gcp[]
```

AWS Key Management Service を使用してCloud Volumes ONTAP暗号化キーを管理する

使用できます"[AWS のキー管理サービス \(KMS\)](#)"AWS にデプロイされたアプリケーションでONTAP暗号化キーを保護します。

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

KMS を使用する場合、クラウド キー管理エンドポイントとの通信にはデフォルトでデータ SVM の LIF が使用されることに注意してください。ノード管理ネットワークは、AWS の認証サービスとの通信に使用されます。クラスタ ネットワークが正しく設定されていないと、クラスタはキー管理サービスを適切に利用できません。

開始する前に

- Cloud Volumes ONTAP はバージョン 9.12.0 以降を実行している必要があります
- ボリューム暗号化 (VE) ライセンスをインストールし、
- マルチテナント暗号化キー管理 (MTEKM) ライセンスがインストールされている必要があります。
- クラスタ管理者またはSVM管理者である必要があります。
- 有効なAWSサブスクリプションが必要です



データ SVM のキーのみを設定できます。

構成

AWS

1. 作成する必要があります"[付与](#)"暗号化を管理する IAM ロールによって使用される AWS KMS キー用。IAM ロールには、次の処理を許可するポリシーが含まれている必要があります。
 - DescribeKey
 - Encrypt
 - Decrypt 助成金を作成するには、"[AWSのドキュメント](#)"。
2. "[適切な IAM ロールにポリシーを追加します。](#)"この政策は、DescribeKey、Encrypt、そして Decrypt 操作。

Cloud Volumes ONTAP

1. Cloud Volumes ONTAP環境に切り替えます。
2. 高度な権限レベルに切り替えます:
`set -privilege advanced`
3. AWS キーマネージャーを有効にします。
`security key-manager external aws enable -vserver data_svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. プロンプトが表示されたら、シークレット キーを入力します。
5. AWS KMS が正しく設定されていることを確認します。
`security key-manager external aws show -vserver svm_name`

Azure Key Vault を使用してCloud Volumes ONTAP暗号化キーを管理する

Azure Key Vault (AKV) を使用して、Azure にデプロイされたアプリケーション内のONTAP暗号化キーを保護できます。参照["Microsoftのドキュメント"](#)。

AKV は、データ SVM のNetApp Volume Encryption (NVE) キーを保護するためにのみ使用できます。詳細については、["ONTAPのドキュメント"](#)。

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

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

開始する前に

- Cloud Volumes ONTAP はバージョン 9.10.1 以降を実行している必要があります
- ボリューム暗号化 (VE) ライセンスがインストールされている (NetAppボリューム暗号化ライセンスは、NetAppサポートに登録されている各Cloud Volumes ONTAPシステムに自動的にインストールされます)
- マルチテナント暗号化キー管理 (MT_EK_MGMT) ライセンスが必要です
- クラスタ管理者またはSVM管理者である必要があります。
- アクティブなAzureサブスクリプション

制限事項

- AKVはデータSVMでのみ構成できます
- NAE は AKV では使用できません。NAE には外部でサポートされている KMIP サーバーが必要です。
- Cloud Volumes ONTAPノードは、アクセス可能性とキーの可用性を確認するために 15 分ごとに AKV をポーリングします。このポーリング期間は構成不可能であり、ポーリング試行が 4 回連続して失敗すると (合計 1 時間)、ボリュームはオフラインになります。

構成プロセス

概要を説明する手順では、Cloud Volumes ONTAP構成を Azure に登録する方法と、Azure Key Vault とキーを作成する方法について説明します。これらの手順をすでに完了している場合は、特に以下の設定が正しいことを確認してください。[Azure Key Vault を作成する](#)、次に進みましょう[Cloud Volumes ONTAP構成](#)。

- [Azure アプリケーション登録](#)
- [Azureクライアントシークレットを作成する](#)
- [Azure Key Vault を作成する](#)
- [暗号化キーを作成する](#)
- [Azure Active Directory エンドポイントを作成する \(HA のみ\)](#)
- [Cloud Volumes ONTAP構成](#)

Azure アプリケーション登録

1. まず、Cloud Volumes ONTAP がAzure Key Vault にアクセスするために使用する Azure サブスクリプション

ョンにアプリケーションを登録する必要があります。Azure ポータル内で、アプリの登録 を選択します。

2. 新規登録を選択します。
3. アプリケーションの名前を指定し、サポートされているアプリケーションの種類を選択します。Azure Key Vault の使用には、デフォルトの単一テナントで十分です。登録を選択します。
4. Azure の概要ウィンドウで、登録したアプリケーションを選択します。アプリケーション (クライアント) ID と ディレクトリ (テナント) ID を安全な場所にコピーします。これらは、登録プロセスの後半で必要になります。

Azureクライアントシークレットを作成する

1. Azure Key Vault アプリ登録用の Azure portal で、[証明書とシークレット] ペインを選択します。
2. 新しいクライアント シークレット を選択します。クライアント シークレットに意味のある名前を入力します。NetApp24 か月の有効期限を推奨していますが、特定のクラウド ガバナンス ポリシーによっては異なる設定が必要になる場合があります。
3. 追加 をクリックしてクライアント シークレットを作成します。値列にリストされている秘密の文字列をコピーし、後で使用するために安全な場所に保存します。[Cloud Volumes ONTAP構成](#)。ページから移動すると、秘密の値は再び表示されなくなります。

Azure Key Vault を作成する

1. 既存の Azure Key Vault がある場合は、それをCloud Volumes ONTAP構成に接続できます。ただし、このプロセスではアクセス ポリシーを設定に合わせて調整する必要があります。
2. Azure ポータルで、**Key Vaults** セクションに移動します。
3. [+ 作成] をクリックし、リソース グループ、リージョン、価格レベルなどの必要な情報を入力します。さらに、削除されたコンテナを保持する日数を入力し、キー コンテナで [消去保護を有効にする] を選択します。
4. アクセス ポリシーを選択するには、[次へ] を選択します。
5. 次のオプションを選択します。
 - a. アクセス構成 で、**Vault** アクセス ポリシー を選択します。
 - b. リソース アクセス で、ボリューム暗号化用の **Azure Disk Encryption** を選択します。
6. アクセス ポリシーを追加するには、[+ 作成] を選択します。
7. テンプレートから構成 の下で、ドロップダウン メニューをクリックし、キー、シークレット、および証明書の管理 テンプレートを選択します。
8. 各ドロップダウン権限メニュー (キー、シークレット、証明書) を選択し、メニュー リストの上部にある [すべて選択] をクリックして、使用可能なすべての権限を選択します。次のものがが必要です:
 - キー権限: 20個選択済み
 - 秘密の権限: 8 個選択済み
 - 証明書の権限: 16 個選択済み

Create an access policy



- 1 Permissions 2 Principal 3 Application (optional) 4 Review + create

Configure from a template

Key, Secret, & Certificate Management

Key permissions

Key Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Cryptographic Operations

- ☒ Select all
- ☒ Decrypt
- ☒ Encrypt
- ☒ Unwrap Key
- ☒ Wrap Key
- ☒ Verify
- ☒ Sign

Privileged Key Operations

- ☒ Select all
- ☒ Purge
- ☒ Release

Rotation Policy Operations

- ☒ Select all
- ☒ Rotate
- ☒ Get Rotation Policy
- ☒ Set Rotation Policy

Secret permissions

Secret Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Set
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore

Privileged Secret Operations

- ☒ Select all
- ☒ Purge

Certificate permissions

Certificate Management Operations

- ☒ Select all
- ☒ Get
- ☒ List
- ☒ Update
- ☒ Create
- ☒ Import
- ☒ Delete
- ☒ Recover
- ☒ Backup
- ☒ Restore
- ☒ Manage Contacts
- ☒ Manage Certificate Authorities
- ☒ Get Certificate Authorities
- ☒ List Certificate Authorities
- ☒ Set Certificate Authorities
- ☒ Delete Certificate Authorities

Privileged Certificate Operations

- ☒ Select all
- ☒ Purge

Previous

Next

9. 次へ をクリックして、プリンシパル Azure登録アプリケーションを選択します。Azure アプリケーション登録。次へを選択します。



ポリシーごとに割り当てることができるプリンシパルは 1 つだけです。

Create an access policy

Permissions

2 Principal

3 Application (optional)

4 Review + create

Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. [Select a principal](#)

Search by object ID, name, or email address

Selected item
No item selected

Previous

Next

10. [確認と作成] に到達するまで [次へ] を 2 回クリックします。次に、[作成] をクリックします。
11. 次へ を選択して、ネットワーク オプションに進みます。
12. 適切なネットワーク アクセス方法を選択するか、すべてのネットワーク と 確認 + 作成 を選択してキーコンテナを作成します。(ネットワーク アクセス方法は、ガバナンス ポリシーまたは企業のクラウドセキュリティ チームによって規定される場合があります。)
13. Key Vault URI を記録します。作成した Key Vault で、[概要] メニューに移動し、右側の列から **Vault URI** をコピーします。これは後のステップで必要になります。

暗号化キーを作成する

1. Cloud Volumes ONTAP用に作成した Key Vault のメニューで、[Keys] オプションに移動します。
2. 新しいキーを作成するには、[生成/インポート] を選択します。
3. デフォルト オプションは [生成] に設定したままにします。
4. 次の情報を入力します。

- 暗号化キー名
- キータイプ: RSA
- RSA鍵サイズ: 2048
- 有効: はい

5. 暗号化キーを作成するには、[作成] を選択します。
6. キー メニューに戻り、作成したキーを選択します。
7. キーのプロパティを表示するには、[現在のバージョン] の下のキー ID を選択します。
8. キー識別子 フィールドを見つけます。URI を 16 進文字列までコピーします (16 進文字列は含まれません)。

Azure Active Directory エンドポイントを作成する (HA のみ)

1. このプロセスは、HA Cloud Volumes ONTAPシステム用に Azure Key Vault を構成する場合にのみ必要です。
2. Azure ポータルで、仮想ネットワーク に移動します。
3. Cloud Volumes ONTAPシステムを導入した仮想ネットワークを選択し、ページの左側にある [サブネット] メニューを選択します。
4. リストからCloud Volumes ONTAPデプロイメントのサブネット名を選択します。
5. サービス エンドポイント の見出しに移動します。ドロップダウン メニューで、以下を選択します。
 - **Microsoft.AzureActiveDirectory**
 - **Microsoft.KeyVault**
 - **Microsoft.Storage** (オプション)

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

3 selected

Service	Status	
Microsoft.Storage	Succeeded	
Microsoft.AzureActiveDirectory	Succeeded	
Microsoft.KeyVault	Succeeded	

Service endpoint policies

0 selected

SUBNET DELEGATION

Delegate subnet to a service ⓘ

None

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled

Save

Cancel

6. 設定を保存するには、[保存] を選択します。

Cloud Volumes ONTAP構成

1. 好みの SSH クライアントを使用してクラスタ管理 LIF に接続します。
2. ONTAPで高度な権限モードに入ります。

```
set advanced -con off
```

3. 必要なデータ SVM を識別し、その DNS 構成を確認します。

```
vserver services name-service dns show
```

- a. 目的のデータ SVM の DNS エントリが存在し、それに Azure DNS のエントリが含まれている場合は、アクションは必要ありません。そうでない場合は、Azure DNS、プライベート DNS、またはオンプレミス サーバーを指すデータ SVM の DNS サーバー エントリを追加します。これは、クラスタ管理 SVM のエントリと一致する必要があります。

```
vserver services name-service dns create -vserver SVM_name -domains domain  
-name-servers IP_address
```

- b. データ SVM に対して DNS サービスが作成されたことを確認します。

```
vserver services name-service dns show
```

4. アプリケーションの登録後に保存されたクライアント ID とテナント ID を使用して Azure Key Vault を有効にします。

```
security key-manager external azure enable -vserver SVM_name -client-id  
Azure_client_ID -tenant-id Azure_tenant_ID -name key_vault_URI -key-id  
full_key_URI
```



その `full\_key\_URI` 値を活用する必要がある `[https:// <key vault host name>/keys/<key label>](https://<key vault host name>/keys/<key label>)` 形式。

5. Azure Key Vaultの有効化に成功したら、`client secret value` プロンプトが表示されたら。

6. キー マネージャーのステータスを確認します。

`security key-manager external azure check` 出力は次のようになります。

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

```
Vserver: data_svm_name
```

```
Node: akvlab01-01
```

```
Category: service_reachability
```

```
Status: OK
```

```
Category: ekvip_server
```

```
Status: OK
```

```
Category: kms_wrapped_key_status
```

```
Status: UNKNOWN
```

```
Details: No volumes created yet for the vserver. Wrapped KEK status  
will be available after creating encrypted volumes.
```

```
3 entries were displayed.
```

もし `service\_reachability` ステータスは `OK` SVM は、必要なすべての接続とアクセス許可を備えて Azure Key Vault サービスにアクセスできません。Azure ネットワーク ポリシーとルーティングによって、プライベート vNet が Azure Key Vault パブリック エンドポイントに到達するのがブロックされないようにしてください。そうなる場合は、Azure プライベート エンドポイントを使用して、vNet 内から

Key Vault にアクセスすることを検討してください。エンドポイントのプライベート IP アドレスを解決するには、SVM に静的ホスト エントリを追加する必要があります。

その `kms\_wrapped\_key\_status` 報告します `UNKNOWN` 初期設定時。ステータスは次のように変わります `OK` 最初のボリュームが暗号化された後。

7. オプション: NVE の機能を検証するためのテスト ボリュームを作成します。

```
vol create -vserver SVM_name -volume volume_name -aggregate aggr -size size  
-state online -policy default
```

正しく設定されていれば、Cloud Volumes ONTAP は自動的にボリュームを作成し、ボリュームの暗号化を有効にします。

8. ボリュームが正しく作成され、暗号化されていることを確認します。もしそうなら、`-is-encrypted` パラメータは次のように表示されます `true`。

```
vol show -vserver SVM_name -fields is-encrypted
```

9. オプション: Azure Key Vault 認証証明書の資格情報を更新する場合は、次のコマンドを使用します。

```
security key-manager external azure update-credentials -vserver v1  
-authentication-method certificate
```

関連リンク

- ["Azureで顧客管理キーを使用するようにCloud Volumes ONTAPを設定する"](#)
- ["Microsoft Azure ドキュメント: Azure Key Vault について"](#)
- ["ONTAPコマンドリファレンスガイド"](#)

Google Cloud KMS でCloud Volumes ONTAP の暗号化キーを管理する

使用できます["Google Cloud Platform の鍵管理サービス \(Cloud KMS\)"](#) Google Cloud Platform にデプロイされたアプリケーションでCloud Volumes ONTAP暗号化キーを保護します。

Cloud KMS によるキー管理は、ONTAP CLI またはONTAP REST API を使用して有効にできます。

Cloud KMS を使用する場合、デフォルトではデータ SVM の LIF を使用してクラウド キー管理エンドポイントと通信することに注意してください。ノード管理ネットワークは、クラウド プロバイダーの認証サービス (oauth2.googleapis.com) との通信に使用されます。クラスター ネットワークが正しく設定されていないと、クラスターはキー管理サービスを適切に利用できません。

開始する前に

- システムではCloud Volumes ONTAP 9.10.1以降が実行されている必要があります
- データ SVM を使用する必要があります。Cloud KMS はデータ SVM でのみ構成できます。
- クラスター管理者またはSVM管理者である必要があります。
- ボリューム暗号化 (VE) ライセンスをSVMにインストールする必要があります
- Cloud Volumes ONTAP 9.12.1 GA以降では、マルチテナント暗号化キー管理 (MTEKM) ライセンスもインストールする必要があります。
- 有効な Google Cloud Platform サブスクリプションが必要です

構成

Google Cloud

1. Google Cloud環境では、["対称GCPキーリングとキーを作成する"](#)。
2. Cloud KMS キーとCloud Volumes ONTAPサービス アカウントにカスタム ロールを割り当てます。
 - a. カスタム ロールを作成します。

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

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

- b. 作成したカスタム ロールを割り当てます。

```
gcloud kms keys add-iam-policy-binding key_name --keyring key_ring_name
  --location key_location --member serviceAccount:_service_account_Name_
  --role projects/customer_project_id/roles/kmsCustomRole
```



Cloud Volumes ONTAP 9.13.0 以降を使用している場合は、カスタム ロールを作成する必要はありません。定義済みの[cloudkms.cryptoKeyEncrypterDecrypter^]の役割。

3. サービス アカウントの JSON キーをダウンロードします:

```
gcloud iam service-accounts keys create key-file --iam-account=sa-name
@project-id.iam.gserviceaccount.com
```

Cloud Volumes ONTAP

1. 好みの SSH クライアントを使用してクラスタ管理 LIF に接続します。
2. 高度な権限レベルに切り替えます:
`set -privilege advanced`
3. データ SVM の DNS を作成します。
`dns create -domains c.<project>.internal -name-servers server_address -vserver SVM_name`
4. CMEK エントリを作成します。
`security key-manager external gcp enable -vserver SVM_name -project-id project -key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
5. プロンプトが表示されたら、GCP アカウントのサービス アカウント JSON キーを入力します。
6. 有効化されたプロセスが成功したことを確認します。

```
security key-manager external gcp check -vserver svm_name
```

7. オプション: 暗号化をテストするためのボリュームを作成する `vol create volume_name -aggregate aggregate -vserver vserver_name -size 10G`

トラブルシューティング

トラブルシューティングが必要な場合は、上記の最後の 2 つの手順で生の REST API ログを tail できます。

1. `set d`
2. `systemshell -node node -command tail -f /mroot/etc/log/mlog/kmip2_client.log`

Cloud Volumes ONTAPでNetAppランサムウェア保護ソリューションを有効にする

ランサムウェア攻撃は、企業の時間、リソース、評判に損害を与える可能性があります。NetAppコンソールを使用すると、一般的なランサムウェア ファイル拡張子からの保護と自律ランサムウェア保護 (ARP) という 2 つのランサムウェア対策NetAppソリューションを実装できます。これらのソリューションは、可視性、検出、修復のための効果的なツールを提供します。

一般的なランサムウェアのファイル拡張子からの保護

コンソールで利用可能なランサムウェア保護設定を使用すると、ONTAP FPolicy 機能を利用して、一般的なランサムウェアのファイル拡張子タイプから保護することができます。

手順

1. *システム*ページで、ランサムウェア保護を使用するように構成したCloud Volumes ONTAPシステムの名前をダブルクリックします。
2. [概要] タブで [機能] パネルをクリックし、[ランサムウェア保護] の横にある鉛筆アイコンをクリックします。

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. ランサムウェアに対するNetAppソリューションを実装します。

- a. スナップショット ポリシーが有効になっていないボリュームがある場合は、[スナップショット ポリシーのアクティブ化] をクリックします。

NetApp Snapshot テクノロジーは、ランサムウェア修復のための業界最高のソリューションを提供します。復旧を成功させる鍵は、感染していないバックアップから復元することです。スナップショット コピーは読み取り専用であるため、ランサムウェアによる破損を防ぎます。また、単一のファイルコピーまたは完全な災害復旧ソリューションのイメージを作成するための細分性も提供できます。

- b. **FPolicy** のアクティブ化 をクリックして、ファイルの拡張子に基づいてファイル操作をブロックできる ONTAP の FPolicy ソリューションを有効にします。

この予防ソリューションは、一般的なランサムウェア ファイルの種類をブロックすることで、ランサムウェア攻撃からの保護を強化します。

デフォルトの FPolicy スコープは、次の拡張子を持つファイルをブロックします。

micro、暗号化、ロック、暗号、crypt、crinf、r5a、XRNT、XTBL、R16M01D05、pzdc、良い、LOL!、OMG!、RDM、RRK、encryptedRS、crjoker、EnCiPhErEd、LeChiffre



このスコープは、Cloud Volumes ONTAPで FPolicy をアクティブ化すると作成されます。リストは、一般的なランサムウェアのファイルタイプに基づいています。Cloud Volumes ONTAP CLI の `vserver fpolicy policy scope` コマンドを使用して、ブロックされるファイル拡張子をカスタマイズできます。

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection ⓘ

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes ⓘ

Activate Snapshot Policy

2 Block Ransomware File Extensions ⓘ

ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names ⓘ](#)

Activate FPolicy

自律型ランサムウェア対策

Cloud Volumes ONTAP は、ワークロードを分析して、ランサムウェア攻撃の兆候となる可能性のある異常なアクティビティをプロアクティブに検出し、警告する Autonomous Ransomware Protection (ARP) 機能をサポートしています。

提供されるファイル拡張子保護とは別に、"[ランサムウェア保護設定](#)" ARP 機能はワークロード分析を使用して、検出された「異常なアクティビティ」に基づいて潜在的な攻撃をユーザーに警告します。ランサムウェア保護設定と ARP 機能の両方を組み合わせて使用することで、包括的なランサムウェア保護を実現できます。

ARP 機能は、BYOL (個人ライセンス使用) およびマーケットプレイス サブスクリプションで追加料金なしでご利用いただけます。

ARP 対応ボリュームには、「学習モード」または「アクティブ」という指定状態があります。

ボリュームの ARP の設定は、ONTAP System Manager および ONTAP CLI を通じて実行されます。

ONTAP System Manager および ONTAP CLI で ARP を有効にする方法の詳細については、"[ONTAP ドキュメント: 自律型ランサムウェア保護の有効化](#)"。

Autonomous Ransomware Protection ⓘ

0 TiB

Protected Capacity

100 TiB

Precommitted capacity

0 TiB

PAYGO

BYOL

100 TiB

Marketplace Contracts

0 TiB

Cloud Volumes ONTAPで WORM ファイルの改ざん防止スナップショット コピーを作成します

Cloud Volumes ONTAPシステムで、一度だけ書き込み、何度も読み取る (WORM) ファイルの改ざん防止スナップショット コピーを作成し、特定の保持期間にわたってスナップショットを変更されていない形式で保持することができます。この機能はSnapLockテクノロジーを活用しており、データ保護とコンプライアンスをさらに強化します。

開始する前に

スナップショット コピーの作成に使用するボリュームがSnapLockボリュームであることを確認します。ボリューム上でSnapLock保護を有効にする方法については、["ONTAPドキュメント: SnapLockの設定"](#)。

手順

1. SnapLockボリュームからスナップショット コピーを作成します。CLIまたはSystem Managerを使用してスナップショットコピーを作成する方法については、["ONTAPドキュメント: ローカルスナップショットコピーの管理の概要"](#)。

スナップショット コピーはボリュームの WORM プロパティを継承し、改ざん防止になります。基盤となるSnapLockテクノロジーにより、指定された保持期間が経過するまで、スナップショットは編集や削除から保護されます。

2. これらのスナップショットを編集する必要がある場合は、保持期間を変更できます。詳細については、["ONTAPドキュメント: 保持期間を設定する"](#)。



スナップショット コピーは特定の保持期間保護されていますが、Cloud Volumes ONTAPの WORM ストレージは「信頼できるストレージ管理者」モデルで動作するため、クラスター管理者はソース ボリュームを削除できます。さらに、信頼できるクラウド管理者は、クラウド ストレージ リソースを操作して WORM データを削除できます。

システム管理

Cloud Volumes ONTAPソフトウェアのアップグレード

NetAppコンソールからCloud Volumes ONTAP をアップグレードして、最新の新機能と拡張機能にアクセスします。ソフトウェアをアップグレードする前に、Cloud Volumes ONTAPシステムを準備する必要があります。

アップグレードの概要

Cloud Volumes ONTAP のアップグレード プロセスを開始する前に、次の点に注意してください。

コンソールからのみアップグレード

Cloud Volumes ONTAP は、ONTAP System Manager またはONTAP CLI ではなく、コンソールのみを使用してアップグレードする必要があります。そうしないと、システムの安定性に影響する可能性があります。

アップグレード方法

コンソールでは、Cloud Volumes ONTAPをアップグレードする方法が2 つあります。

- ・システムに表示されるアップグレード通知に従うことで
- ・アップグレードイメージをHTTPSの場所に配置し、コンソールにURLを提供することで

サポートされているアップグレード パス

アップグレードできるCloud Volumes ONTAPのバージョンは、現在実行しているCloud Volumes ONTAPのバージョンによって異なります。

現在のバージョン	直接アップグレードできるバージョン
9.16.1 (Azure および Google Cloud のみ)	9.17.1 (Azure および Google Cloud のみ)
9.15.1	9.16.1 (Azure および Google Cloud のみ)
9.15.0	9.15.1
9.14.1	9.15.1
	9.15.0
9.14.0	9.14.1
9.13.1	9.14.1
	9.14.0
9.13.0	9.13.1
9.12.1	9.13.1
	9.13.0
9.12.0	9.12.1

現在のバージョン	直接アップグレードできるバージョン
9.11.1	9.12.1
	9.12.0
9.11.0	9.11.1
9.10.1	9.11.1
	9.11.0
9.10.0	9.10.1
9.9.1	9.10.1
	9.10.0
9.9.0	9.9.1
9.8	9.9.1
9.7	9.8
9.6	9.7
9.5	9.6
9.4	9.5
9.3	9.4
9.2	9.3
9.1	9.2
9.0	9.1
8.3	9.0

次の点に注意してください。

- Cloud Volumes ONTAPでサポートされているアップグレード パスは、オンプレミスのONTAPクラスターの場合とは異なります。
- システムに表示される通知に従ってアップグレードする場合、コンソールは、サポートされているアップグレード パスに従うリリースにアップグレードするように要求します。
- アップグレード イメージを HTTPS の場所に配置してアップグレードする場合は、サポートされているアップグレード パスに必ず従ってください。
- 場合によっては、目標リリースに到達するまでに数回のアップグレードが必要になることがあります。

たとえば、バージョン 9.8 を実行していて、9.10.1 にアップグレードする場合は、最初にバージョン 9.9.1 にアップグレードし、次に 9.10.1 にアップグレードする必要があります。

パッチリリース

2024 年 1 月以降、パッチ アップグレードは、Cloud Volumes ONTAPの最新の 3 つのバージョンのパッチ リリースがある場合にのみ利用できます。RC バージョンまたは GA バージョンが展開に使用できない場合、パッチ バージョンが展開に使用できるようになることがあります。

最新の GA リリースを使用して、コンソールに表示する最新の 3 つのバージョンを決定します。たとえば、現在の GA リリースが 9.13.1 の場合、コンソールには 9.11.1 ～ 9.13.1 のパッチが表示されます。バージョン 9.11.1 以下のパッチリリースにアップグレードする場合は、以下の手動アップグレード手順に従う必要があります。[ONTAP イメージのダウンロード](#)。

パッチ (P) リリースの一般的なルールとして、1 つのバージョン リリースから、現在実行中のバージョンまたは次のバージョンの任意の P リリースにアップグレードできます。

以下にいくつかの例を挙げます。

- 9.13.0 > 9.13.1P15
- 9.12.1 > 9.13.1P2

元に戻すまたはダウングレードする

Cloud Volumes ONTAP を以前のリリースに戻したりダウングレードしたりすることはサポートされていません。

サポート登録

このページに記載されているいずれかの方法を使用してソフトウェアをアップグレードするには、Cloud Volumes ONTAP を NetApp サポートに登録する必要があります。これは、従量課金制 (PAYGO) とライセンス持ち込み (BYOL) の両方に適用されます。必要となるのは["PAYGO システムを手動で登録する"](#) BYOL システムはデフォルトで登録されます。



サポートに登録されていないシステムでも、新しいバージョンが利用可能になったときにコンソールに表示されるソフトウェア更新通知を受信します。ただし、ソフトウェアをアップグレードする前にシステムを登録する必要があります。

HA メディエーターのアップグレード

コンソールは、Cloud Volumes ONTAP のアップグレード プロセス中に必要に応じてメディエーター インスタンスも更新します。

AWS の c4、m4、r4 EC2 インスタンスタイプのアップグレード

Cloud Volumes ONTAP は、c4、m4、および r4 EC2 インスタンス タイプをサポートしなくなりました。これらのインスタンス タイプを使用して、既存のデプロイメントを Cloud Volumes ONTAP バージョン 9.8 ～ 9.12.1 にアップグレードできます。アップグレードする前に、[インスタンスタイプを変更する](#)。インスタンスタイプを変更できない場合は、[拡張ネットワークを有効にする](#)アップグレードする前に。インスタンスタイプの変更と拡張ネットワークの有効化の詳細については、次のセクションをお読みください。

バージョン 9.13.0 以降を実行している Cloud Volumes ONTAP では、c4、m4、および r4 EC2 インスタンス タイプを使用してアップグレードすることはできません。この場合は、ディスクの数を減らしてから[インスタンスタイプを変更する](#)または、c5、m5、r5 EC2 インスタンス タイプを使用して新しい HA ペア構成を展開し、データを移行します。

インスタンスタイプを変更する

c4、m4、r4 EC2 インスタンス タイプでは、c5、m5、r5 EC2 インスタンス タイプよりもノードあたりのディスク数が多くなります。実行中の c4、m4、または r4 EC2 インスタンスのノードあたりのディスク数が、c5、m5、および r5 インスタンスのノードあたりの最大ディスク許容量を下回っている場合は、EC2 インスタンスタイプを c5、m5、または r5 に変更できます。

"EC2インスタンスごとにディスクと階層化の制限を確認する" "Cloud Volumes ONTAPのEC2インスタンスタイプを変更する"

インスタンスタイプを変更できない場合は、[\[拡張ネットワークを有効にする\]](#)。

拡張ネットワークを有効にする

Cloud Volumes ONTAPバージョン 9.8 以降にアップグレードするには、c4、m4、または r4 インスタンスタイプを実行しているクラスターで拡張ネットワークを有効にする必要があります。ENAを有効にするには、ナレッジベースの記事を参照してください。"[AWS Cloud Volumes ONTAPインスタンスでSR-IOVやENAなどの拡張ネットワークを有効にする方法](#)"。

アップグレードの準備

アップグレードを実行する前に、システムの準備ができていることを確認し、必要な構成の変更を行う必要があります。

- [\[ダウンタイムを計画する\]](#)
- [\[自動ギブバックがまだ有効になっていることを確認します\]](#)
- SnapMirror転送を一時停止する
- [\[集計がオンラインであることを確認する\]](#)
- [すべてのLIFがホームポートにあることを確認する](#)

ダウンタイムを計画する

単一ノード システムをアップグレードする場合、アップグレード プロセスによりシステムが最大 25 分間オフラインになり、その間に I/O が中断されます。

多くの場合、HA ペアのアップグレードは中断を伴わず、I/O も中断されません。この中断のないアップグレード プロセスでは、各ノードが同時にアップグレードされ、クライアントへの I/O の提供が継続されます。

セッション指向プロトコルは、アップグレード中に特定の領域のクライアントとアプリケーションに悪影響を及ぼす可能性があります。詳細については、"[ONTAPのドキュメント](#)"

自動ギブバックがまだ有効になっていることを確認します

Cloud Volumes ONTAP HA ペアでは自動ギブバックを有効にする必要があります (これがデフォルト設定です)。そうでない場合、操作は失敗します。

"ONTAPドキュメント: 自動ギブバックを設定するためのコマンド"

SnapMirror転送を一時停止する

Cloud Volumes ONTAPシステムにアクティブなSnapMirror関係がある場合は、Cloud Volumes ONTAPソフトウェアを更新する前に転送を一時停止することをお勧めします。転送を一時停止すると、SnapMirror の障害を防ぐことができます。宛先システムからの転送を一時停止する必要があります。



NetApp Backup and Recovery はSnapMirrorの実装を使用してバックアップ ファイル (SnapMirror Cloud と呼ばれる) を作成しますが、システムのアップグレード時にバックアップを中断する必要はありません。

タスク概要

これらの手順では、バージョン 9.3 以降のONTAP System Manager を使用方法について説明します。

手順

1. 宛先システムから System Manager にログインします。

Web ブラウザでクラスタ管理 LIF の IP アドレスを指定すると、System Manager にログインできます。
IP アドレスはCloud Volumes ONTAPシステムで確認できます。



コンソールにアクセスするコンピューターは、Cloud Volumes ONTAPへのネットワーク接続が必要です。たとえば、クラウド プロバイダー ネットワーク内のジャンプ ホストからコンソールにログインする必要がある場合があります。

2. *保護 > 関係*をクリックします。
3. 関係を選択し、*操作 > 静止*をクリックします。

集計がオンラインであることを確認する

ソフトウェアを更新する前に、Cloud Volumes ONTAPのアグリゲートがオンラインになっている必要があります。ほとんどの構成ではアグリゲートはオンラインになるはずですが、そうでない場合はオンラインにする必要があります。

タスク概要

これらの手順では、バージョン 9.3 以降のONTAP System Manager を使用方法について説明します。

手順

1. Cloud Volumes ONTAPシステムで、**[Aggregates]** タブをクリックします。
2. 必要な集計タイルで、...アイコンをクリックし、[集計の詳細を表示] を選択します。

Aggregate Details
aggr1

Overview	Capacity Allocation	Provider Properties
State	online	
Home Node	shimadzu-01	
Encryption Type	cloudEncrypted	
Volumes	2	▼

3. アグリゲートがオフラインの場合は、ONTAP System Manager を使用してアグリゲートをオンラインにします。

- a. *ストレージ > アグリゲートとディスク > アグリゲート*をクリックします。
- b. 集約を選択し、*その他のアクション > ステータス > オンライン*をクリックします。

すべてのLIFがホームポートにあることを確認する

アップグレードする前に、すべての LIF がホーム ポート上にある必要があります。ONTAPのドキュメントを参照してください。["すべてのLIFがホームポートにあることを確認する"](#)。

アップグレード失敗エラーが発生した場合は、ナレッジベース（KB）の記事を参照してください。["Cloud Volumes ONTAPのアップグレードが失敗する"](#)。

Cloud Volumes ONTAP のアップグレード

新しいバージョンがアップグレード可能になると、コンソールから通知されます。この通知からアップグレード プロセスを開始できます。詳細については、以下を参照してください。[\[コンソールからのアップグレード通知\]](#)。

外部 URL 上のイメージを使用してソフトウェア アップグレードを実行する別の方法。このオプションは、コンソールがソフトウェアをアップグレードするために S3 バケットにアクセスできない場合、またはパッチが提供された場合に役立ちます。詳細については、以下を参照してください。[URL で入手可能なイメージからアップグレードする](#)。

コンソールからのアップグレード通知

Cloud Volumes Cloud Volumes ONTAPの新しいバージョンが利用可能になると、コンソールにCloud Volumes ONTAP の作業環境に通知が表示されます。



通知を通じてCloud Volumes ONTAPをアップグレードする前に、NetAppサポート サイト アカウントが必要です。

この通知からアップグレード プロセスを開始できます。このプロセスでは、S3 バケットからソフトウェア イメージを取得し、イメージをインストールして、システムを再起動することでプロセスが自動化されます。

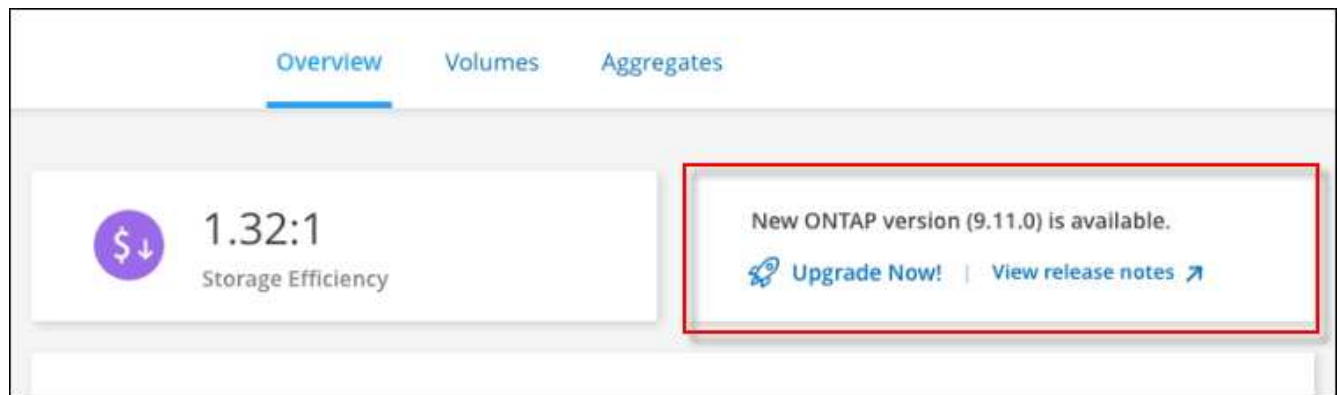
開始する前に

Cloud Volumes ONTAPシステムでは、ボリュームやアグリゲートの作成などの操作が進行中であってはなりません。

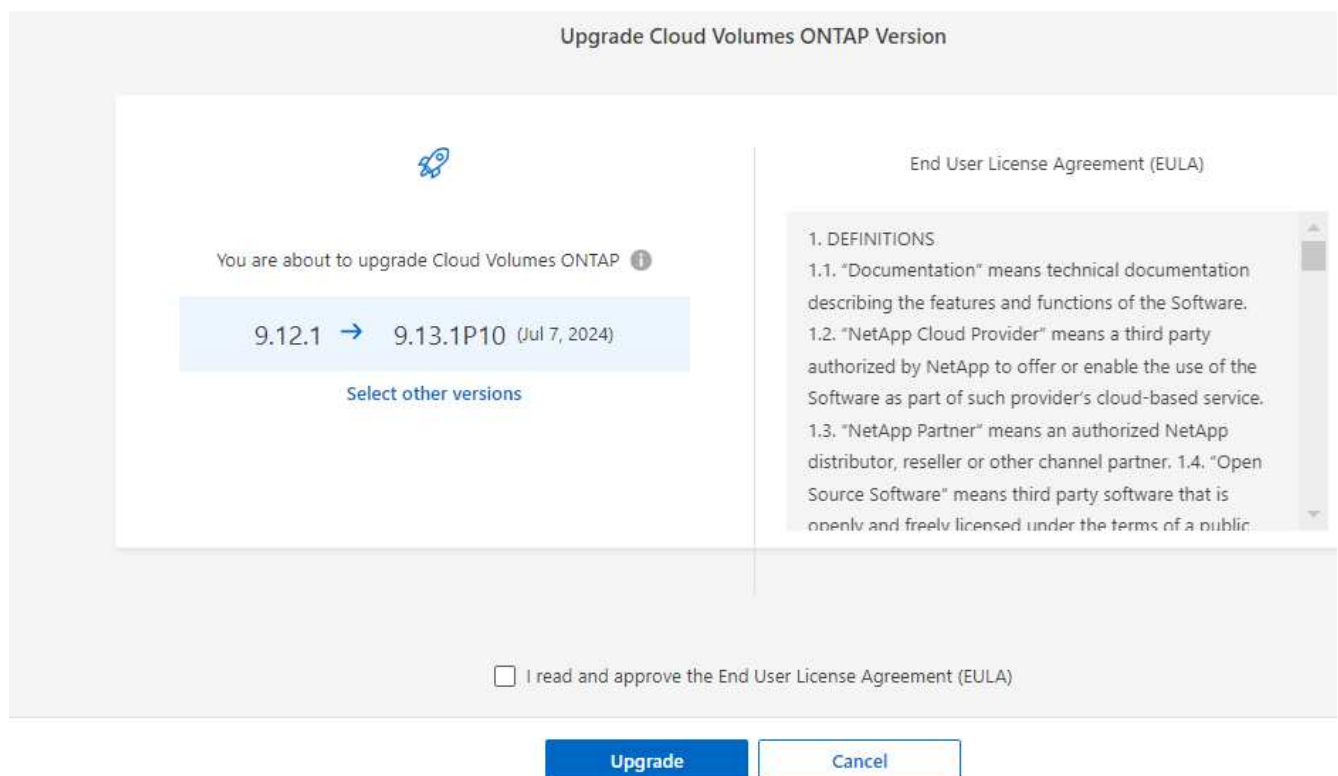
手順

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. Cloud Volumes ONTAPシステムを選択します。

新しいバージョンが利用可能な場合は、[概要] タブに通知が表示されます。



3. インストールされているCloud Volumes ONTAPのバージョンをアップグレードする場合は、[今すぐアップグレード] をクリックします。デフォルトでは、アップグレード用に最新の互換性のあるバージョンが表示されます。



別のバージョンにアップグレードする場合は、「他のバージョンを選択」をクリックします。システムにインストールされているバージョンと互換性のある最新のCloud Volumes ONTAPバージョンがリストされます。たとえば、システムにインストールされているバージョンが 9.12.1P3 で、次の互換性のあるバージョンが利用可能です。

- 9.12.1P4～9.12.1P14
- 9.13.1 および 9.13.1P1 アップグレードのデフォルト バージョンとして 9.13.1P1 が表示され、その他の使用可能なバージョンとして 9.12.1P13、9.13.1P14、9.13.1、および 9.13.1P1 が表示されます。

4. オプションで、[すべてのバージョン] をクリックして、アップグレードする別のバージョン (インストールされているバージョンの次のパッチなど) を入力することもできます。現在のCloud Volumes ONTAPバージョンの互換性のあるアップグレードパスについては、以下を参照してください。"サポートされているアップグレード パス"。

5. **【保存】***をクリックし、**【適用】***をクリックしま

Select the ONTAP version you want to upgrade to:

Version	Date
☐ 9.12.1P14	Aug 22, 2024
☐ 9.12.1P13	Jul 7, 2024
☐ 9.13.1P10	Jul 7, 2024
☐ 9.13.1P9	May 9, 2024

☒ All versions

Write the version you want to upgrade to:

Write the version here

Save Cancel

Apply Cancel

す。

- Cloud Volumes ONTAP のアップグレードページで、EULA を読み、***EULA を読んで承認します***を選択します。
- *アップグレード***を選択します。
- 進行状況を表示するには、Cloud Volumes ONTAPシステムで **Audit** を選択します。

結果

コンソールはソフトウェアのアップグレードを開始します。ソフトウェアの更新が完了すると、システム上でアクションを実行できます。

終了後の操作

SnapMirror転送を一時停止した場合は、System Manager を使用して転送を再開します。

URL で入手可能なイメージからアップグレードする

Cloud Volumes ONTAPソフトウェア イメージをコンソール エージェントまたは HTTP サーバーに配置し、コンソールからソフトウェア アップグレードを開始できます。コンソールが S3 バケットにアクセスできず、ソフトウェアをアップグレードできない場合は、このオプションを使用できます。

開始する前に

- Cloud Volumes ONTAPシステムでは、ボリュームやアグリゲートの作成などの操作が進行中であってはなりません。
- HTTPS を使用してONTAPイメージをホストする場合、証明書の不足によって発生する SSL 認証の問題により、アップグレードが失敗する可能性があります。回避策としては、ONTAPとコンソール間の認証に使用する CA 署名付き証明書を生成してインストールします。

NetAppナレッジベースにアクセスして、手順ごとの説明を参照してください。

["NetApp KB: アップグレードイメージをホストする HTTPS サーバーとしてコンソールを構成する方法"](#)

手順

1. オプション: Cloud Volumes ONTAPソフトウェア イメージをホストできる HTTP サーバーをセットアップします。

仮想ネットワークへの VPN 接続がある場合は、Cloud Volumes ONTAPソフトウェア イメージを独自のネットワーク内の HTTP サーバーに配置できます。それ以外の場合は、クラウド内の HTTP サーバーにファイルを配置する必要があります。

2. Cloud Volumes ONTAPに独自のセキュリティ グループを使用する場合は、Cloud Volumes ONTAP がソフトウェア イメージにアクセスできるように、送信ルールで HTTP 接続が許可されていることを確認します。



事前定義されたCloud Volumes ONTAPセキュリティ グループは、デフォルトで送信 HTTP 接続を許可します。

3. ソフトウェアイメージを入手する ["NetAppサポート サイト"](#)。
4. ソフトウェア イメージを、コンソール エージェント上のディレクトリまたはファイルの提供元となる HTTP サーバー上のディレクトリにコピーします。

2つのパスが利用可能です。正しいパスは、コンソール エージェントのバージョンによって異なります。

- /opt/application/netapp/cloudmanager/docker_occm/data/ontap/images/
- /opt/application/netapp/cloudmanager/ontap/images/

5. システム上で、 アイコンをクリックし、* Cloud Volumes ONTAPの更新*をクリックします。
6. Cloud Volumes ONTAPバージョンの更新ページで URL を入力し、[イメージの変更] をクリックします。

上記のパスにあるコンソール エージェントにソフトウェア イメージをコピーした場合は、次の URL を入力します。

`http://<コンソールエージェントのプライベートIPアドレス>/ontap/images/<イメージファイル名>`



URL では、**image-file-name** は「cot.image.9.13.1P2.tgz」という形式に従う必要があります。

7. *続行*をクリックして確認します。

結果

コンソールがソフトウェアの更新を開始します。ソフトウェアの更新が完了すると、システム上でアクションを実行できるようになります。

終了後の操作

SnapMirror転送を一時停止した場合は、System Manager を使用して転送を再開します。

Google Cloud NAT ゲートウェイ使用時のダウンロード失敗を修正

コンソール エージェントは、Cloud Volumes ONTAPのソフトウェア アップデートを自動的にダウンロードします。構成で Google Cloud NAT ゲートウェイを使用している場合、ダウンロードが失敗する可能性があります。ソフトウェア イメージを分割する部分の数を制限することで、この問題を修正できます。このステップを完了するには、API を使用する必要があります。

手順

1. 次の JSON を本文として PUT リクエストを `/occm/config` に送信します。

```
{
  "maxDownloadSessions": 32
}
```

`maxDownloadSessions` の値は 1 または 1 より大きい任意の整数にすることができます。値が 1 の場合、ダウンロードされたイメージは分割されません。

32 は例の値であることに注意してください。使用する値は、NAT 構成と同時に実行できるセッションの数によって異なります。

["/occm/config API呼び出しの詳細"](#)。

Cloud Volumes ONTAP従量課金制システムを登録する

NetAppからのサポートはCloud Volumes ONTAP従量課金制 (PAYGO) システムに含まれていますが、まずシステムをNetAppに登録してサポートを有効にする必要があります。

いずれかの方法でONTAPソフトウェアをアップグレードするには、PAYGOシステムをNetAppに登録する必要があります。["このページに記載されている"](#)。



サポートに登録されていないシステムでも、新しいバージョンが利用可能になったときにNetAppコンソールに表示されるソフトウェア更新通知を受信します。ただし、ソフトウェアをアップグレードする前にシステムを登録する必要があります。

手順

1. NetAppサポート サイト アカウントをコンソールにまだ追加していない場合は、[アカウント設定] に移動して今すぐ追加してください。

["NetAppサポートサイトアカウントを追加する方法を学ぶ"](#)。

2. システム ページで、登録するシステムの名前をダブルクリックします。
3. [概要] タブで [機能] パネルをクリックし、[サポート登録] の横にある鉛筆アイコンをクリックします。

Information	Features
System Tags	3 Tags 
Scheduled Downtime	Off 
Blob Access Tiering	Hot 
Instance Type	Standard_E8ds_v4 
Charging Method	Capacity-based 
Write Speed	<i>Not Supported</i> 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

4. NetAppサポート サイトのアカウントを選択し、[登録] をクリックします。

結果

システムはNetAppに登録されています。

Cloud Volumes ONTAP 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

ノードベースのライセンスの提供終了 (EOA) 後は、NetApp コンソールのライセンス変換ツールを使用して、容量ベースのライセンスに移行する必要があります。

年間契約または長期契約の場合、NetApp では、EOA 日 (2024 年 11 月 11 日) またはライセンスの有効期限の前に NetApp の担当者に連絡して、移行の前提条件が満たされていることを確認することをお勧めします。Cloud Volumes ONTAP ノードの長期契約がなく、オンデマンドの従量課金制 (PAYGO) サブスクリプションに対してシステムを実行している場合は、2024 年 12 月 31 日のサポート終了 (EOS) 前に変換を計画することが重要です。どちらの場合も、シームレスな移行を実現するために、NetApp コンソールのライセンス変換ツールを使用する前に、システムが要件を満たしていることを確認する必要があります。

EOA と EOS の詳細については、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](#)"。

タスク概要

- ライセンス変換ツールを使用すると、ノードベースのライセンス モデルから容量ベースのライセンス モデルへの移行がオンラインで実行されるため、データの移行や追加のクラウド リソースのプロビジョニングが不要になります。
- これは中断のない操作であり、サービス中断やアプリケーションのダウンタイムは発生しません。
- Cloud Volumes ONTAP システム内のアカウントとアプリケーション データはそのまま残ります。
- 変換後も、基盤となるクラウド リソースは影響を受けません。
- ライセンス変換ツールは、単一ノード、単一可用性ゾーン (AZ) での高可用性 (HA)、複数 AZ での HA、ライセンス持ち込み (BYOL)、PAYGO など、すべてのデプロイメント タイプをサポートします。
- このツールは、すべてのノードベースライセンスをソースとして、すべての容量ベースライセンスをターゲットとしてサポートしています。例えば、PAYGO Standard のノードベースライセンスをお持ちの場合、マーケットプレイスで購入した任意の容量ベースライセンスに変換できます。NetApp 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](#)"。
- 変換は、すべてのクラウド プロバイダー (AWS、Azure、Google Cloud) でサポートされています。
- 変換後、ノードベースのライセンスのシリアル番号は、容量ベースの形式に置き換えられます。これは変換の一環として実行され、NetApp サポート サイト (NSS) アカウントに反映されます。
- 容量ベースのモデルに移行すると、データは引き続きノードベースのライセンスと同じ場所に保持されます。このアプローチにより、データ配置の中断が保証されず、移行全体を通じてデータ主権の原則が維持されます。

始める前に

- 顧客アクセスまたは管理者アクセスを持つ NSS アカウントが必要です。
- NSS アカウントは、コンソールにアクセスするために使用したユーザー資格情報で登録する必要があります。
- Cloud Volumes ONTAP システムは、顧客アクセスまたは管理者アクセスを持つ NSS アカウントにリンクする必要があります。
- BYOL ライセンスまたはマーケットプレイス サブスクリプションのいずれか、有効な容量ベースのライセンスを用意する必要があります。
- 容量ベースのライセンスがアカウントで利用可能になります。このライセンスは、コンソールの ライセンスとサブスクリプション で利用できるマーケットプレイス サブスクリプションまたは BYOL/プライバー

ト オファー パッケージになります。

- 宛先パッケージを選択する前に、次の基準を理解してください。
 - アカウントに容量ベースの BYOL ライセンスがある場合、選択した宛先パッケージはアカウントの BYOL 容量ベース ライセンスと一致する必要があります。
 - いくつか `Professional` を宛先パッケージとして選択する場合、アカウントには Professional パッケージの BYOL ライセンスが必要です。
 - いくつか `Essentials` を宛先パッケージとして選択する場合、アカウントには Essentials パッケージの BYOL ライセンスが必要です。
 - 宛先パッケージがアカウントの BYOL ライセンスの可用性と一致しない場合は、容量ベースのライセンスに選択したパッケージが含まれていない可能性があります。この場合、マーケットプレイスのサブスクリプションを通じて料金が請求されます。
 - 容量ベースの BYOL ライセンスがなく、マーケットプレイス サブスクリプションのみがある場合は、選択したパッケージが容量ベースのマーケットプレイス サブスクリプションに含まれていることを確認する必要があります。
 - 既存の容量ベースのライセンスに十分な容量がなく、追加の容量の使用に対して課金するマーケットプレイス サブスクリプションがある場合、マーケットプレイス サブスクリプションを通じて追加の容量に対して課金されます。
 - 既存の容量ベースのライセンスに十分な容量がなく、追加の容量の使用に対して課金するマーケットプレイス サブスクリプションがない場合は、変換は実行できません。追加の容量を請求するか、現在のライセンスに利用可能な容量を拡張するには、マーケットプレイス サブスクリプションを追加する必要があります。
 - 宛先パッケージがアカウントの BYOL ライセンスの可用性と一致しない場合、また既存の容量ベースのライセンスに十分な容量がない場合は、マーケットプレイスのサブスクリプションを通じて料金が請求されます。



これらの要件のいずれかが満たされていない場合、ライセンスの変換は行われません。特定のケースでは、ライセンスは変換される可能性がありますが、使用することはできません。情報アイコンをクリックして問題を特定し、修正措置を講じます。

手順

1. システム ページで、ライセンスの種類を変更するシステムの名前をダブルクリックします。
2. [概要] タブで、[機能] パネルをクリックします。
3. *充電方法*の横にある鉛筆アイコンを確認してください。システムの充電方法が `Node Based` 容量課金に変更することができます。



Cloud Volumes ONTAPシステムがすでに容量によって課金されている場合、またはいずれかの要件が満たされていない場合、アイコンは無効になります。

4. *ノードベースのライセンスを容量ベースに変換する*画面で、システム名とソース ライセンスの詳細を確認します。
5. 既存のライセンスを変換するための宛先パッケージを選択します。
 - 必需品。デフォルト値は Essentials。
 - プロ
6. BYOL ライセンスをお持ちの場合は、変換が完了した後にコンソールからノードベースのライセンスを削

除するチェックボックスを選択できます。変換がまだ進行中の場合は、このチェックボックスを選択してもコンソールからライセンスは削除されません。このオプションはマーケットプレイスのサブスクリプションでは使用できません。

7. 変更の影響を理解していることを確認するためにチェックボックスを選択し、「続行」をクリックします。

終了後の操作

新しいライセンスのシリアル番号を表示し、コンソールの **ライセンスとサブスクリプション** メニューで変更を確認します。

さまざまなハイパースカラーの価格設定

価格の詳細については、"[NetAppコンソールのウェブサイト](#)"。

特定のハイパースカラーのプライベートオファーに関する情報については、下記までお問い合わせください。

- AWS - awsapo@netapp.com
- Azure - azurepo@netapp.com
- Google Cloud - gcppo@netapp.com

Cloud Volumes ONTAPシステムの起動と停止

NetAppコンソールからCloud Volumes ONTAP を停止および起動して、クラウド コンピューティング コストを管理できます。

Cloud Volumes ONTAPの自動シャットダウンのスケジュール設定

コンピューティング コストを削減するために、特定の時間間隔でCloud Volumes ONTAP をシャットダウンする必要がある場合があります。これを手動で行うのではなく、特定の時間にシステムを自動的にシャットダウンして再起動するようにコンソールを構成することができます。

タスク概要

- Cloud Volumes ONTAPシステムの自動シャットダウンをスケジュールすると、アクティブなデータ転送が進行中の場合、コンソールはシャットダウンを延期します。

転送が完了するとシステムをシャットダウンします。

- このタスクは、HA ペアの両方のノードの自動シャットダウンをスケジュールします。
- スケジュールされたシャットダウンによってCloud Volumes ONTAP をオフにすると、ブート ディスクとルート ディスクのスナップショットは作成されません。

スナップショットは、次のセクションで説明するように、手動シャットダウンを実行する場合にのみ自動的に作成されます。

手順

1. ***システム*** ページで、Cloud Volumes ONTAPシステムをダブルクリックします。
2. **[概要]** タブで **[機能]** パネルをクリックし、**[スケジュールされたダウンタイム]** の横にある鉛筆アイコンをクリックします。

Information	Features
System Tags	3 Tags 
Scheduled Downtime	On 
S3 Storage Classes	Standard 
Instance Type	m5.xlarge 
Charging Method	Capacity-based 
Write Speed	Normal 
Ransomware Protection	Off 
Support Registration	Not Registered 
WORM	Disabled 
CIFS Setup	

3. シャットダウン スケジュールを指定します。

- システムを毎日、平日毎日、週末ごとにシャットダウンするか、またはこれら 3 つのオプションを組み合わせてシャットダウンするかを選択します。
- システムをオフにするタイミングと、オフにしたい時間を指定します。

例

次の画像は、毎週土曜日の午後 20:00 (午後 8:00) に 12 時間システムをシャットダウンするようにコ

ンソールに指示するスケジュールを示しています。コンソールは毎週月曜日の午前12時にシステムを再起動します。

Schedule Downtime

Console Time Zone: 13:48 UTC

Select when to turn off your system:

Turn off every day

at

20

:

00

for

12

hours (1-24)

Sun, Mon, Tue, Wed, Thu, Fri, Sat

Turn off every weekdays

at

20

:

00

for

12

hours (1-24)

Mon, Tue, Wed, Thu, Fri

Turn off every weekend

at

08

:

00

for

48

hours (1-48)

Sat

4. *保存*をクリックします。

結果

スケジュールが保存されました。機能パネルの対応するスケジュールされたダウンタイムの行項目に「オン」と表示されます。

Cloud Volumes ONTAPの停止

Cloud Volumes ONTAPを停止すると、コンピューティング コストの発生が抑えられ、ルート ディスクとブート ディスクのスナップショットが作成されるため、トラブルシューティングに役立ちます。



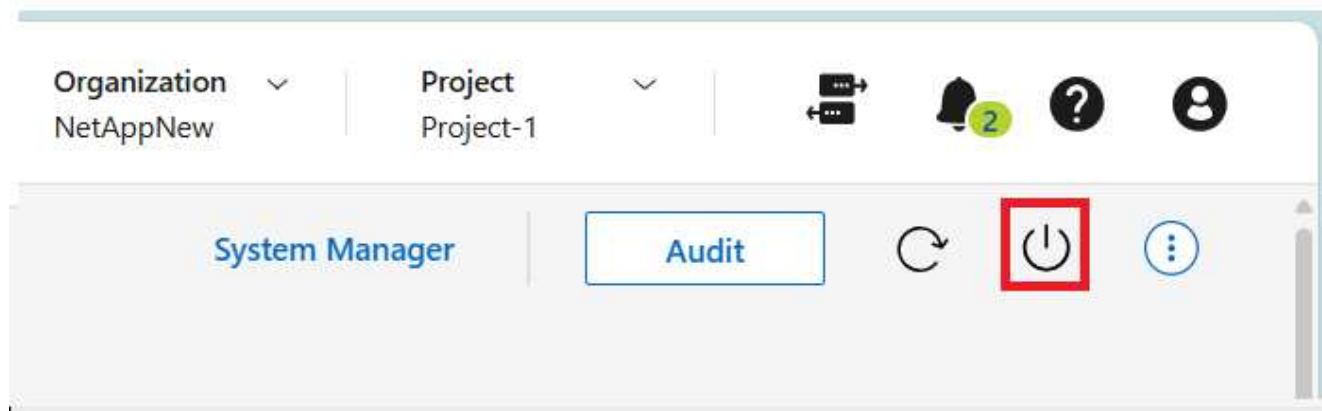
コストを削減するために、コンソールはルート ディスクとブート ディスクの古いスナップショットを定期的に削除します。ルート ディスクとブート ディスクの両方に対して、最新の2つのスナップショットのみが保持されます。

タスク概要

HA ペアを停止すると、コンソールは両方のノードをシャットダウンします。

手順

1. システムから、[オフにする] アイコンをクリックします。



2. スナップショットによってシステムの回復が可能になるため、スナップショットを作成するオプションを有効にしておきます。
3. *[オフにする]*をクリックします。

システムを停止するには数分かかる場合があります。システム ページから後でシステムを再起動できます。



スナップショットは再起動時に自動的に作成されます。

NTPサーバーを使用してCloud Volumes ONTAPのシステム時間を同期する

NTP サーバーを指定すると、ネットワーク内のシステム間の時間が同期され、時間差による問題を防ぐことができます。

NTPサーバーを指定するには、["NetAppコンソール API"](#)またはユーザーインターフェースから["CIFSサーバーを作成する"](#)。

システムの書き込み速度を変更する

NetAppコンソールで、Cloud Volumes ONTAPの通常または高速の書き込み速度を選択できます。デフォルトの書き込み速度は通常です。ワークロードに高速書き込みパフォーマンスが必要な場合は、高速書き込みに変更できます。

すべてのタイプの単一ノード システムと一部の HA ペア構成で、高速書き込み速度がサポートされます。サポートされている構成については、["Cloud Volumes ONTAPリリースノート"](#)

書き込み速度を変更する前に、["通常設定と高設定の違いを理解する"](#)。

タスク概要

- ボリュームやアグリゲートの作成などの操作が進行中でないことを確認します。
- この変更により、Cloud Volumes ONTAPシステムが再起動されることに注意してください。これはシステム全体のダウンタイムを必要とする中断を伴うプロセスです。

手順

1. システム ページで、書き込み速度を設定するシステムの名前をダブルクリックします。

2. [概要] タブで [機能] パネルをクリックし、[書き込み速度] の横にある鉛筆アイコンをクリックします。
3. *標準*または*高*を選択します。

「高」を選択した場合は、「理解しました」という文言を読み、ボックスにチェックを入れて確認する必要があります。



*高*書き込み速度オプションは、バージョン 9.13.0 以降の Google Cloud のCloud Volumes ONTAP HA ペアでサポートされます。

4. *保存*をクリックし、確認メッセージを確認して*承認*をクリックします。

Cloud Volumes ONTAPクラスタ管理者のパスワードを変更する

Cloud Volumes ONTAPにはクラスタ管理者アカウントが含まれています。必要に応じて、NetAppコンソールからこのアカウントのパスワードを変更できます。



ONTAP System Manager またはONTAP CLI を使用して管理者アカウントのパスワードを変更しないでください。パスワードはコンソールに反映されません。その結果、コンソールはインスタンスを適切に監視できません。

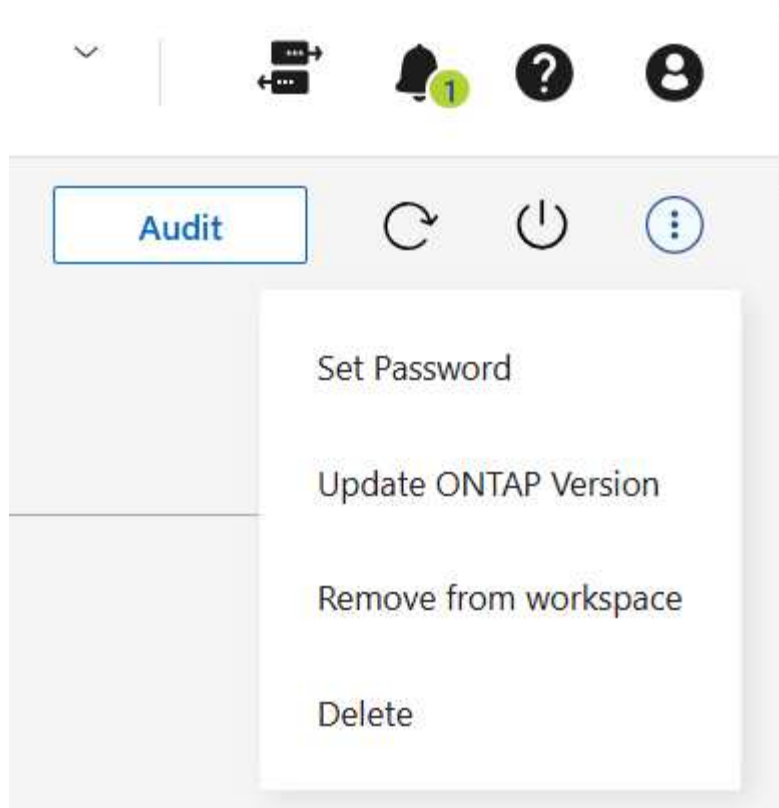
タスク概要

パスワードはいくつかのルールに従う必要があります。新しいパスワード:

- 単語が含まれていない admin
- 8文字から50文字までの長さにする必要があります
- 少なくとも1つの英語の文字と1つの数字を含める必要があります
- 次の特殊文字を含めることはできません: / () { } [] # : % " ? \

手順

1. *システム*ページで、Cloud Volumes ONTAPシステムの名前をダブルクリックします。
2. コンソールの右上にある アイコンをクリックし、[パスワードの設定] を選択します。



システムの追加、削除、または削除

既存の**Cloud Volumes ONTAP**システムを**NetApp**コンソールに追加する

既存のCloud Volumes ONTAPシステムを検出し、NetAppコンソールに追加できます。新しいシステムを導入した場合には、これを行う可能性があります。

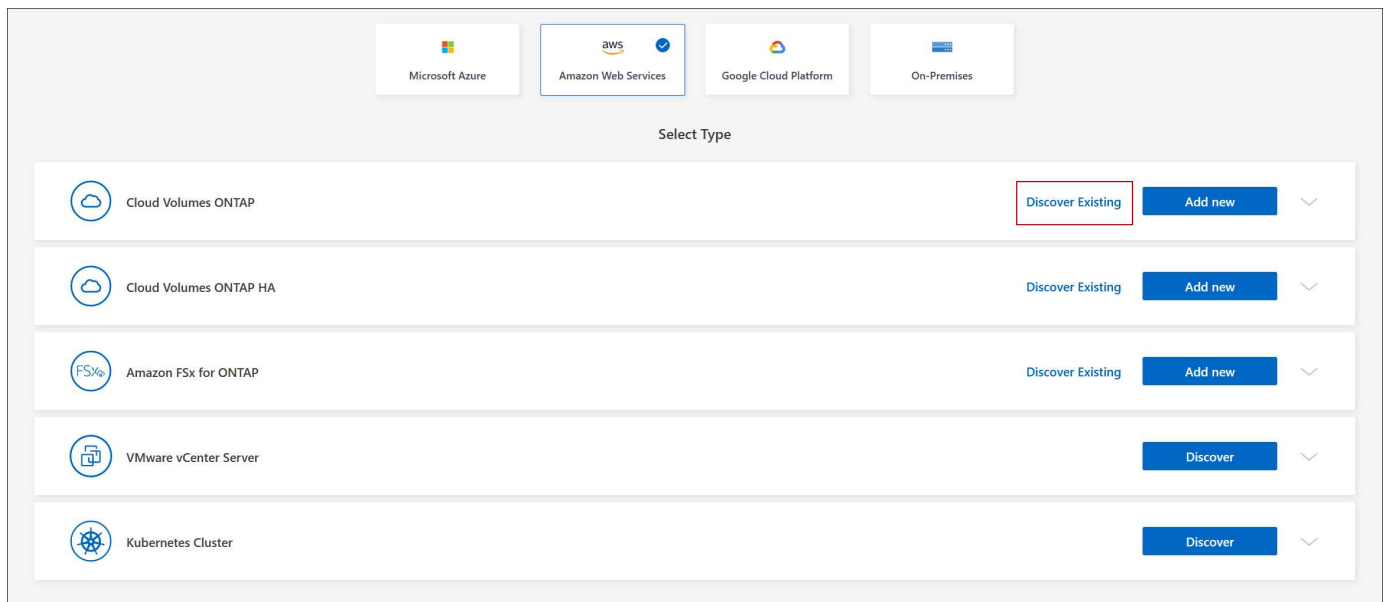
開始する前に

Cloud Volumes ONTAP管理者ユーザー アカウントのパスワードを知っている必要があります。

手順

1. 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*をクリックします。
3. システムが存在するクラウド プロバイダーを選択します。
4. 追加するCloud Volumes ONTAPシステムのタイプを選択します。
5. 既存のシステムを見つけるには、リンクをクリックします。

+



1. 「リージョン」 ページでリージョンを選択します。選択したリージョンで実行されているシステムを確認できます。



Cloud Volumes ONTAPシステムは、このページではインスタンスとして表されます。リストから、現在のアカウントに登録されているインスタンスのみを選択できます。

2. [資格情報] ページで、Cloud Volumes ONTAP管理者ユーザーのパスワードを入力し、[Go] を選択します。

結果

コンソールは、Cloud Volumes ONTAPシステムを システム ページに追加します。

NetAppコンソールからCloud Volumes ONTAPシステムを削除する

Cloud Volumes ONTAPシステムを削除して、別のシステムに移動したり、検出の問題をトラブルシューティングしたりすることができます。

タスク概要

Cloud Volumes ONTAPシステムを削除すると、NetAppコンソールからも削除されます。Cloud Volumes ONTAPシステムは削除されません。必要に応じて、後でシステムを再検出できます。

手順

1. システム ページで、削除するシステムをダブルクリックします。
2. コンソールの右上にある ... アイコンをクリックし、[ワークスペースから削除] を選択します。
3. ワークスペースから削除 ウィンドウで、削除 をクリックします。

結果

コンソールはシステムを削除します。ユーザーは、システム ページから削除されたシステムをいつでも再発見できます。

NetAppコンソールからCloud Volumes ONTAPシステムを削除する

Cloud Volumes ONTAPシステムは、クラウド プロバイダーのアプリケーションからではなく、常にNetAppコンソールから削除する必要があります。たとえば、クラウド プロバイダーからライセンスを取得したCloud Volumes ONTAPインスタンスを終了した場合、そのライセンス キーを別のインスタンスに使用することはできません。ライセンスを解放するには、コンソールからCloud Volumes ONTAPシステムを削除する必要があります。

システムを削除すると、コンソールはCloud Volumes ONTAPインスタンスを終了し、ディスクとスナップショットを削除します。



システムを削除しても、NetApp Backup and Recovery によって管理されるバックアップやNetApp Data Classification のインスタンスなどの他のリソースは削除されません。手動で削除する必要があります。そうしないと、これらのリソースに対して引き続き料金が発生します。

コンソールがクラウド プロバイダーにCloud Volumes ONTAP をデプロイすると、インスタンスの終了保護が有効になります。このオプションは、誤って終了するのを防ぐのに役立ちます。

手順

1. システムでバックアップとリカバリを有効にした場合は、バックアップしたデータがまだ必要かどうかを確認し、["必要に応じてバックアップを削除する"](#)。

バックアップとリカバリは、設計上、Cloud Volumes ONTAPから独立しています。バックアップとリカバリでは、Cloud Volumes ONTAPシステムを削除してもバックアップは自動的に削除されません。また、システムの削除後にバックアップを削除するための UI は現在サポートされていません。

2. このシステムでデータ分類を有効にしている、他のシステムでこのサービスが使用されていない場合は、サービスのインスタンスを削除する必要があります。

["データ分類インスタンスの詳細"](#)。

3. Cloud Volumes ONTAPシステムを削除します。
 - a. *システム*ページで、削除するCloud Volumes ONTAPシステムの名前をダブルクリックします。
 - b. コンソールの右上にある アイコンをクリックし、[削除] を選択します。
 - c. 削除するシステムの名前を入力し、「削除」をクリックします。システムの削除には最大 5 分かかる場合があります。



バックアップとリカバリは、Cloud Volumes ONTAP Professional ライセンスに対してのみ無料です。この無料特典は削除された環境には適用されません。Cloud Volumes ONTAP環境のバックアップ コピーがバックアップおよびリカバリ インスタンスに保持されている場合、バックアップ コピーは削除されるまで課金されます。

AWS管理

AWS のCloud Volumes ONTAPシステムの EC2 インスタンス タイプを変更する

AWS でCloud Volumes ONTAP を起動するときに、複数のインスタンスとタイプから選択できます。インスタンス タイプがニーズに対して小さすぎる、または大きすぎると判断した場合は、いつでもインスタンス タイプを変更できます。

タスク概要

- Cloud Volumes ONTAP HA ペアでは自動ギブバックを有効にする必要があります (これがデフォルト設定です)。そうでない場合、操作は失敗します。

"ONTAP 9ドキュメント: 自動ギブバックを設定するためのコマンド"

- インスタンスタイプを変更すると、AWS サービスの料金に影響する可能性があります。
- この操作により、Cloud Volumes ONTAPが再起動します。

単一ノード システムの場合、I/O が中断されます。

HA ペアの場合、変更は中断なく行われます。HA ペアは引き続きデータを提供します。



NetAppコンソールは、テイクオーバーを開始し、ギブバックを待機することで、一度に 1 つのノードを変更します。NetApp の品質保証チームは、このプロセス中にファイルの書き込みと読み取りの両方をテストしましたが、クライアント側に問題は見られませんでした。接続が変更されると、I/O レベルで再試行がいくつか発生しましたが、アプリケーション層は NFS/CIFS 接続の再配線を克服しました。

参照

AWSでサポートされているインスタンスタイプのリストについては、以下を参照してください。"[サポートされているEC2インスタンス](#)"。

インスタンスタイプをc4、m4、またはr4インスタンスから変更できない場合は、KB記事を参照してください。"[AWS Xen CVO インスタンスを Nitro \(KVM\) に変換する](#)"。

手順

1. *システム*ページで、システムを選択します。
2. [概要] タブで [機能] パネルをクリックし、[インスタンス タイプ] の横にある鉛筆アイコンをクリックします。

Information		Features
System Tags	Tags	
Scheduled Downtime	Off	
S3 Storage Classes	Standard-Infrequent Access	
Instance Type	m5.xlarge	
Write Speed	Normal	
Ransomware Protection	Off	
Support Registration	Not Registered	
CIFs Setup		

ノードベースの従量課金制 (PAYGO) ライセンスを使用している場合は、ライセンス タイプ の横にある鉛筆アイコンをクリックして、オプションで別のライセンスとインスタンス タイプを選択できます。

3. インスタンス タイプを選択し、変更の影響を理解していることを確認するためにチェックボックスをオンにして、[変更] をクリックします。

結果

Cloud Volumes ONTAP は新しい構成で再起動します。

複数の **AWS AZ** にある **Cloud Volumes ONTAP HA** ペアのルートテーブルを変更する

複数の AWS アベイラビリティゾーン (AZ) にデプロイされている HA ペアのフローティング IP アドレスへのルートを含む AWS ルートテーブルを変更できます。新しい NFS または CIFS クライアントが AWS 内の HA ペアにアクセスする必要がある場合は、これを実行できます。

手順

1. *システム* ページで、システムを選択します。
2. [概要] タブで [機能] パネルをクリックし、[ルート テーブル] の横にある鉛筆アイコンをクリックします。
3. 選択したルート テーブルのリストを変更し、[保存] をクリックします。

結果

NetApp コンソールは、ルート テーブルを変更するための AWS リクエストを送信します。

Azure 管理

Cloud Volumes ONTAP の Azure VM タイプを変更する

Microsoft Azure で Cloud Volumes ONTAP を起動するときに、いくつかの VM タイプから選択できます。VM のタイプがニーズに対して小さすぎるか大きすぎると判断した場合は、いつでも VM タイプを変更できます。

タスク概要

- Cloud Volumes ONTAP HA ペアでは自動ギブバックを有効にする必要があります (これがデフォルト設定です)。そうでない場合、操作は失敗します。

["ONTAP 9 ドキュメント: 自動ギブバックを設定するためのコマンド"](#)

- VM タイプを変更すると、Microsoft Azure サービスの料金に影響する可能性があります。
- この操作により、Cloud Volumes ONTAP が再起動します。

単一ノード システムの場合、I/O が中断されます。

HA ペアの場合、変更は中断なく行われます。HA ペアは引き続きデータを提供します。



NetApp コンソールは、テイクオーバーを開始し、ギブバックを待機することで、一度に 1 つのノードを変更します。NetApp の品質保証チームは、このプロセス中にファイルの書き込みと読み取りの両方をテストしましたが、クライアント側に問題は見られませんでした。接続が変更されると、I/O レベルで再試行がいくつか発生しましたが、アプリケーション層は NFS/CIFS 接続の再配線を克服しました。

手順

1. *システム*ページで、システムを選択します。
2. [概要] タブで [機能] パネルをクリックし、[VM タイプ] の横にある鉛筆アイコンをクリックします。

ノードベースの従量課金制 (PAYGO) ライセンスを使用している場合は、ライセンス タイプ の横にある鉛筆アイコンをクリックして、オプションで別のライセンスと VM タイプを選択できます。

3. VM タイプを選択し、変更の影響を理解していることを確認するためのチェック ボックスをオンにして、[変更] をクリックします。

結果

Cloud Volumes ONTAP は新しい構成で再起動します。

Azure のCloud Volumes ONTAP HA ペアの CIFS ロックをオーバーライドする

組織またはアカウント管理者は、Azure メンテナンス イベント中にCloud Volumes ONTAPストレージ ギブバックに関する問題を防ぐ設定をNetAppコンソールで有効にすることができます。この設定を有効にすると、Cloud Volumes ONTAP はCIFS ロックを拒否し、アクティブな CIFS セッションをリセットします。

タスク概要

Microsoft Azure は、仮想マシン上で定期的なメンテナンス イベントをスケジュールします。Cloud Volumes ONTAP HA ペアでメンテナンス イベントが発生すると、HA ペアはストレージ テイクオーバーを開始します。このメンテナンス イベント中にアクティブな CIFS セッションがある場合、CIFS ファイルのロックによりストレージのギブバックが妨げられる可能性があります。

この設定を有効にすると、Cloud Volumes ONTAP はロックを拒否し、アクティブな CIFS セッションをリセットします。その結果、HA ペアはこれらのメンテナンス イベント中にストレージのギブバックを完了できません。



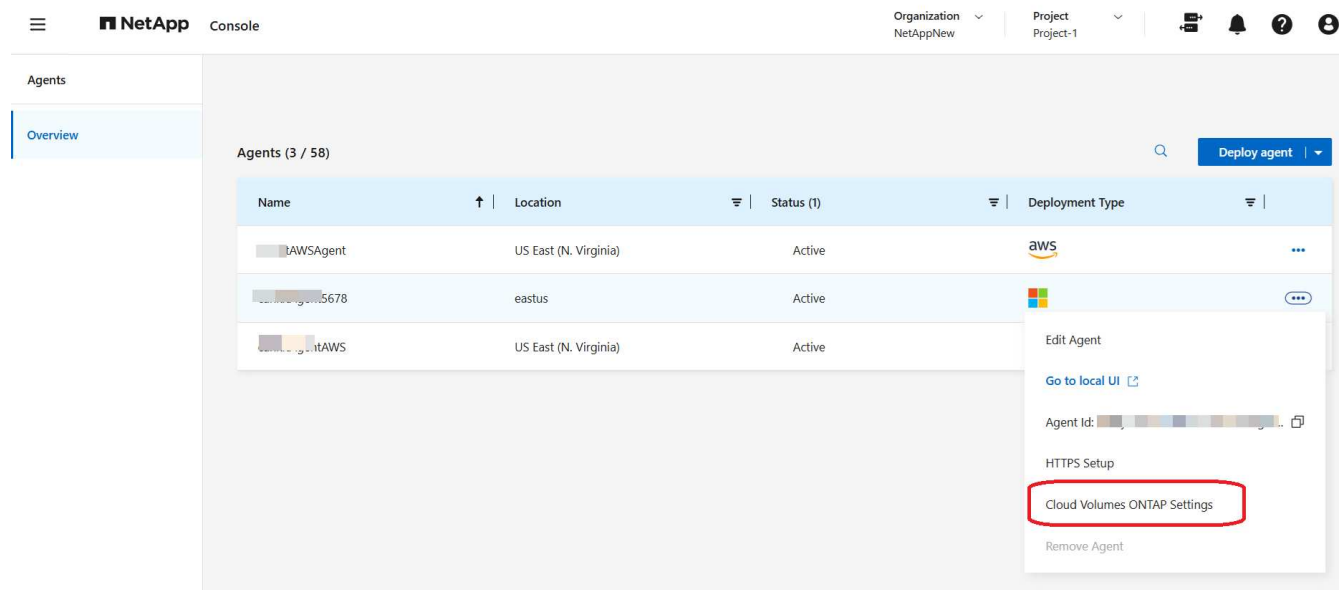
このプロセスは CIFS クライアントに混乱をもたらす可能性があります。CIFS クライアントからコミットされていないデータは失われる可能性があります。

開始する前に

コンソール設定を変更する前に、コンソール エージェントを作成する必要があります。 ["方法を学ぶ"](#)。

手順

1. 左側のナビゲーション ペインから、管理 > エージェント に移動します。
2. クリック Cloud Volumes ONTAPシステムを管理するコンソール エージェントのアイコン。
3. * Cloud Volumes ONTAP設定*を選択します。



4. **Azure** の下で、**Azure HA** システムの **Azure CIFS** ロック をクリックします。

5. チェックボックスをクリックして機能を有効にし、[保存] をクリックします。

Cloud Volumes ONTAPシステムに **Azure Private Link** またはサービス エンドポイントを使用する

Cloud Volumes ONTAP は、関連付けられたストレージ アカウントへの接続に Azure Private Link を使用します。必要に応じて、Azure Private Links を無効にして、代わりにサービス エンドポイントを使用できます。

概要

デフォルトでは、NetAppコンソールは、Cloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間の接続に Azure プライベート リンクを有効にします。Azure Private Link は、Azure 内のエンドポイント間の接続を保護し、パフォーマンス上の利点をもたらします。

必要に応じて、Azure Private Link の代わりにサービス エンドポイントを使用するようにCloud Volumes ONTAPを構成できます。

どちらの構成でも、コンソールは常にCloud Volumes ONTAPとストレージ アカウント間の接続のネットワーク アクセスを制限します。ネットワーク アクセスは、Cloud Volumes ONTAPがデプロイされている VNet と、コンソール エージェントがデプロイされている VNet に制限されます。

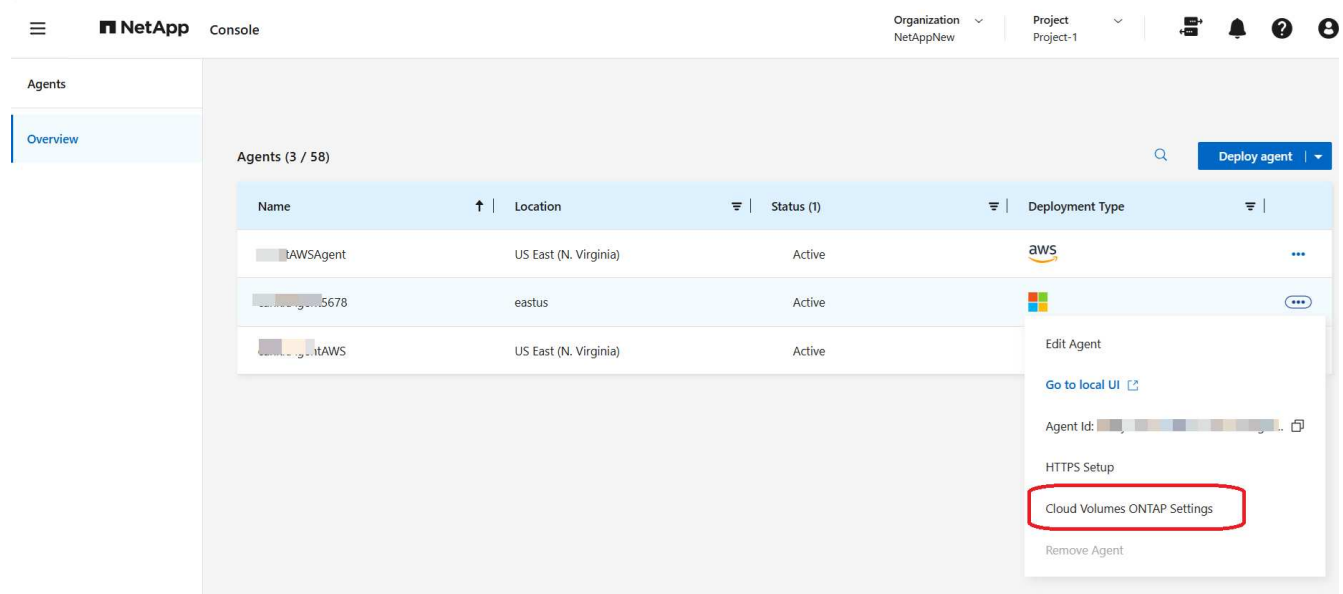
Azure プライベート リンクを無効にして、代わりにサービス エンドポイントを使用する

ビジネスで必要な場合は、コンソールの設定を変更して、Cloud Volumes ONTAPが Azure Private Link ではなくサービス エンドポイントを使用するように構成できます。この設定の変更は、作成する新しいCloud Volumes ONTAPシステムに適用されます。サービスエンドポイントは、"**Azureリージョンペア**"コンソール エージェントとCloud Volumes ONTAP VNet 間。

コンソールエージェントは、管理するCloud Volumes ONTAPシステムと同じAzureリージョン、または "**Azure リージョン ペア**"Cloud Volumes ONTAPシステム用。

手順

1. 左側のナビゲーション ペインから、管理 > エージェント に移動します。
2. クリック ... Cloud Volumes ONTAPシステムを管理するコンソール エージェントのアイコン。
3. * Cloud Volumes ONTAP設定*を選択します。



4. **Azure** の下で、**Azure Private Link** を使用する をクリックします。
5. * Cloud Volumes ONTAPとストレージアカウント間のプライベートリンク接続*の選択を解除します。
6. *保存*をクリックします。

終了後の操作

Azure プライベート リンクを無効にし、コンソール エージェントがプロキシ サーバーを使用する場合は、直接 API トラフィックを有効にする必要があります。

["コンソールエージェントで直接APIトラフィックを有効にする方法を学びます"](#)

Azure プライベート リンクの操作

ほとんどの場合、Cloud Volumes ONTAPを使用して Azure プライベート リンクを設定するために必要な操作はありません。コンソールは Azure Private Links を管理します。ただし、既存の Azure プライベート DNS ゾーンを使用する場合は、構成ファイルを編集する必要があります。

カスタムDNSの要件

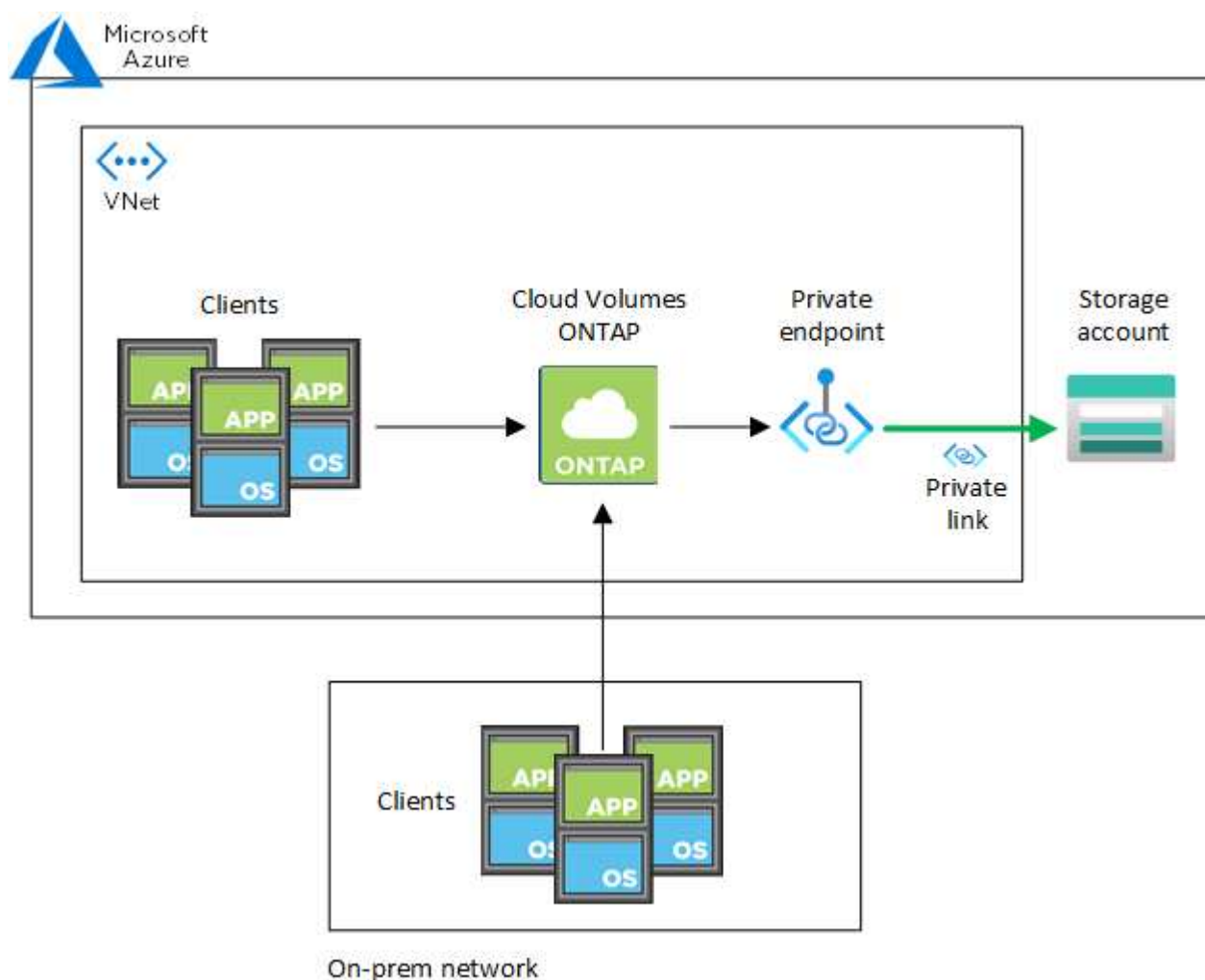
必要に応じて、カスタム DNS を使用する場合は、カスタム DNS サーバーから Azure プライベート DNS ゾーンへの条件付きフォワーダーを作成する必要があります。詳細については、["DNSフォワーダーの使用に関するAzureのドキュメント"](#)。

プライベートリンク接続の仕組み

コンソールが Azure にCloud Volumes ONTAP をデプロイすると、リソース グループにプライベート エンドポイントが作成されます。プライベート エンドポイントは、Cloud Volumes ONTAPのストレージ アカウントに関連付けられています。その結果、Cloud Volumes ONTAPストレージへのアクセスは、Microsoft バックボーン ネットワークを経由することになります。

クライアントがCloud Volumes ONTAPと同じ VNet 内、ピアリングされた VNet 内、またはオンプレミス ネットワーク内でプライベート VPN または ExpressRoute 接続を使用して VNet に接続している場合、クライアント アクセスはプライベート リンクを経由します。

以下は、同じ VNet 内およびプライベート VPN または ExpressRoute 接続を持つオンプレミス ネットワークからのプライベート リンク経由のクライアント アクセスを示す例です。



コンソール エージェントとCloud Volumes ONTAPシステムが異なる VNet にデプロイされている場合は、コンソール エージェントがデプロイされている VNet とCloud Volumes ONTAPシステムがデプロイされている VNet の間に VNet ピアリングを設定する必要があります。

Azure プライベート DNS の詳細を入力してください

使用する場合 ["Azure プライベート DNS"](#)、各コンソール エージェントの構成ファイルを変更する必要があります。そうしないと、コンソールはCloud Volumes ONTAPとそれに関連付けられたストレージ アカウント間の Azure Private Link 接続を設定できません。

DNS名はAzure DNSの命名要件に一致する必要があることに注意してください。 ["Azureドキュメントに記載されているとおり"](#)。

手順

1. コンソール エージェント ホストに SSH で接続してログインします。

2. に移動 `/opt/application/netapp/cloudmanager/docker_occm/data` ディレクトリ。
3. 編集 `app.conf` 追加することで `user-private-dns-zone-settings` 次のキーワードと値のペアを持つパラメータ:

```
"user-private-dns-zone-settings" : {  
  "resource-group" : "<resource group name of the DNS zone>",  
  "subscription" : "<subscription ID>",  
  "use-existing" : true,  
  "create-private-dns-zone-link" : true  
}
```

その `subscription` キーワードは、プライベート DNS ゾーンがコンソール エージェントのサブスクリプションとは異なるサブスクリプションにある場合にのみ必要です。

4. ファイルを保存し、コンソール エージェントからログオフします。

再起動は必要ありません。

失敗時のロールバックを有効にする

コンソールが特定のアクションの一部として Azure プライベート リンクの作成に失敗した場合、Azure プライベート リンク接続なしでアクションが完了します。これは、新しいシステム (単一ノードまたは HA ペア) を作成するとき、または HA ペアで次のアクション (新しいアグリゲートの作成、既存のアグリゲートへのディスクの追加、32 TiB を超えたときに新しいストレージ アカウントの作成) が発生したときに発生する可能性があります。

コンソールが Azure プライベート リンクの作成に失敗した場合、ロールバックを有効にすることでこのデフォルトの動作を変更できます。これにより、会社のセキュリティ規制に完全に準拠していることを確認できます。

ロールバックを有効にすると、コンソールはアクションを停止し、アクションの一部として作成されたすべてのリソースをロールバックします。

ロールバックは、API 経由で、または `app.conf` ファイルを更新することで有効にできます。

API経由でロールバックを有効にする

手順

1. 使用 `PUT /occm/config` 次のリクエスト本文を含む API 呼び出し:

```
{ "rollbackOnAzurePrivateLinkFailure": true }
```

`app.conf`を更新してロールバックを有効にする

手順

1. コンソール エージェントのホストに SSH で接続してログインします。

2. 次のディレクトリに移動します: /opt/application/netapp/cloudmanager/docker_occm/data
3. 次のパラメータと値を追加して app.conf を編集します。

```
"rollback-on-private-link-failure": true
```

・ ファイルを保存し、コンソール エージェントからログオフします。

再起動は必要ありません。

Azure コンソールで Cloud Volumes ONTAP の Azure リソースグループを移動する

Cloud Volumes ONTAP は Azure リソース グループの移動をサポートしますが、ワークフローは Azure コンソールでのみ実行されます。

Cloud Volumes ONTAP システムを、同じ Azure サブスクリプション内の Azure 内の 1 つのリソース グループから別のリソース グループに移動できます。異なる Azure サブスクリプション間でのリソース グループの移動はサポートされていません。

手順

1. Cloud Volumes ONTAP システムを削除します。。 ["Cloud Volumes ONTAP システムの削除"](#)。
2. Azure コンソールでリソース グループの移動を実行します。

移動を完了するには、["Microsoft Azure のドキュメントでリソースを新しいリソース グループまたはサブスクリプションに移動する"](#)。

3. *システム* ページでシステムを検出します。
4. システムの情報で新しいリソース グループを探します。

結果

システムとそのリソース (VM、ディスク、ストレージ アカウント、ネットワーク インターフェイス、スナップショット) は、新しいリソース グループに含まれます。

Azure で SnapMirror トラフィックを分離する

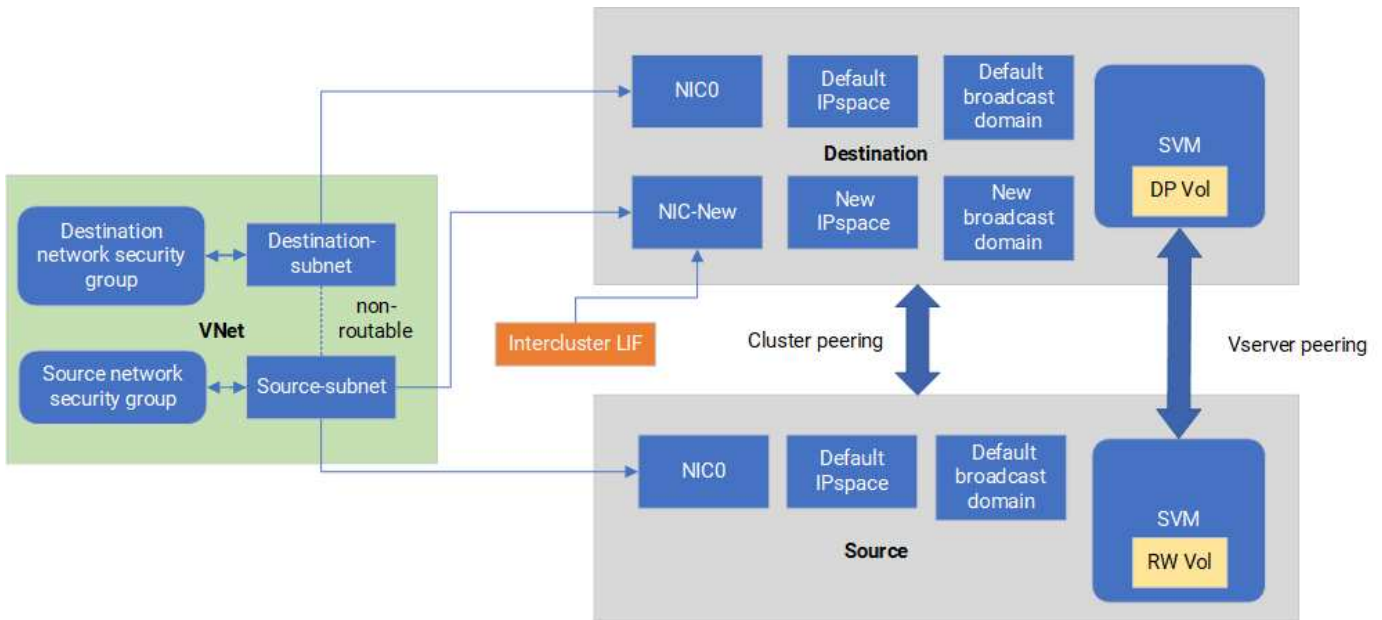
Azure の Cloud Volumes ONTAP を使用すると、SnapMirror レプリケーション トラフィックをデータおよび管理トラフィックから分離できます。SnapMirror レプリケーション トラフィックをデータ トラフィックから分離するには、新しいネットワーク インターフェイス カード (NIC)、関連付けられたクラスター間 LIF、およびルーティング不可能なサブネットを追加します。

Azure における SnapMirror トラフィック分離について

デフォルトでは、NetApp コンソールは、Cloud Volumes ONTAP デプロイメント内のすべての NIC と LIF を同じサブネット上に構成します。このような構成では、SnapMirror レプリケーション トラフィックとデータおよび管理トラフィックは同じサブネットを使用します。SnapMirror トラフィックを分離すると、データおよび管理トラフィックに使用される既存のサブネットにルーティングできない追加のサブネットが活用されます。

図1

次の図は、単一ノード展開における追加の NIC、関連付けられたクラスター間 LIF、およびルーティング不可能なサブネットを使用した SnapMirror レプリケーション トラフィックの分離を示しています。 HA ペアの展開は少し異なります。



開始する前に

次の考慮事項を確認してください。

- SnapMirror トラフィック分離のために、Cloud Volumes ONTAP の単一ノードまたは HA ペアのデプロイメント (VM インスタンス) に追加できるのは単一の NIC のみです。
- 新しい NIC を追加するには、デプロイする VM インスタンス タイプに未使用の NIC が必要です。
- ソース クラスターと宛先クラスターは同じ仮想ネットワーク (VNet) にアクセスできる必要があります。宛先クラスターは、Azure の Cloud Volumes ONTAP システムです。ソース クラスターは、Azure の Cloud Volumes ONTAP システムまたは ONTAP システムになります。

ステップ1: 追加の NIC を作成し、宛先 VM に接続する

このセクションでは、追加の NIC を作成し、それを宛先 VM に接続する方法について説明します。宛先 VM は、追加の NIC を設定する Azure の Cloud Volumes ONTAP の単一ノードまたは HA ペア システムです。

手順

1. ONTAP CLI でノードを停止します。

```
dest::> halt -node <dest_node-vm>
```

2. Azure ポータルで、VM (ノード) の状態が停止していることを確認します。

```
az vm get-instance-view --resource-group <dest-rg> --name <dest-vm>
--query instanceView.statuses[1].displayStatus
```

3. Azure Cloud Shell の Bash 環境を使用してノードを停止します。

a. ノードを停止します。

```
az vm stop --resource-group <dest_node-rg> --name <dest_node-vm>
```

b. ノードの割り当てを解除します。

```
az vm deallocate --resource-group <dest_node-rg> --name <dest_node-vm>
```

4. 2つのサブネット (ソース クラスター サブネットと宛先クラスター サブネット) が相互にルーティングできないように、ネットワーク セキュリティ グループ ルールを構成します。

a. 宛先 VM に新しい NIC を作成します。

b. ソース クラスター サブネットのサブネット ID を検索します。

```
az network vnet subnet show -g <src_vnet-rg> -n <src_subnet> --vnet-name <vnet> --query id
```

c. ソース クラスターのサブネットのサブネット ID を使用して、宛先 VM に新しい NIC を作成します。ここで新しい NIC の名前を入力します。

```
az network nic create -g <dest_node-rg> -n <dest_node-vm-nic-new> --subnet <id_from_prev_command> --accelerated-networking true
```

d. privateIPAddressを保存します。このIPアドレス<new_added_nic_primary_addr>は、クラスター間LIFを作成するために使用されます。[ブロードキャストドメイン](#)、[新しいNICのクラスター間LIF](#)。

5. 新しい NIC を VM に接続します。

```
az vm nic add -g <dest_node-rg> --vm-name <dest_node-vm> --nics <dest_node-vm-nic-new>
```

6. VM (ノード) を起動します。

```
az vm start --resource-group <dest_node-rg> --name <dest_node-vm>
```

7. Azure ポータルで、ネットワーク に移動し、新しい NIC (例: nic-new) が存在し、高速ネットワークが有効になっていることを確認します。

```
az network nic list --resource-group azure-59806175-60147103-azure-rg
--query "[].{NIC: name, VM: virtualMachine.id}"
```

HA ペアの展開の場合は、パートナー ノードに対して手順を繰り返します。

ステップ2: 新しいNIC用の新しいIPspace、ブロードキャストドメイン、およびクラスタ間LIFを作成する

クラスタ間 LIF 用の個別の IPspace により、クラスタ間のレプリケーションのネットワーク機能が論理的に分離されます。

次の手順ではONTAP CLI を使用します。

手順

1. 新しい IPspace (new_ipspace) を作成します。

```
dest::> network ipspace create -ipspace <new_ipspace>
```

2. 新しい IPspace (new_ipspace) にブロードキャスト ドメインを作成し、nic-new ポートを追加します。

```
dest::> network port show
```

3. 単一ノード システムの場合、新しく追加されたポートは *e0b* です。管理対象ディスクを使用した HA ペアの展開の場合、新しく追加されたポートは *e0d* です。ページ BLOB を使用した HA ペアの展開の場合、新しく追加されたポートは *e0e* です。VM 名ではなくノード名を使用します。ノード名を見つけるには、以下を実行します。 `node show`。

```
dest::> broadcast-domain create -broadcast-domain <new_bd> -mtu 1500
-ipspace <new_ipspace> -ports <dest_node-cot-vm:e0b>
```

4. 新しいブロードキャスト ドメイン (new_bd) と新しい NIC (nic-new) にクラスタ間 LIF を作成します。

```
dest::> net int create -vserver <new_ipspace> -lif <new_dest_node-ic-
lif> -service-policy default-intercluster -address
<new_added_nic_primary_addr> -home-port <e0b> -home-node <node> -netmask
<new_netmask_ip> -broadcast-domain <new_bd>
```

5. 新しいクラスタ間 LIF の作成を確認します。

```
dest::> net int show
```

HA ペアの展開の場合は、パートナー ノードに対して手順を繰り返します。

ステップ3: ソースシステムとターゲットシステム間のクラスタピアリングを確認する

このセクションでは、ソース システムと宛先システム間のピアリングを確認する方法について説明します。

次の手順ではONTAP CLI を使用します。

手順

1. 宛先クラスタのクラスタ間 LIF がソース クラスタのクラスタ間 LIF に ping できることを確認します。このコマンドは宛先クラスタによって実行されるため、宛先 IP アドレスはソース上のクラスタ間 LIF IP アドレスになります。

```
dest::> ping -lif <new_dest_node-ic-lif> -vserver <new_ipspace>
        -destination <10.161.189.6>
```

2. ソース クラスタのクラスタ間 LIF が宛先クラスタのクラスタ間 LIF に ping できることを確認します。宛先は、宛先に作成された新しい NIC の IP アドレスです。

```
src::> ping -lif <src_node-ic-lif> -vserver <src_svm> -destination
        <10.161.189.18>
```

HA ペアの展開の場合は、パートナー ノードに対して手順を繰り返します。

ステップ4: ソースシステムと宛先システム間のSVMピアリングを作成する

このセクションでは、ソース システムと宛先システム間の SVM ピアリングを作成する方法について説明します。

次の手順ではONTAP CLI を使用します。

手順

1. 送信元クラスタ間LIF IPアドレスを宛先にクラスタピアリングを作成します。-peer-addr。HAペアの場合は、両方のノードのソースクラスタ間LIF IPアドレスを次のようにリストします。-peer-addr。

```
dest::> cluster peer create -peer-addr <10.161.189.6> -ipspace
        <new_ipspace>
```

2. パスフレーズを入力して確認します。
3. 宛先クラスタLIF IPアドレスを使用してソースにクラスタピアリングを作成します。peer-addr。HAペアの場合は、両方のノードの宛先クラスタ間LIF IPアドレスを次のようにリストします。-peer-addr。

```
src::> cluster peer create -peer-addr <10.161.189.18>
```

4. パスフレーズを入力して確認します。
5. クラスタがピアリングされていることを確認します。

```
src::> cluster peer show
```

ピアリングが成功すると、可用性フィールドに「使用可能」と表示されます。

6. 宛先に SVM ピアリングを作成します。ソース SVM と宛先 SVM は両方ともデータ SVM である必要があります。

```
dest::> vservers peer create -vservers <dest_svm> -peer-vservers <src_svm>  
-peer-cluster <src_cluster> -applications snapmirror``
```

7. SVM ピアリングを受け入れます。

```
src::> vservers peer accept -vservers <src_svm> -peer-vservers <dest_svm>
```

8. SVM がピアリングされたことを確認します。

```
dest::> vservers peer show
```

ピアの状態は*peered* ピアリングアプリケーションは*snapmirror*。

ステップ5: ソースシステムとターゲットシステム間の**SnapMirror**レプリケーション関係を作成する

このセクションでは、ソース システムと宛先システム間のSnapMirrorレプリケーション関係を作成する方法について説明します。

既存のSnapMirrorレプリケーション関係を移動するには、まず既存のSnapMirrorレプリケーション関係を解除してから、新しいSnapMirrorレプリケーション関係を作成する必要があります。

次の手順ではONTAP CLI を使用します。

手順

1. 宛先 SVM にデータ保護ボリュームを作成します。

```
dest::> vol create -volume <new_dest_vol> -vservers <dest_svm> -type DP  
-size <10GB> -aggregate <aggr1>
```

2. レプリケーションのSnapMirrorポリシーとスケジュールを含む、宛先にSnapMirrorレプリケーション関係を作成します。

```
dest::> snapmirror create -source-path src_svm:src_vol -destination  
-path dest_svm:new_dest_vol -vserver dest_svm -policy  
MirrorAllSnapshots -schedule 5min
```

3. 宛先でSnapMirrorレプリケーション関係を初期化します。

```
dest::> snapmirror initialize -destination-path <dest_svm:new_dest_vol>
```

4. ONTAP CLI で、次のコマンドを実行してSnapMirror関係のステータスを検証します。

```
dest::> snapmirror show
```

関係のステータスは `Snapmirrored`` そして関係の健全性は ``true`。

5. オプション: ONTAP CLI で次のコマンドを実行して、 SnapMirror関係のアクション履歴を表示します。

```
dest::> snapmirror show-history
```

オプションで、ソース ボリュームと宛先ボリュームをマウントし、ソースにファイルを書き込み、ボリュームが宛先にレプリケートされていることを確認できます。

Google Cloud 管理

Cloud Volumes ONTAPの Google Cloud マシンタイプを変更する

Google Cloud でCloud Volumes ONTAP を起動するときに、いくつかのマシンタイプから選択できます。インスタンスまたはマシンタイプがニーズに対して小さすぎる、または大きすぎると判断した場合は、いつでも変更できます。

タスク概要

- Cloud Volumes ONTAP HA ペアでは自動ギブバックを有効にする必要があります (これがデフォルト設定です)。そうでない場合、操作は失敗します。

["ONTAP 9ドキュメント: 自動ギブバックを設定するためのコマンド"](#)

- マシンタイプを変更すると、Google Cloud サービスの料金に影響する可能性があります。
- この操作により、Cloud Volumes ONTAPが再起動します。

単一ノード システムの場合、I/O が中断されます。

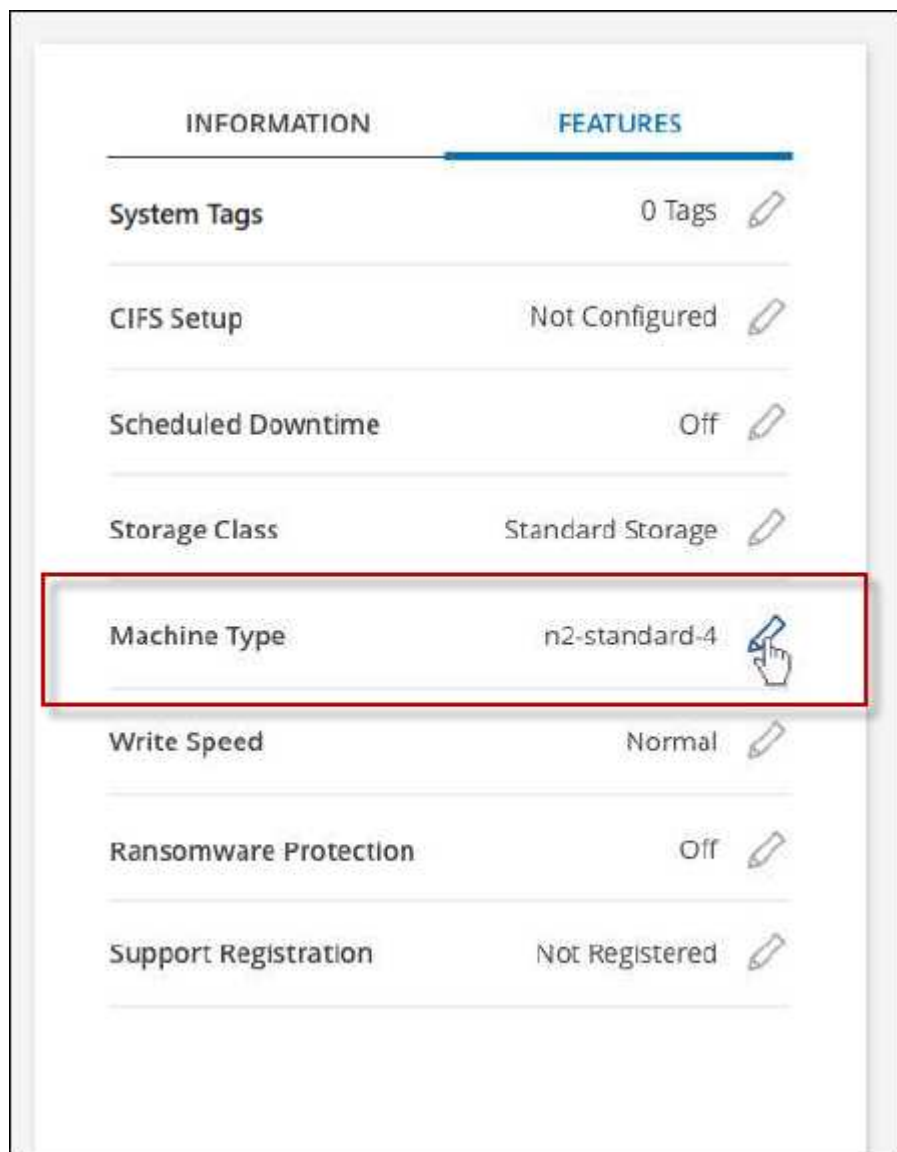
HA ペアの場合、変更は中断なく行われます。HA ペアは引き続きデータを提供します。



NetAppコンソールは、テイクオーバーを開始し、ギブバックを待機することで、一度に1つのノードを変更します。NetAppの品質保証チームは、このプロセス中にファイルの書き込みと読み取りの両方をテストしましたが、クライアント側に問題は見られませんでした。接続が変更されると、I/Oレベルで再試行がいくつか発生しましたが、アプリケーション層はNFS/CIFS接続の再配線を克服しました。

手順

1. *システム*ページで、システムを選択します。
2. [概要] タブで [機能] パネルをクリックし、[マシン タイプ] の横にある鉛筆アイコンをクリックします。



ノードベースの従量課金制 (PAYGO) ライセンスを使用している場合は、ライセンス タイプ の横にある鉛筆アイコンをクリックして、オプションで別のライセンスとマシン タイプを選択できます。

1. マシンの種類を選択し、変更の影響を理解していることを確認するためにチェックボックスをオンにして、[変更] をクリックします。

結果

Cloud Volumes ONTAP は新しい構成で再起動します。

System Manager を使用してCloud Volumes ONTAPを管理する

Cloud Volumes ONTAPの高度なストレージ管理機能は、ONTAPシステムに付属の管理インターフェースであるONTAP System Managerを通じて利用できます。SystemNetAppコンソールから直接 System Manager にアクセスできます。

機能

コンソールのONTAP System Manager を使用して、さまざまなストレージ管理機能を実行できます。以下に、それらの機能の一部を示しますが、網羅的なものではありません。

- 高度なストレージ管理: 整合性グループ、共有、qtree、クォータ、およびストレージ VM を管理します。
- ボリューム移動: ["ボリュームを別のアグリゲートに移動します。"](#)
- ネットワーク管理: IPspace、ネットワーク インターフェイス、ポートセット、イーサネット ポートを管理します。
- FlexGroupボリュームの管理: FlexGroupボリュームの作成と管理は、System Managerからのみ行えます。BlueXPコンソールはFlexGroupボリュームの作成をサポートしていません。
- イベントとジョブ: イベント ログ、システム アラート、ジョブ、監査ログを表示します。
- 高度なデータ保護: ストレージ VM、LUN、整合性グループを保護します。
- ホスト管理: SAN イニシエーター グループと NFS クライアントを設定します。
- S3 オブジェクト ストレージ管理: Cloud Volumes ONTAPの S3 ストレージ管理機能は、System Managerでのみ使用でき、コンソールでは使用できません。

サポートされている構成

- ONTAP System Manager による高度なストレージ管理は、標準クラウド リージョンのCloud Volumes ONTAP 9.10.0 以降で利用できます。
- System Manager の統合は、GovCloud リージョンまたはアウトバウンド インターネット アクセスがないリージョンではサポートされません。

制限事項

System Manager インターフェースに表示されるいくつかの機能は、Cloud Volumes ONTAPではサポートされていません。

- NetAppクラウド ティアリング: Cloud Volumes ONTAP はクラウド ティアリングをサポートしていません。ボリュームを作成するときは、標準ビューから直接オブジェクト ストレージへのデータの階層化を設定する必要があります。
- 階層: System Managerではアグリゲート管理（ローカル階層とクラウド階層を含む）はサポートされていません。集計は標準ビューから直接管理する必要があります。
- ファームウェアのアップグレード: Cloud Volumes ONTAP は、システム マネージャの クラスタ > 設定 ページからの自動ファームウェア更新をサポートしていません。
- ロールベースのアクセス制御: System Manager からのロールベースのアクセス制御はサポートされていません。

- SMB継続的可用性（CA）： Cloud Volumes ONTAPはサポートしていません "継続的に利用可能なSMB共有"中断のない運用を実現します。

システムマネージャにアクセスするための認証を構成する

管理者は、コンソールからONTAP System Manager にアクセスするユーザの認証をアクティブ化できます。ONTAPユーザー ロールに基づいて適切なアクセス権限のレベルを決定し、必要に応じて認証を有効または無効にすることができます。認証を有効にすると、コンソールは認証情報を内部に保存しないため、ユーザーはコンソールから System Manager にアクセスするたび、またはページが再ロードされるたびにONTAPユーザー認証情報を入力する必要があります。認証を無効にすると、ユーザーは管理者の資格情報を使用して System Manager にアクセスできるようになります。



この設定は、 Cloud Volumes ONTAPシステムに関係なく、組織またはアカウント内のONTAPユーザーの各コンソール エージェントに適用されます。

必要な権限

Cloud Volumes ONTAPユーザー認証のコンソールエージェント設定を変更するには、組織またはアカウントの管理者権限が割り当てられている必要があります。

手順

1. 左側のナビゲーション ペインから、管理 > エージェント に移動します。
2. クリック ... 必要なコンソール エージェントのアイコンをクリックし、*コンソール エージェントの編集* を選択します。
3. *ユーザー資格情報の強制*の下で、*有効化/無効化*チェックボックスを選択します。デフォルトでは、認証は無効になっています。



この値を 有効 に設定すると、認証がリセットされ、この変更に対応するために既存のワークフローを変更する必要があります。

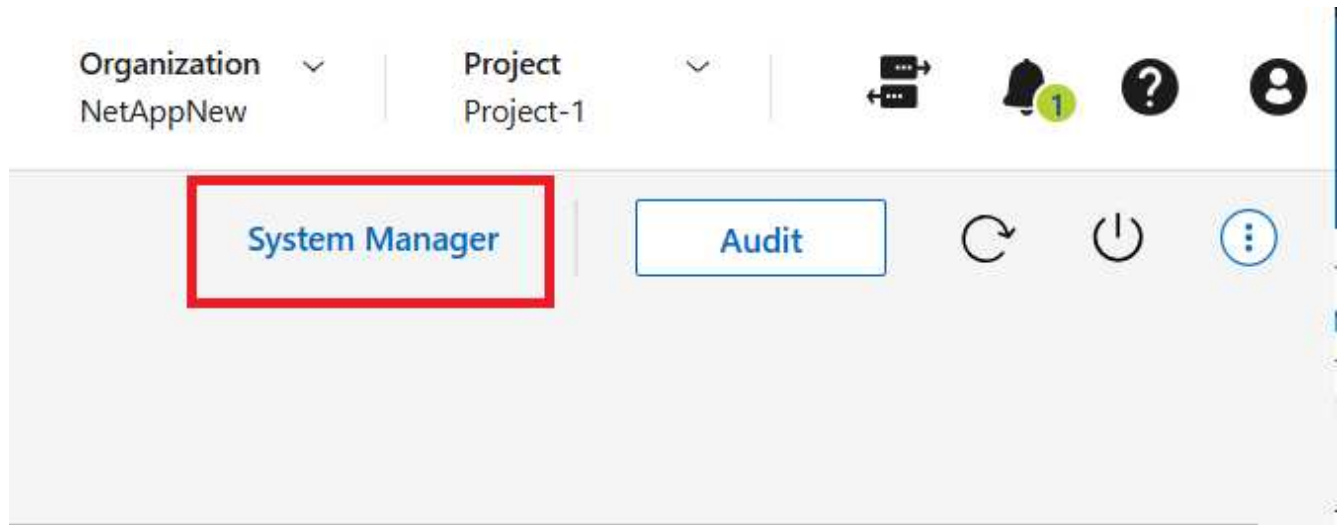
4. *保存*をクリックします。

システムマネージャーを使い始める

Cloud Volumes ONTAPシステムからONTAP System Manager にアクセスできます。

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、必要なCloud Volumes ONTAPシステムをダブルクリックします。
3. *システム マネージャー*をクリックします。



4. プロンプトが表示されたら、ONTAPユーザーの認証情報を入力し、[ログイン] をクリックします。
5. 確認メッセージが表示された場合は、内容を確認して「閉じる」をクリックします。

System Manager を使用して、Cloud Volumes ONTAPシステムを管理します。*戻る*をクリックするとコンソールに戻ることができます。

システムマネージャの使用に関するヘルプ

Cloud Volumes ONTAPでSystem Managerを使用する際にヘルプが必要な場合は、["ONTAPのドキュメント"](#) ステップバイステップの手順についてはこちらをご覧ください。役立つ可能性のあるONTAPドキュメントのリンクをいくつか示します。

- ["ONTAPのロール、アプリケーション、認証"](#)
- ["System Managerを使用したクラスタへのアクセス"](#)。
- ["ボリュームとLUNの管理"](#)
- ["ネットワーク管理"](#)
- ["データ保護"](#)
- ["継続的可用性を備えたSMB共有の作成"](#)

CLIからCloud Volumes ONTAPを管理する

Cloud Volumes ONTAP CLI を使用すると、すべての管理コマンドを実行できるため、高度なタスクや、CLI の使用に慣れている場合に適しています。Secure Shell (SSH) を使用して CLI に接続できます。

開始する前に

SSH を使用してCloud Volumes ONTAPに接続するホストには、Cloud Volumes ONTAPへのネットワーク接続が必要です。たとえば、クラウド プロバイダー ネットワーク内にあるジャンプ ホストから SSH を実行する必要がある場合があります。



複数の AZ に展開されている場合、Cloud Volumes ONTAP HA 構成では、クラスター管理インターフェースにフローティング IP アドレスが使用されるため、外部ルーティングは利用できません。同じルーティング ドメインに属するホストから接続する必要があります。

手順

1. NetAppコンソールで、クラスター管理インターフェースの IP アドレスを特定します。
 - a. 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。
 - b. *システム* ページで、Cloud Volumes ONTAP システムを選択します。
 - c. 右側のペインに表示されるクラスター管理 IP アドレスをコピーします。
2. SSH を使用して、管理者アカウントでクラスター管理インターフェースの IP アドレスに接続します。

例

次の画像は PuTTY を使用した例を示しています。

Specify the destination you want to connect to

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

Connection type:

☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

3. ログインプロンプトで、管理者アカウントのパスワードを入力します。

例

```
Password: *****  
COT2::>
```

システムの健全性とイベント

Cloud Volumes ONTAPのAutoSupport設定を確認する

AutoSupport は、システムの健全性をプロアクティブに監視し、NetAppテクニカル サポートにメッセージを送信します。デフォルトでは、各ノードでAutoSupportが有効になっており、HTTPS トランスポート プロトコルを使用してテクニカル サポートにメッセージを送信します。AutoSupport がこれらのメッセージを送信できることを確認することをお勧めします。

必要な構成手順は、Cloud Volumes ONTAP にアウトバウンドのインターネット接続があることを確認することだけです。詳細については、クラウド プロバイダーのネットワーク要件を参照してください。

AutoSupportの要件

Cloud Volumes ONTAP ノードには、システムの健全性をプロアクティブに監視し、NetAppテクニカル サポートにメッセージを送信するNetApp AutoSupport用のアウトバウンド インターネット アクセスが必要です。

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

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

AutoSupportメッセージを送信するためのアウトバウンド インターネット接続が利用できない場合、NetApp コンソールは、コンソール エージェントをプロキシ サーバーとして使用するようCloud Volumes ONTAPシステムを自動的に構成します。唯一の要件は、コンソール エージェントのセキュリティ グループがポート 3128 経由の受信接続を許可していることを確認することです。コンソール エージェントを展開した後、このポートを開く必要があります。

Cloud Volumes ONTAPに厳密なアウトバウンド ルールを定義した場合は、Cloud Volumes ONTAPセキュリティ グループがポート 3128 経由のアウトバウンド接続を許可していることも確認する必要があります。



HA ペアを使用している場合、HA メディエーターは発信インターネット アクセスを必要としません。

送信インターネット アクセスが利用可能であることを確認したら、AutoSupportをテストして、メッセージを送信できることを確認できます。手順については、"[ONTAPドキュメント: AutoSupportのセットアップ](#)"。

AutoSupport構成のトラブルシューティング

アウトバウンド接続が利用できず、コンソールがCloud Volumes ONTAPシステムをコンソール エージェントをプロキシ サーバーとして使用するよう構成できない場合は、コンソールから「<システム名>はAutoSupportメッセージを送信できません」というタイトルの通知が表示されます。

おそらく、ネットワークの問題が原因でこのメッセージが表示されていると思われます。

この問題に対処するには、次の手順に従ってください。

手順

1. ONTAP CLI からシステムを管理できるように、Cloud Volumes ONTAPシステムに SSH で接続します。

["Cloud Volumes ONTAPへのSSH接続方法を学ぶ"](#)。

2. AutoSupportサブシステムの詳細なステータスを表示します。

```
autosupport check show-details
```

応答は次のようになります。

```

Category: smtp
  Component: mail-server
    Status: failed
    Detail: SMTP connectivity check failed for destination:
            mailhost. Error: Could not resolve host -
'mailhost'
    Corrective Action: Check the hostname of the SMTP server

Category: http-https
  Component: http-put-destination
    Status: ok
    Detail: Successfully connected to:
            <https://support.netapp.com/put/AsupPut/>.

  Component: http-post-destination
    Status: ok
    Detail: Successfully connected to:

https://support.netapp.com/asupprod/post/1.0/postAsup.

Category: on-demand
  Component: ondemand-server
    Status: ok
    Detail: Successfully connected to:
            https://support.netapp.com/aods/asupmessage.

Category: configuration
  Component: configuration
    Status: ok
    Detail: No configuration issues found.
5 entries were displayed.

```

http-https カテゴリのステータスが「ok」の場合、AutoSupportが適切に構成されており、メッセージを送信できることを意味します。

3. ステータスが正常でない場合は、各Cloud Volumes ONTAPノードのプロキシ URL を確認します。

```
autosupport show -fields proxy-url
```

4. プロキシ URL パラメータが空の場合は、コンソール エージェントをプロキシとして使用するよう
にCloud Volumes ONTAPを構成します。

```
autosupport modify -proxy-url http://<console agent private ip>:3128
```

5. AutoSupport のステータスを再度確認します。

```
autosupport check show-details
```

6. ステータスがまだ失敗の場合、ポート 3128 経由でCloud Volumes ONTAPとコンソール エージェント間の接続があることを確認します。
7. 接続があることを確認した後もステータス ID が失敗する場合は、コンソール エージェントに SSH で接続します。

"コンソールエージェントの Linux VM への接続の詳細"

8. ヘ移動 /opt/application/netapp/cloudmanager/docker_occm/data/
9. プロキシ設定ファイルを開く squid.conf

ファイルの基本構造は次のとおりです。

```
http_port 3128
acl localnet src 172.31.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

localnet src 値は、Cloud Volumes ONTAPシステムの CIDR です。

10. Cloud Volumes ONTAPシステムの CIDR ブロックがファイルに指定されている範囲内でない場合は、次のように値を更新するか、新しいエントリを追加します。

```
acl cvonet src <cidr>
```

この新しいエントリを追加する場合は、許可エントリも追加することを忘れないでください。

```
http_access allow cvonet
```

次に例を示します。

```
http_port 3128
acl localnet src 172.31.0.0/16
acl cvonet src 172.33.0.0/16
acl azure_aws_metadata dst 169.254.169.254

http_access allow localnet
http_access allow cvonet
http_access deny azure_aws_metadata
http_access allow localhost
http_access deny all
```

11. 設定ファイルを編集した後、sudo としてプロキシ コンテナを再起動します。

```
docker restart squid
```

12. Cloud Volumes ONTAP CLI に戻り、Cloud Volumes ONTAP が AutoSupport メッセージを送信できることを確認します。

```
autosupport check show-details
```

Cloud Volumes ONTAP システム用の EMS を構成する

イベント管理システム (EMS) は、ONTAP システムで発生するイベントに関する情報を収集して表示します。イベント通知を受信するには、特定のイベント重大度に対してイベントの宛先 (電子メール アドレス、SNMP トラップ ホスト、または Syslog サーバー) とイベント ルートを設定できます。

CLI を使用して EMS を設定できます。手順については、["ONTAP ドキュメント: EMS 構成の概要"](#)。

概念

ライセンス

Cloud Volumes ONTAPのライセンス

Cloud Volumes ONTAPにはいくつかのライセンス オプションがあります。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。

ライセンスの概要

新規のお客様には、次のライセンス オプションをご利用いただけます。

容量ベースのライセンス

プロビジョニングされた容量に応じて、NetAppアカウント内の複数のCloud Volumes ONTAPシステムの料金を支払います。アドオンのクラウド データ サービスを購入する機能が含まれます。容量ベースのライセンスの消費モデルの詳細については、以下を参照してください。["容量ベースのライセンスについて詳しく見る"](#)。

Keystoneサブスクリプション

高可用性 (HA) ペアにシームレスなハイブリッド クラウド エクスペリエンスを提供する、成長に合わせて支払うサブスクリプション ベースのサービスです。

次のセクションでは、これらの各オプションについて詳しく説明します。



ライセンスなしでライセンス機能を使用する場合、サポートは提供されません。

容量ベースのライセンス

容量ベースのライセンス パッケージでは、容量 1 TiB ごとにCloud Volumes ONTAP の料金を支払うことができます。ライセンスはNetAppアカウントに関連付けられており、ライセンスを通じて十分な容量が利用できる限り、複数のシステムにライセンスを課金することができます。

たとえば、20 TiB のライセンスを 1 つ購入し、4 つのCloud Volumes ONTAPシステムを導入し、各システムに 5 TiB のボリュームを割り当てて、合計 20 TiB にすることができます。容量は、そのアカウントに導入された各Cloud Volumes ONTAPシステム上のボリュームで利用できます。

容量ベースのライセンスは、パッケージ の形式で利用できます。Cloud Volumes ONTAPシステムを導入する場合、ビジネス ニーズに応じて複数のライセンス パッケージから選択できます。



NetAppコンソールで管理される製品とサービスの実際の使用量と計測値は常に GiB と TiB で計算されますが、GB/GiB と TB/TiB という用語は同じ意味で使用されます。これは、クラウド マーケットプレイスのリスト、価格見積、リストの説明、およびその他のサポート ドキュメントに反映されます。

パッケージ

Cloud Volumes ONTAPでは、次の容量ベースのパッケージが利用できます。容量ベースのライセンスパッケ

ージの詳細については、以下を参照してください。"[容量ベースのライセンスについて詳しく見る](#)"。

次の容量ベースのパッケージでサポートされている VM タイプの一覧については、以下を参照してください。

- "[Azureでサポートされている構成](#)"
- "[Google Cloud でサポートされている構成](#)"

フリーミアム

NetAppからすべてのCloud Volumes ONTAP機能を無料で提供します (クラウド プロバイダーの料金は引き続き適用されます)。フリーミアム パッケージには次の特徴があります。

- ライセンスや契約は必要ありません。
- NetAppからのサポートは含まれていません。
- Cloud Volumes ONTAPシステムごとにプロビジョニングできる容量は 500 GiB に制限されます。
- どのクラウド プロバイダーでも、NetAppアカウントごとに最大 10 個のCloud Volumes ONTAPシステムを Freemium で使用できます。
- Cloud Volumes ONTAPシステムのプロビジョニングされた容量が 500 GiB を超える場合、コンソールはシステムを Essentials パッケージに変換します。

システムがEssentialsパッケージに変換されるとすぐに、"[最低充電](#)"それに適用されます。

Essentials パッケージに変換されたCloud Volumes ONTAPシステムは、プロビジョニングされた容量が 500 GiB 未満に削減された場合でも、Freemium に戻すことはできません。プロビジョニングされた容量が 500 GiB 未満のその他のシステムは、フリーミアムのままとなります (フリーミアム オファリングを使用して展開されている限り)。

必需品

さまざまな構成で容量に応じてお支払いいただけます。

- Cloud Volumes ONTAP構成を選択します。
 - 単一ノードまたはHAシステム
 - 災害復旧 (DR) 用のファイルおよびブロック ストレージまたはセカンダリ データ
- 追加料金でNetAppのクラウドデータサービスを追加できます

プロ

無制限のバックアップを備えたあらゆるタイプのCloud Volumes ONTAP構成に対して、容量に応じて料金を支払います。

- あらゆるCloud Volumes ONTAP構成のライセンスを提供します

プライマリボリュームとセカンダリボリュームの容量が同じ料金で課金される単一ノードまたはHA

- NetApp Backup and Recovery を使用した無制限のボリューム バックアップが含まれますが、Professional パッケージを使用するCloud Volumes ONTAPシステムのみが対象です。



バックアップとリカバリには従量課金制 (PAYGO) サブスクリプションが必要ですが、このサービスの使用に対して料金は発生しません。バックアップとリカバリのライセンス設定の詳細については、以下を参照してください。 ["バックアップとリカバリのライセンスを設定する"](#)。

- 追加料金でNetAppのクラウドデータサービスを追加できます

容量ベースのライセンスの可用性

Cloud Volumes ONTAPシステムで PAYGO ライセンスと BYOL ライセンスを使用するには、コンソール エージェントが稼働している必要があります。

["コンソールエージェントについて学ぶ"](#)。



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"](#)。

始め方

容量ベースのライセンスを開始する方法については、以下をご覧ください。

- ["AWSでCloud Volumes ONTAPのライセンスを設定する"](#)
- ["AzureでCloud Volumes ONTAPのライセンスを設定する"](#)
- ["Google Cloud でCloud Volumes ONTAPのライセンスを設定する"](#)

Keystoneサブスクリプション

成長に合わせて支払うサブスクリプションベースのサービスで、先行の CapEx やリースよりも OpEx 消費モデルを好むユーザーにシームレスなハイブリッド クラウド エクスペリエンスを提供します。

料金は、Keystoneサブスクリプション内の 1 つ以上のCloud Volumes ONTAP HA ペアのコミット容量のサイズに基づいて計算されます。

各ボリュームのプロビジョニングされた容量は定期的に集計され、Keystoneサブスクリプションのコミットされた容量と比較され、超過分はKeystoneサブスクリプションのバーストとして課金されます。

["NetApp Keystoneの詳細はこちら"](#)。

サポートされている構成

Keystoneサブスクリプションは HA ペアでサポートされます。現時点では、このライセンス オプションは単一ノード システムではサポートされていません。

容量制限

容量ベースのライセンス モデルでは、各Cloud Volumes ONTAPシステムはオブジェクト ストレージへの階層化をサポートし、階層化された合計容量はクラウド プロバイダーのバケット制限まで拡張できます。ライセンスには容量制限はありませんが、 ["『FabricPoolのベストプラクティス』"](#) 階層化を構成および管理する際に最適なパフォーマンス、信頼性、コスト効率を確保します。

各クラウド プロバイダーの容量制限については、各プロバイダーのドキュメントを参照してください。

- ["AWSのドキュメント"](#)
- ["マネージド ディスクに関する Azure ドキュメント"](#)そして ["BLOB ストレージに関する Azure ドキュメント"](#)
- ["Google Cloud ドキュメント"](#)

始め方

Keystoneサブスクリプションの開始方法については、以下をご覧ください。

- ["AWSでCloud Volumes ONTAPのライセンスを設定する"](#)
- ["AzureでCloud Volumes ONTAPのライセンスを設定する"](#)
- ["Google Cloud でCloud Volumes ONTAPのライセンスを設定する"](#)

ノードベースのライセンス

ノードベースのライセンスは、ノードごとにCloud Volumes ONTAP のライセンスを取得できる前世代のライセンス モデルです。このライセンス モデルは新規顧客にはご利用いただけません。ノード単位の課金は、上記の容量単位の課金方法に置き換えられました。

NetApp は、ノードベースのライセンスの提供終了 (EOA) とサポート終了 (EOS) を計画しています。EOA および EOS の後は、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必要があります。

詳細については、["顧客通信: CPC-00589"](#)。

ノードベースライセンスの提供終了

2024 年 11 月 11 日以降、ノードベースのライセンスの限定的な提供は終了しました。ノードベースのライセンスのサポートは、2024 年 12 月 31 日に終了します。

EOA 日付を超えて有効なノードベースの契約がある場合は、契約の有効期限が切れるまでライセンスを引き続き使用できます。契約期間が終了すると、容量ベースのライセンス モデルに移行する必要があります。Cloud Volumes ONTAPノードの長期契約がない場合は、EOS 日付までに変換を計画することが重要です。

各ライセンスの種類と EOA の影響について詳しくは、次の表をご覧ください。

ライセンス タイプ	EOA後の影響
BYOL（個人ライセンス持ち込み）を通じて購入した有効なノードベースのライセンス	ライセンスは有効期限まで有効です。既存の未使用のノードベースのライセンスは、新しいCloud Volumes ONTAPシステムの展開に使用できます。
BYOL を通じて購入したノードベースのライセンスの期限切れ	このライセンスを使用して新しいCloud Volumes ONTAPシステムを展開する権利はありません。既存のシステムは引き続き動作する可能性があります。が、EOS 日以降はシステムに対するサポートや更新は受けられなくなります。
PAYGOサブスクリプション付きの有効なノードベースのライセンス	EOS 日以降は、容量ベースのライセンスに移行するまで、NetApp のサポートを受けられなくなります。

除外事項

NetApp は、特定の状況では特別な考慮が必要であることを認識しており、ノードベースのライセンスの EOA と EOS は次の場合には適用されません。

- 米国公共部門の顧客
- プライベートモードでのデプロイメント
- AWS における Cloud Volumes ONTAP の中国リージョン展開

これらの特定のシナリオでは、NetApp は契約上の義務と運用上のニーズに準拠した固有のライセンス要件に対処するためのサポートを提供します。



このようなシナリオの場合でも、新しいノードベースのライセンスとライセンスの更新は、承認日から最大 1 年間有効です。

ライセンス変換

コンソールでは、ライセンス変換ツールを使用して、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シームレスに変換できます。ノードベースライセンスのEOA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"](#)。

移行する前に、2 つのライセンス モデルの違いを理解しておくことをお勧めします。ノードベースのライセンスには、各 ONTAP インスタンスの固定容量が含まれるため、柔軟性が制限される可能性があります。一方、容量ベースのライセンスでは、複数のインスタンス間でストレージの共有プールが可能になり、柔軟性が向上し、リソース使用率が最適化され、ワークロードを再配分する際の金銭的なペナルティの可能性が軽減されます。容量ベースの課金により、変化するストレージ要件にシームレスに適応します。

この変換を実行する方法については、["Cloud Volumes ONTAP 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"](#)。



システムを容量ベースからノードベースのライセンスに変換することはサポートされていません。

Cloud Volumes ONTAP の容量ベースのライセンスの詳細

容量ベースのライセンスの課金と容量使用について理解しておく必要があります。

消費モデル

容量ベースのライセンス パッケージは、次の消費モデルで利用できます。

- **BYOL:** 自分のライセンスを持ち込みます (BYOL)。NetApp から購入したライセンスで、任意のクラウド プロバイダーに Cloud Volumes ONTAP を展開するために使用できます。



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"](#)。

- **PAYGO:** 従量課金制 (PAYGO) サブスクリプションは、クラウド プロバイダーのマーケットプレイスからの時間単位のサブスクリプションです。

- 年間: クラウド プロバイダーのマーケットプレイスからの年間契約。

次の点に注意してください。

- NetApp (BYOL) からライセンスを購入する場合は、クラウドプロバイダーのマーケットプレイスからPAYGOプランに加入する必要があります。NetAppはBYOLライセンスに制限を設けています。BYOLライセンスの有効期限が切れた場合は、クラウドマーケットプレイスのサブスクリプションに切り替えていただく必要があります。

ライセンスは常に最初に課金されますが、以下の場合にはマーケットプレイスの時間単位料金で課金されます。

- ライセンス容量を超えた場合
- ライセンスの有効期限が切れた場合
- マーケットプレイスから年間契約を結んでいる場合、導入するすべてのCloud Volumes ONTAPシステムに対してその契約料金が課金されます。年間マーケットプレイス契約と BYOL を組み合わせることはできません。
- 中国リージョンでは、BYOL 対応のシングルノードシステムのみがサポートされます。中国リージョンでのデプロイメントは、BYOL ライセンスの制限の対象外となります。

パッケージの変更

展開後に、容量ベースのライセンスを使用するCloud Volumes ONTAPシステムのパッケージを変更できます。たとえば、Essentials パッケージを使用してCloud Volumes ONTAPシステムを導入した場合、ビジネスニーズの変化に応じて Professional パッケージに変更できます。

["充電方法の変更方法を学ぶ"](#)。

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方法については、[以下を参照してください](#)。

価格とサポートされる構成

価格の詳細については、["NetAppコンソールのウェブサイト"](#)。

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

Storage VM

- 追加のデータ サービス ストレージ VM (SVM) には追加のライセンス コストは発生しませんが、データ サービス SVM ごとに 4 TiB の最小容量料金が発生します。
- ディザスタリカバリ SVM は、プロビジョニングされた容量に応じて課金されます。

HAペア

HA ペアの場合、ノードにプロビジョニングされた容量に対してのみ課金されます。パートナー ノードに同期的にミラーリングされるデータに対しては料金は発生しません。

FlexCloneおよびFlexCacheボリューム

- FlexCloneボリュームで使用される容量に対しては料金は発生しません。

- ソースおよび宛先のFlexCacheボリュームはプライマリ データと見なされ、プロビジョニングされたスペースに応じて課金されます。

容量制限

容量ベースのライセンス モデルでは、各Cloud Volumes ONTAPシステムはオブジェクト ストレージへの階層化をサポートし、階層化された合計容量はクラウド プロバイダーのバケット制限まで拡張できます。ライセンスには容量制限はありませんが、"[『FabricPoolのベストプラクティス』](#)"階層化を構成および管理する際に最適なパフォーマンス、信頼性、コスト効率を確保します。

各クラウド プロバイダーの容量制限については、各プロバイダーのドキュメントを参照してください。

- "[AWSのドキュメント](#)"
- "[マネージド ディスクに関する Azure ドキュメント](#)"そして "[BLOB ストレージに関する Azure ドキュメント](#)"
- "[Google Cloud ドキュメント](#)"

システムの最大数

容量ベースのライセンスでは、Cloud Volumes ONTAPシステムの最大数は、NetAppコンソール アカウントごとに 24 に制限されます。システム とは、Cloud Volumes ONTAP HA ペア、Cloud Volumes ONTAPシングルノード システム、または作成した追加のストレージ VM です。デフォルトのストレージ VM は制限にカウントされません。この制限はすべてのライセンス モデルに適用されます。

たとえば、次の 3 つのシステムがあるとして。

- 1 つのストレージ VM を備えた単一ノードのCloud Volumes ONTAPシステム (これは、Cloud Volumes ONTAPを展開するときに作成されるデフォルトのストレージ VM です)

このシステムは 1 つのシステムとしてカウントされます。

- 2 つのストレージ VM (デフォルトのストレージ VM と、作成した追加のストレージ VM 1 つ) を備えた単一ノードのCloud Volumes ONTAPシステム

このシステムは、単一ノード システム用と追加ストレージ VM 用の 1 つの合計 2 つのシステムとしてカウントされます。

- 3 つのストレージ VM (デフォルトのストレージ VM と、作成した 2 つの追加ストレージ VM) を備えたCloud Volumes ONTAP HA ペア

このシステムは、HA ペア用に 1 つ、追加のストレージ VM 用に 2 つ、合わせて 3 つのシステムとしてカウントされます。

合計で6つのシステムになります。すると、アカウントにさらに 14 個のシステムを追加できるスペースが確保されます。

24 台を超えるシステムが必要な大規模な展開の場合は、アカウント担当者または営業チームにお問い合わせください。

["コンソールアカウントの詳細"](#)。

充電に関する注意事項

次の詳細は、容量ベースのライセンスでの課金の仕組みを理解するのに役立ちます。

最低料金

少なくとも 1 つのプライマリ (読み取り/書き込み) ボリュームを持つデータ サービス ストレージ VM ごとに、4 TiB の最小料金がかかります。プライマリ ボリュームの合計が 4 TiB 未満の場合、コンソールはそのストレージ VM に 4 TiB の最小料金を適用します。

まだボリュームをプロビジョニングしていない場合は、最低料金は適用されません。

Essentials パッケージの場合、4 TiB の最小容量料金は、セカンダリ (データ保護) ボリュームのみを含むストレージ VM には適用されません。たとえば、1 TiB のセカンダリ データを持つストレージ VM がある場合、その 1 TiB のデータに対してのみ課金されます。プロフェッショナル パッケージ タイプでは、ボリューム タイプに関係なく、4 TiB の最小容量課金が適用されます。

超過料金

BYOL容量を超過した場合、マーケットプレースのサブスクリプションに基づいて、超過分に対して時間単位の料金が請求されます。超過分はマーケットプレースの料金で請求され、他のライセンスの利用可能な容量が優先されます。BYOLライセンスの有効期限が切れた場合は、クラウドマーケットプレースを通じて容量ベースのライセンスモデルに移行する必要があります。

エッセンシャルパッケージ

Essentials パッケージでは、デプロイメント タイプ (HA または単一ノード) とボリューム タイプ (プライマリまたはセカンダリ) に基づいて課金されます。価格は、高いものから低いものの順に、*Essentials Primary HA*、*Essentials Primary Single Node*、*Essentials Secondary HA*、*Essentials Secondary Single Node* となります。あるいは、マーケットプレース契約を購入するか、プライベート オファーを受け入れる場合、容量料金はどのデプロイメントまたはボリューム タイプでも同じになります。

ライセンスは、Cloud Volumes ONTAPシステム内で作成されたボリューム タイプに基づいて決定されます。

- Essentials シングルノード: 1 つのONTAPノードのみを使用して、Cloud Volumes ONTAPシステムで作成されたボリュームの読み取り/書き込み。
- Essentials HA: 相互にフェイルオーバーして中断のないデータ アクセスを実現できる 2 つのONTAPノードを使用してボリュームの読み取り/書き込みを行います。
- Essentials セカンダリ シングル ノード: 1 つのONTAPノードのみを使用してCloud Volumes ONTAPシステム上に作成されたデータ保護 (DP) タイプのボリューム (通常は読み取り専用のSnapMirrorまたはSnapVault宛先ボリューム)。



読み取り専用/DP ボリュームがプライマリ ボリュームになった場合、コンソールはそれをプライマリ データと見なし、ボリュームが読み取り/書き込みモードであった時間に基づいて課金コストを計算します。ボリュームが再び読み取り専用/DP になると、ボリュームは再びセカンダリ データとして扱われ、コンソール内の最適なライセンスを使用してそれに応じて課金されます。

- Essentials セカンダリ HA: 中断のないデータ アクセスのために相互にフェイルオーバーできる 2 つのONTAPSnapMirrorを使用してCloud Volumes ONTAPシステム上に作成されたデータ保護 (DP) タイプの

ボリューム (通常はSnapVault専用の SnapMirror または SnapVault 宛先ボリューム)。

BYOL

NetAppから Essentials ライセンスを購入し (BYOL)、そのデプロイメントとボリューム タイプに対してライセンスされた容量を超えた場合、コンソールはより高価な Essentials ライセンス (所有していて、使用可能な容量がある場合) に対して超過分を請求します。これは、マーケットプレイスに対して請求する前に、すでに購入済みの利用可能な容量をまずプリペイド容量として使用するためです。BYOL ライセンスで利用可能な容量がない場合、超過した容量はマーケットプレイスのオンデマンド時間料金 (PAYGO) で課金され、毎月の請求額にコストが追加されます。

ここに例があります。Essentials パッケージの次のライセンスがあるとします。

- 500 TiB のコミット容量を持つ 500 TiB の *Essentials Secondary HA* ライセンス
- コミットされた容量が100 TiBのみである500 TiBの *_Essentials Single Node_* ライセンス

セカンダリ ボリュームを持つ HA ペアにさらに 50 TiB がプロビジョニングされます。コンソールは、その 50 TiB を PAYGO に請求する代わりに、*Essentials Single Node* ライセンスに対して 50 TiB の超過分を請求します。このライセンスの価格は *Essentials Secondary HA* よりも高額ですが、すでに購入済みのライセンスを使用するため、毎月の請求額に追加費用はかかりません。

管理 > ライセンスとサブスクリプション で、*Essentials Single Node* ライセンスに対して 50 TiB が課金されていることを確認できます。

もう一つの例を挙げます。Essentials パッケージの次のライセンスがあるとします。

- 500 TiB のコミット容量を持つ 500 TiB の *Essentials Secondary HA* ライセンス
- コミットされた容量が100 TiBのみである500 TiBの *_Essentials Single Node_* ライセンス

プライマリ ボリュームを持つ HA ペアにさらに 100 TiB がプロビジョニングされます。購入したライセンスには、*Essentials Primary HA* コミット容量がありません。*Essentials Primary HA* ライセンスの価格は、*Essentials Primary Single Node* ライセンスと *Essentials Secondary HA* ライセンスの両方よりも高くなります。

この例では、コンソールは追加の 100 TiB に対してマーケットプレイス レートで超過料金を請求します。超過料金は毎月の請求書に表示されます。

マーケットプレイス契約またはプライベートオファー

マーケットプレイス契約またはプライベート オファーの一部として Essentials ライセンスを購入した場合、BYOL ロジックは適用されず、使用目的に合った正確なライセンス タイプが必要になります。ライセンス タイプには、ボリューム タイプ (プライマリまたはセカンダリ) と展開タイプ (HA または単一ノード) が含まれます。

たとえば、Essentials ライセンスを使用して Cloud Volumes ONTAP インスタンスをデプロイするとします。次に、読み取り/書き込みボリューム (プライマリ単一ノード) と読み取り専用ボリューム (セカンダリ単一ノード) をプロビジョニングします。マーケットプレイス契約またはプライベート オファーには、プロビジョニングされた容量をカバーするために、*Essentials* シングル ノード と *Essentials* セカンダリ シングル ノード の容量が含まれている必要があります。マーケットプレイス契約またはプライベート オファーの一部ではないプロビジョニングされた容量については、オンデマンドの時間単位料金 (PAYGO) で課金され、毎月の請求額にコストが追加されます。

ストレージ

Cloud Volumes ONTAPでサポートされているクライアント プロトコル

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

iSCSI

iSCSIは、標準のイーサネット ネットワークで実行できるブロック プロトコルです。ほとんどのクライアント オペレーティング システムでは、標準のイーサネット ポート経由で実行されるソフトウェア イニシエーターが提供されます。

NFS

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

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

SMB

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

S3

Cloud Volumes ONTAP は、スケールアウト ストレージのオプションとして S3 をサポートしています。S3 プロトコル サポートにより、ストレージ VM (SVM) 内のバケットに含まれるオブジェクトへの S3 クライアント アクセスを構成できます。

["ONTAPドキュメント: S3マルチプロトコルの仕組みを学ぶ"](#)。 ["ONTAPドキュメント: ONTAPでS3オブジェクトストレージサービスを設定および管理する方法を学びます"](#)。

NVMe-TCP

ONTAPバージョン 9.12.1 以降では、クラウド プロバイダーで NVMe-TCP がサポートされます。NetApp コンソールは、NVMe-TCP の管理機能を提供しません。

ONTAP経由での NVMe の設定の詳細については、["ONTAPドキュメント: NVMe用のストレージVMを構成する"](#)。

Cloud Volumes ONTAPクラスターに使用されるディスクとアグリゲート

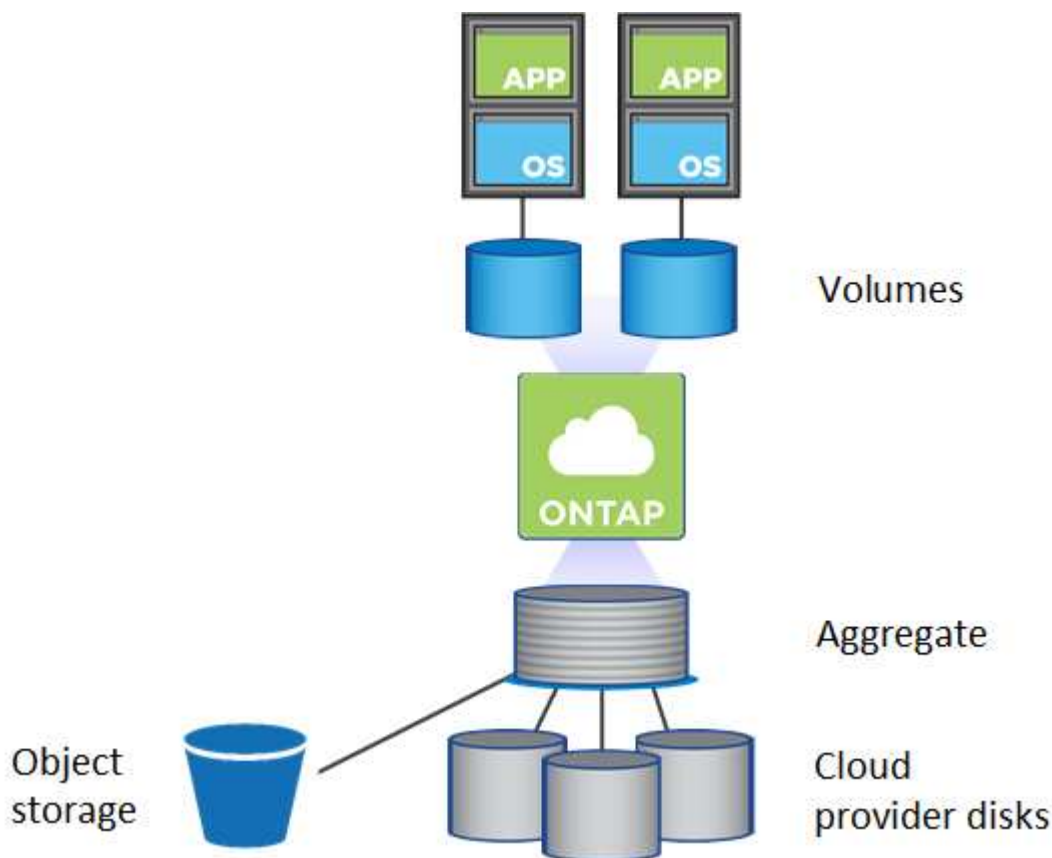
Cloud Volumes ONTAP がクラウド ストレージを使用する方法を理解すると、ストレージ コストを理解するのに役立ちます。



すべてのディスクとアグリゲートはNetAppコンソールから作成および削除する必要があります。これらのアクションを別の管理ツールから実行しないでください。そうすると、システムの安定性に影響が及び、将来的にディスクを追加する能力が妨げられ、クラウド プロバイダーの料金が重複して発生する可能性があります。

概要

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



いくつかの種類のクラウド ディスクがサポートされています。ボリュームを作成するときにディスク タイプを選択し、Cloud Volumes ONTAPをデプロイするときにデフォルトのディスク サイズを選択します。



クラウド プロバイダーから購入したストレージの合計量が生の容量 です。使用可能な容量 が少なくなるのは、約 12 ~ 14 パーセントがCloud Volumes ONTAP の使用のために予約されているオーバーヘッドであるためです。たとえば、コンソールが 500 GiB のアグリゲートを作成した場合、使用可能な容量は 442.94 GiB になります。

AWSストレージ

AWS では、Cloud Volumes ONTAP はユーザー データ用に EBS ストレージを使用し、一部の EC2 インスタンス タイプではフラッシュ キャッシュとしてローカル NVMe ストレージを使用します。

EBSストレージ

AWS では、アグリゲートには最大 6 個の同じサイズのディスクを含めることができます。ただし、Amazon EBS Elastic Volumes 機能をサポートする構成の場合、アグリゲートには最大 8 個のディスク

を含めることができます。["エラスティックボリュームのサポートについて詳しくはこちら"](#)。

最大ディスク サイズは 16 TiB です。

基盤となる EBS ディスク タイプは、汎用 SSD (gp3 または gp2)、プロビジョニングされた IOPS SSD (io1)、またはスループット最適化 HDD (st1) のいずれかになります。EBS ディスクを Amazon S3 とペアリングして、["低コストのオブジェクトストレージ"](#)。



スループット最適化 HDD (st1) を使用する場合、オブジェクト ストレージへのデータの階層化は推奨されません。

ローカル NVMe ストレージ

一部の EC2 インスタンスタイプにはローカル NVMe ストレージが含まれており、Cloud Volumes ONTAP はこれを ["Flash Cache"](#)。

関連リンク

- ["AWS ドキュメント: EBS ボリュームタイプ"](#)
- ["AWS のシステムに適したディスクタイプとディスクサイズの選択方法を学びます"](#)
- ["AWS の Cloud Volumes ONTAP のストレージ制限を確認する"](#)
- ["AWS で Cloud Volumes ONTAP がサポートする構成を確認する"](#)

Azure ストレージ

Azure では、アグリゲートには、すべて同じサイズのディスクを最大 12 個まで含めることができます。ディスク タイプと最大ディスク サイズは、単一ノード システムを使用するか、HA ペアを使用するかによって異なります。

単一ノードシステム

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、単一ノードと HA ペアの両方で、より高いパフォーマンスとより低いレイテンシ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。

各マネージド ディスク タイプの最大ディスク サイズは 32 TiB です。

マネージドディスクを Azure Blob ストレージとペアリングして、["低コストのオブジェクトストレージ"](#)。

HA ペア

HA ペアは、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する 2 種類のディスクを使用します。

- 最大ディスクサイズが 8 TiB の プレミアム ページ BLOB
- 最大ディスクサイズが 32 TiB の マネージド ディスク

関連リンク

- ["Azure のシステムに適したディスクの種類とディスク サイズを選択する方法を学びます"](#)
- ["AzureでCloud Volumes ONTAP HAペアを起動する"](#)
- ["Microsoft Azure ドキュメント: Azure マネージド ディスクの種類"](#)
- ["Microsoft Azure ドキュメント: Azure ページ BLOB の概要"](#)
- ["Azure のCloud Volumes ONTAPのストレージ制限を確認する"](#)

Google Cloud ストレージ

Google Cloud では、アグリゲートには最大 6 個の同じサイズのディスクを含めることができます。最大ディスク サイズは 64 TiB です。

ディスク タイプは、ゾーン SSD 永続ディスク、ゾーン バランス永続ディスク、ゾーン標準永続ディスク のいずれかになります。永続ディスクをGoogle Storageバケットとペアリングして、["低コストのオブジェクトストレージ"](#)。

関連リンク

- ["Google Cloud ドキュメント: ストレージ オプション"](#)
- ["Google Cloud のCloud Volumes ONTAPのストレージ制限を確認する"](#)

RAIDタイプ

各Cloud Volumes ONTAPアグリゲートの RAID タイプは RAID0 (ストライピング) です。Cloud Volumes ONTAP は、ディスクの可用性と耐久性をクラウド プロバイダーに依存します。他の RAID タイプはサポートされていません。

ホット スペア

RAID0 は冗長性のためのホットスペアの使用をサポートしていません。

Cloud Volumes ONTAPインスタンスに接続された未使用のディスク (ホット スペア) を作成することは不必要な費用がかかり、必要に応じて追加のスペースをプロビジョニングできなくなる可能性があります。したがって、お勧めできません。

Cloud Volumes ONTAPによる AWS Elastic Volumes のサポートについて学ぶ

Cloud Volumes ONTAPアグリゲートによる Amazon EBS Elastic Volumes 機能のサポートにより、パフォーマンスが向上し、容量が追加されるとともに、NetAppコンソールが必要に応じて基盤となるディスク容量を自動的に増やすことが可能になります。

利点

- ダイナミックディスクの拡張

コンソールは、Cloud Volumes ONTAP の実行中、およびディスクがまだ接続されている間に、ディスクのサイズを動的に増やすことができます。

- パフォーマンスの向上

エラスティック ボリュームが有効になっているアグリゲートには、2 つの RAID グループ間で均等に利用される最大 8 個のディスクを含めることができます。この構成により、スループットが向上し、パフォーマンスが安定します。

- より大きな骨材

8 つのディスクをサポートすることで、最大合計容量は 128 TiB になります。これらの制限は、Elastic Volumes 機能が有効になっていないアグリゲートの 6 ディスク制限および 96 TiB 制限よりも高くなります。

システム全体の容量制限は同じままであることに注意してください。

"AWSドキュメント: AWSのElastic Volumesの詳細"

サポートされている構成

Amazon EBS Elastic Volumes 機能は、特定のCloud Volumes ONTAPバージョンおよび特定の EBS ディスクタイプでサポートされています。

Cloud Volumes ONTAPバージョン

Elastic Volumes 機能は、バージョン 9.11.0 以降で作成された新しいCloud Volumes ONTAPシステムでサポートされています。この機能は、9.11.0 より前に導入された既存のCloud Volumes ONTAPシステムではサポートされていません。

たとえば、Cloud Volumes ONTAP 9.9.0 システムを作成し、後でそのシステムをバージョン 9.11.0 にアップグレードした場合、Elastic Volumes 機能はサポートされません。バージョン 9.11.0 以降を使用して導入された新しいシステムである必要があります。

EBSディスクタイプ

汎用 SSD (gp3) またはプロビジョニングされた IOPS SSD (io1) を使用する場合、Elastic Volumes 機能は集約レベルで自動的に有効になります。エラスティック ボリューム機能は、他のディスク タイプを使用するアグリゲートではサポートされません。

必要なAWS権限

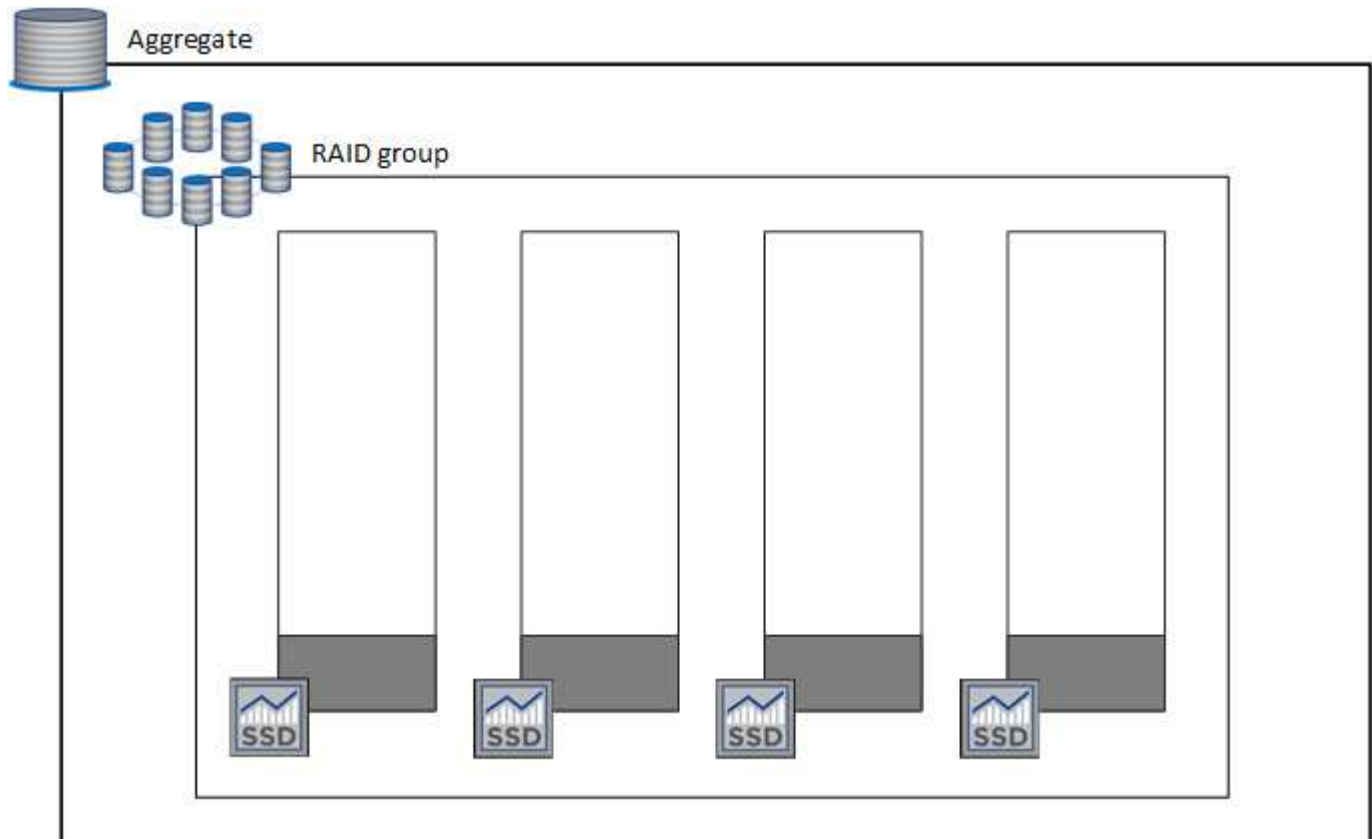
3.9.19 リリース以降、コンソール エージェントでは、Cloud Volumes ONTAPアグリゲートの Elastic Volumes 機能を有効にして管理するために次の権限が必要です。

- ec2:ボリュームの変更の説明
- ec2:ボリュームの変更

これらの権限は、"[NetAppが提供するポリシー](#)"

エラスティックボリュームのサポートの仕組み

エラスティック ボリューム機能が有効になっているアグリゲートは、1 つまたは 2 つの RAID グループで構成されます。各 RAID グループには、同じ容量を持つ 4 つの同一ディスクがあります。以下は、それぞれ 2.5 TiB のディスク 4 つを持つ 10 TiB アグリゲートの例です。



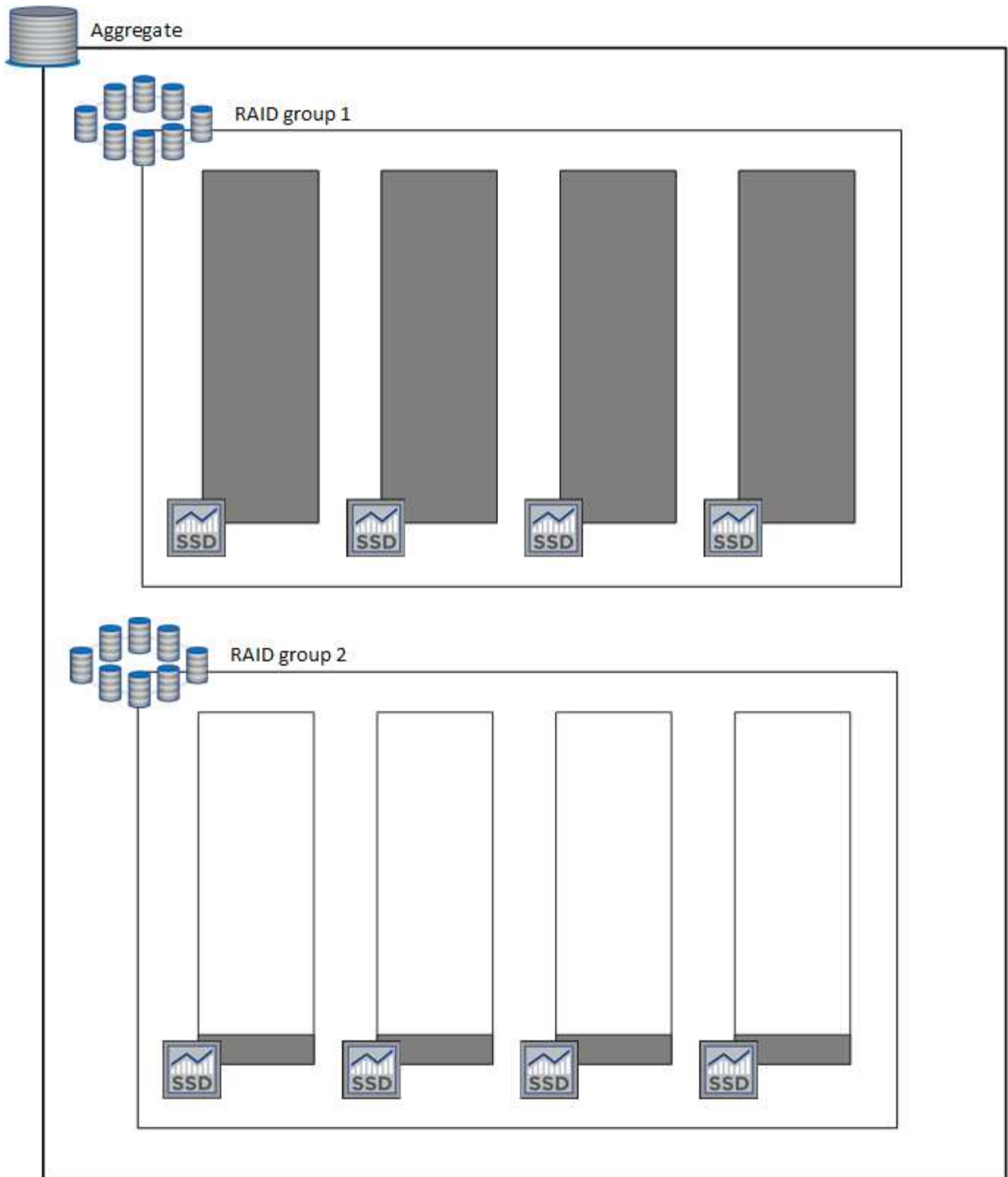
コンソールがアグリゲートを作成すると、1 つの RAID グループから開始されます。追加の容量が必要な場合は、RAID グループ内のすべてのディスクの容量を同じ量だけ増やすことによってアグリゲートを拡張します。容量の増加は、最小 256 GiB またはアグリゲートのサイズの 10% のいずれかになります。

たとえば、1 TiB のアグリゲートがある場合、各ディスクは 250 GiB になります。アグリゲートの容量の 10% は 100 GiB です。これは 256 GiB より小さいため、アグリゲートのサイズは最小の 256 GiB (またはディスクごとに 64 GiB) だけ増加されます。

コンソールは、Cloud Volumes ONTAPシステムの実行中、およびディスクがまだ接続されている間に、ディスクのサイズを増加します。変更は中断を伴いません。

アグリゲートが 64 TiB (または各ディスクで 16 TiB) に達すると、コンソールは追加容量用に 2 番目の RAID グループを作成します。この 2 番目の RAID グループは最初のグループと同じように動作します。つまり、まったく同じ容量を持つ 4 つのディスクがあり、最大 64 TiB まで拡張できます。つまり、アグリゲートの最大容量は 128 TiB になります。

以下は、2 つの RAID グループを持つアグリゲートの例です。最初の RAID グループでは容量制限に達していますが、2 番目の RAID グループのディスクには十分な空き領域があります。



ボリュームを作成すると何が起こるか

gp3 または io1 ディスクを使用するボリュームを作成する場合、コンソールは次のようにアグリゲート上にボリュームを作成します。

- エラスティック ボリュームが有効になっている既存の gp3 または io1 アグリゲートがある場合、コンソールはそのアグリゲート上にボリュームを作成します。

- エラスティック ボリュームが有効になっている gp3 または io1 アグリゲートが複数ある場合、コンソールは、必要なリソースが最も少ないアグリゲート上にボリュームを作成します。
- システムに、Elastic Volumes が有効になっていない gp3 または io1 アグリゲートのみがある場合は、そのアグリゲート上にボリュームが作成されます。

このシナリオは起こりそうにありませんが、次の 2 つの場合には起こり得ます。



- API からアグリゲートを作成するときに、Elastic Volumes 機能を明示的に無効にしました。
- ユーザー インターフェイスから新しいCloud Volumes ONTAPシステムを作成しましたが、この場合、初期アグリゲートで Elastic Volumes 機能が無効になっています。レビュー[\[制限事項\]](#)詳細については以下をご覧ください。

- 既存のアグリゲートに十分な容量がない場合、コンソールはエラスティック ボリュームを有効にしたアグリゲートを作成し、その新しいアグリゲート上にボリュームを作成します。

アグリゲートのサイズは、要求されたボリューム サイズに 10% の追加容量を加えたものに基づきます。

容量管理モード

コンソール エージェントの容量管理モードは、他の種類のアグリゲートと同様に、エラスティック ボリュームでも機能します。

- 自動モードが有効になっている場合 (これがデフォルトの設定です)、追加の容量が必要な場合、コンソールは自動的にアグリゲートのサイズを増やします。
- 容量管理モードを手動に変更すると、コンソールは追加容量の購入の承認を求めます。

["容量管理モードの詳細"](#)。

制限事項

集計のサイズを増やすには最大 6 時間かかる場合があります。その間、コンソールはそのアグリゲートに対して追加の容量を要求することはできません。

エラスティックボリュームの使い方

エラスティック ボリュームを使用して次のタスクを実行できます。

- gp3 または io1 ディスクを使用する場合は、初期アグリゲートでエラスティック ボリュームが有効になっている新しいシステムを作成します。

["Cloud Volumes ONTAPシステムの作成方法を学ぶ"](#)

- エラスティックボリュームが有効になっているアグリゲートに新しいボリュームを作成します

gp3 または io1 ディスクを使用するボリュームを作成すると、コンソールは、エラスティック ボリュームが有効になっているアグリゲート上にボリュームを自動的に作成します。詳細については、[\[ボリュームを作成すると何が起きるか\]](#)。

["ボリュームの作成方法を学ぶ"](#)。

- エラスティックボリュームを有効にした新しいアグリゲートを作成する

Cloud Volumes ONTAPシステムがバージョン 9.11.0 以降で作成されている限り、gp3 または io1 ディスクを使用する新しいアグリゲートでは Elastic Volumes が自動的に有効になります。

アグリゲートを作成すると、コンソールにアグリゲートの容量サイズの入力を求めるプロンプトが表示されます。これは、ディスク サイズとディスクの数を選択する他の構成とは異なります。

次のスクリーンショットは、gp3 ディスクで構成された新しいアグリゲートの例を示しています。

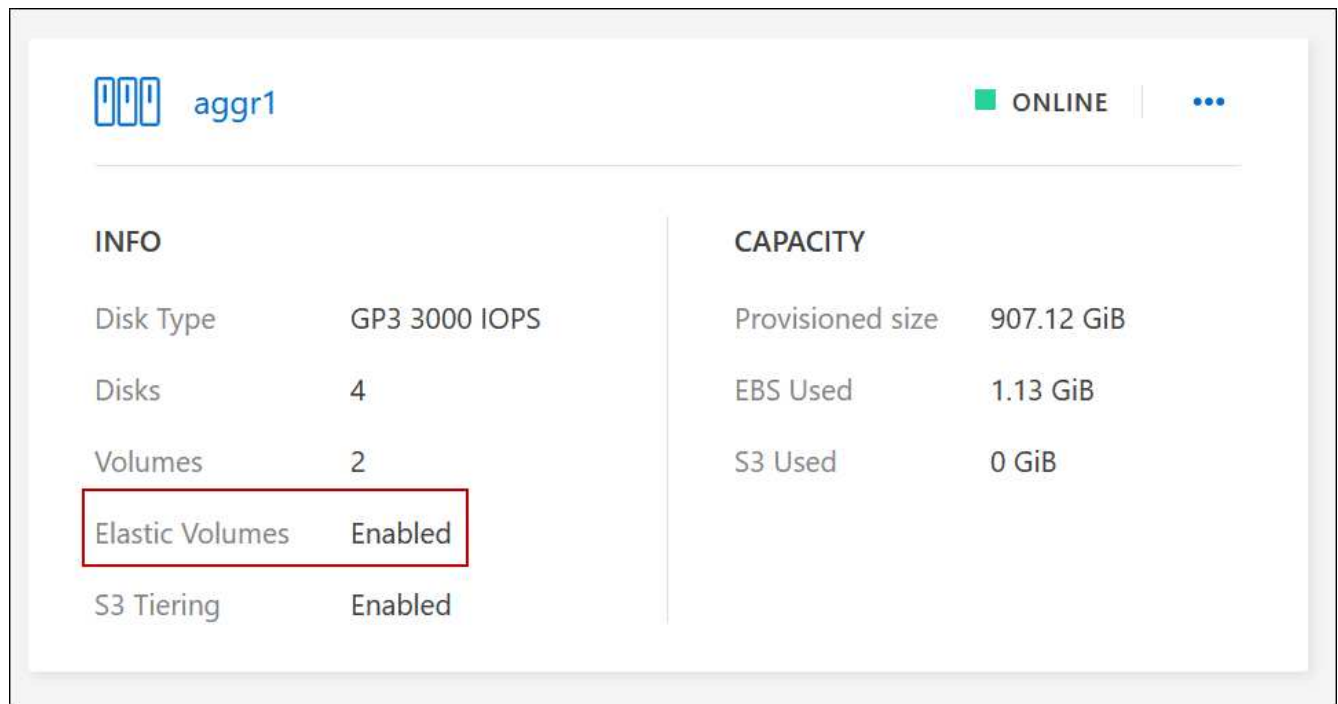
The screenshot displays the 'Select Disk Type' configuration page. At the top, a progress bar indicates the current step is '1 Disk Type', with subsequent steps being '2 Aggregate details', '3 Tiering Data', and '4 Review'. The main heading is 'Select Disk Type'. Below this, the 'Disk Type' dropdown menu is set to 'GP3 - General Purpose SSD Dynamic Performance'. A detailed box for 'General Purpose SSD (gp3) Disk Properties' is shown, containing the following information:

- Description:** General purpose SSD volume that balances price and performance (performance level is independent of storage capacity)
- IOPS Value:** 12000
- Throughput MB/s:** 250

"集計の作成方法を学ぶ"。

- エラスティックボリュームが有効になっているアグリゲートを識別する

「詳細割り当て」ページに移動すると、アグリゲートで Elastic Volumes 機能が有効になっているかどうかを確認できます。次の例では、aggr1 で Elastic Volumes が有効になっています。



- 集約に容量を追加する

コンソールは必要に応じて自動的にアグリゲートに容量を追加しますが、手動で容量を増やすこともできます。

["総容量を増やす方法を学ぶ"](#)。

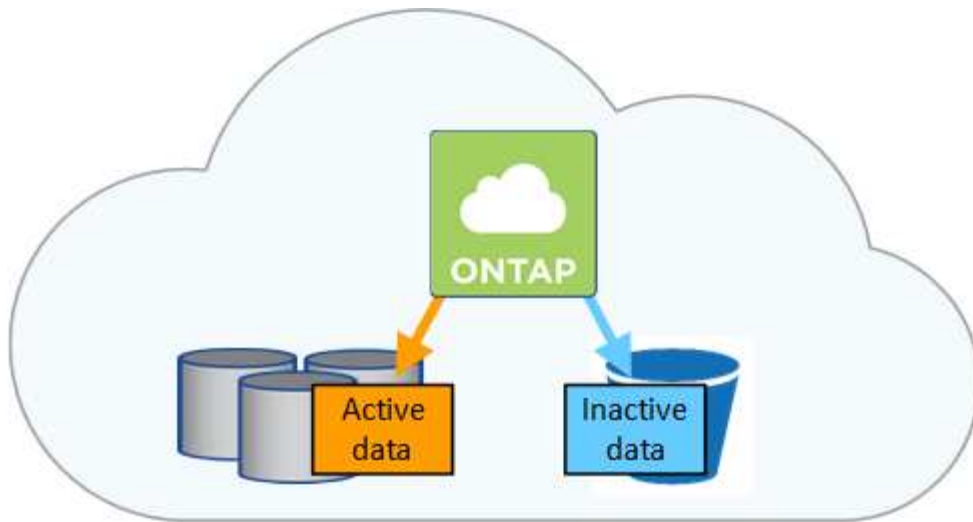
- エラスティックボリュームが有効になっているアグリゲートにデータを複製する

宛先のCloud Volumes ONTAPシステムが Elastic Volumes をサポートしている場合、宛先ボリュームは Elastic Volumes が有効になっているアグリゲートに配置されます (gp3 または io1 ディスクを選択した場合)。

["データレプリケーションの設定方法を学ぶ"](#)

AWS、Azure、Google Cloud でのCloud Volumes ONTAPによるデータ階層化について学習します

非アクティブなデータを低コストのオブジェクト ストレージに自動的に階層化することで、ストレージ コストを削減します。アクティブなデータは高性能の SSD または HDD に残り、非アクティブなデータは低コストのオブジェクト ストレージに階層化されます。これにより、プライマリ ストレージのスペースを再利用し、セカンダリ ストレージを縮小することができます。



データ階層化はFabricPoolテクノロジーによって実現されます。Cloud Volumes ONTAP は、追加のライセンスなしで、すべてのCloud Volumes ONTAPクラスターのデータ階層化を提供します。データ階層化を有効にすると、オブジェクト ストレージに階層化されたデータに対して料金が発生します。オブジェクト ストレージのコストの詳細については、クラウド プロバイダーのドキュメントを参照してください。

AWS におけるデータ階層化

AWS でデータ階層化を有効にすると、Cloud Volumes ONTAP はホットデータのパフォーマンス階層として EBS を使用し、非アクティブデータの容量階層として AWS S3 を使用します。

パフォーマンス層

パフォーマンス層は、汎用 SSD (gp3 または gp2) またはプロビジョニングされた IOPS SSD (io1) にすることができます。

スループット最適化 HDD (st1) を使用する場合、オブジェクト ストレージへのデータの階層化は推奨されません。

容量層

Cloud Volumes ONTAPシステムは、非アクティブなデータを単一の S3 バケットに階層化します。

NetAppコンソールは、システムごとに 1 つの S3 バケットを作成し、*fabric-pool-cluster unique identifier* という名前を付けます。ボリュームごとに異なる S3 バケットは作成されません。

コンソールが S3 バケットを作成するときは、次のデフォルト設定が使用されます。

- ストレージクラス: 標準
- デフォルトの暗号化: 無効
- パブリックアクセスをブロック: すべてのパブリックアクセスをブロック
- オブジェクトの所有権: ACL が有効
- バケットのバージョン管理: 無効
- オブジェクトロック: 無効

ストレージクラス

AWS の階層化データのデフォルトのストレージ クラスは *Standard* です。Standard は、複数のアベイラビリティゾーンに保存され、頻繁にアクセスされるデータに最適です。

非アクティブなデータにアクセスする予定がない場合は、ストレージ クラスを次のいずれかに変更することで、ストレージ コストを削減できます: *Intelligent Tiering*、*One-Zone Infrequent Access*、*Standard-Infrequent Access*、または *S3 Glacier Instant Retrieval*。ストレージ クラスを変更すると、非アクティブなデータは標準ストレージ クラスから開始され、30 日間アクセスされない場合、選択したストレージ クラスに移行します。

データにアクセスする場合はアクセス コストが高くなるため、ストレージ クラスを変更する前にこの点を考慮してください。"[Amazon S3 ドキュメント: Amazon S3 ストレージクラスの詳細](#)"。

システムを作成するときにストレージ クラスを選択でき、その後いつでも変更できます。ストレージクラスの変更手順については、"[非アクティブなデータを低コストのオブジェクトストレージに階層化](#)"。

データ階層化のストレージ クラスはシステム全体にわたっており、ボリュームごとではありません。

Azure のデータ階層化

Azure でデータ階層化を有効にすると、Cloud Volumes ONTAP は、ホット データのパフォーマンス層として Azure マネージド ディスクを使用し、非アクティブ データの容量層として Azure Blob ストレージを使用します。

パフォーマンス層

パフォーマンス層は SSD または HDD のいずれかになります。

容量層

Cloud Volumes ONTAPシステムは、非アクティブなデータを単一の BLOB コンテナに階層化します。

コンソールは、各Cloud Volumes ONTAPシステムのコンテナを含む新しいストレージ アカウントを作成します。ストレージ アカウントの名前はランダムです。ボリュームごとに異なるコンテナは作成されません。

コンソールは、次の設定でストレージ アカウントを作成します。

- アクセス層: ホット
- パフォーマンス: 標準
- 冗長性: Cloud Volume ONTAP の展開に準拠
 - 単一の可用性ゾーン: ローカル冗長ストレージ (LRS)
 - 複数の可用性ゾーン: ゾーン冗長ストレージ (ZRS)
- アカウント: StorageV2 (汎用 v2)
- REST API操作に安全な転送を要求する: 有効
- ストレージ アカウント キー アクセス: 有効
- 最小 TLS バージョン: バージョン 1.2
- インフラストラクチャ暗号化: 無効

ストレージアクセス層

Azure の階層化データの既定のストレージ アクセス層は、ホット 層です。ホット層は、容量層で頻繁にアクセスされるデータに最適です。

容量層の非アクティブなデータにアクセスする予定がない場合は、非アクティブなデータが最低 30 日間保持される「クール」ストレージ層を選択できます。非アクティブなデータが最低 90 日間保存される *cold* 層を選択することもできます。ストレージ要件とコストの考慮事項に基づいて、ニーズに最適な層を選択できます。ストレージ層を *cool* または *cold* に変更すると、非アクティブな容量層のデータはクールまたはコールド ストレージ層に直接移動されます。クール層とコールド層はホット層に比べてストレージ コストが低くなりますが、アクセス コストが高くなるため、ストレージ層を変更する前にその点を考慮してください。参照 ["Microsoft Azure ドキュメント: Azure Blob ストレージのアクセス層の詳細"](#)。

Cloud Volumes ONTAPシステムを追加するときにストレージ層を選択でき、その後いつでも変更できます。ストレージ階層の変更の詳細については、["非アクティブなデータを低コストのオブジェクトストレージに階層化"](#)。

データ階層化のストレージ アクセス層はシステム全体にわたっており、ボリュームごとではありません。

Google Cloud におけるデータ階層化

Google Cloud でデータ階層化を有効にすると、Cloud Volumes ONTAP は、ホット データのパフォーマンス階層として永続ディスクを使用し、非アクティブなデータの容量階層として Google Cloud Storage バケットを使用します。

パフォーマンス層

パフォーマンス レベルは、SSD 永続ディスク、バランス永続ディスク、標準永続ディスクのいずれかになります。

容量層

Cloud Volumes ONTAPシステムは、非アクティブなデータを単一の Google Cloud Storage バケットに階層化します。

コンソールは各システムのバケットを作成し、*fabric-pool-cluster unique identifier* という名前を付けます。ボリュームごとに異なるバケットは作成されません。

コンソールがバケットを作成するときは、次のデフォルト設定が使用されます。

- 場所の種類: 地域
- ストレージクラス: 標準
- パブリックアクセス: オブジェクト ACL の対象
- アクセス制御: きめ細かな
- 保護: なし
- データ暗号化: Google 管理の鍵

ストレージクラス

階層化データのデフォルトのストレージ クラスは、*Standard Storage* クラスです。データへのアクセス頻度が低い場合は、*Nearline Storage* または *Coldline Storage* に変更することでストレージ コストを削減できます。ストレージ クラスを変更すると、それ以降の非アクティブなデータは選択したクラスに直接移動されます。



ストレージ クラスを変更しても、既存の非アクティブなデータはデフォルトのストレージ クラスを維持します。既存の非アクティブ データのストレージ クラスを変更するには、指定を手動で実行する必要があります。

データにアクセスする場合はアクセス コストが高くなるため、ストレージ クラスを変更する前にその点を考慮してください。詳細については、"[Google Cloud ドキュメント: ストレージ クラス](#)"。

システムを作成するときにストレージ層を選択でき、その後いつでも変更できます。ストレージクラスの変更の詳細については、"[非アクティブなデータを低コストのオブジェクトストレージに階層化](#)"。

データ階層化のストレージ クラスはシステム全体にわたっており、ボリュームごとではありません。

データの階層化と容量制限

データ階層化を有効にすると、システムの容量制限は変わりません。制限はパフォーマンス層と容量層にまたがって適用されます。

ボリューム階層化ポリシー

データ階層化を有効にするには、ボリュームを作成、変更、または複製するときにボリューム階層化ポリシーを選択する必要があります。ボリュームごとに異なるポリシーを選択できます。

一部の階層化ポリシーには、最小冷却期間が関連付けられており、ボリューム内のユーザー データが「コールド」であるとみなされて容量階層に移動されるまでの非アクティブ状態を維持する必要がある時間を設定します。冷却期間は、データがアグリゲートに書き込まれたときに開始されます。



最小冷却期間とデフォルトの集計しきい値 50% を変更できます (詳細は後述)。"[冷却期間を変更する方法を学ぶ](#)"そして"[しきい値を変更する方法を学ぶ](#)"。

コンソールでは、ボリュームを作成または変更するときに、次のボリューム階層化ポリシーを選択できます。

Snapshot のみ

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

読み取られると、容量層のコールド データ ブロックがホットになり、パフォーマンス層に移動されます。

全て

すべてのデータ (メタデータを除く) は直ちにコールドとしてマークされ、できるだけ早くオブジェクト ストレージに階層化されます。ボリューム内の新しいブロックがコールドになるまで 48 時間待つ必要はありません。「すべて」ポリシーが設定される前にボリューム内に配置されていたブロックがコールド状態になるには 48 時間かかることに注意してください。

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

オート

アグリゲートの容量が 50% に達すると、Cloud Volumes ONTAPはボリューム内のコールド データ ブロックを容量層に階層化します。コールド データには、スナップショット コピーだけでなく、アクティブ ファイル システムからのコールド ユーザー データも含まれます。冷却期間は約31日間です。

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

ランダム読み取りによって読み取られると、キャパシティ層のコールド データ ブロックがホットになり、パフォーマンス層に移動します。インデックスやウイルス対策スキャンなどに関連する順次読み取りによって読み取られた場合、コールド データ ブロックはコールドのままとなり、パフォーマンス層に移動されません。

なし

ボリュームのデータをパフォーマンス層に保持し、容量層に移動されないようにします。

ボリュームを複製するときに、データをオブジェクト ストレージに階層化するかどうかを選択できます。そうすると、コンソールはデータ保護ボリュームに バックアップ ポリシーを適用します。Cloud Volumes ONTAP 9.6 以降では、バックアップ ポリシーが **All** 階層化ポリシーに置き換えられます。

Cloud Volumes ONTAPをオフにすると冷却期間に影響します

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

- 自動: 31日間
- スナップショットのみ: 2日間

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



Cloud Volumes ONTAP をオフにすると、システムを再起動するまで各ブロックの温度が保持されます。たとえば、システムをオフにしたときにブロックの温度が 5 だった場合、システムを再びオンにしたときも温度は 5 のままです。

データ階層化の設定

手順とサポートされている構成のリストについては、以下を参照してください。"[非アクティブなデータを低コストのオブジェクトストレージに階層化](#)"。

Cloud Volumes ONTAPストレージ管理

NetAppコンソールは、Cloud Volumes ONTAPストレージの簡素化された高度な管理を提供します。



すべてのディスクとアグリゲートはコンソールから直接作成および削除する必要があります。これらのアクションを別の管理ツールから実行しないでください。そうすると、システムの安定性に影響が及び、将来的にディスクを追加する能力が妨げられ、クラウド プロバイダーの料金が重複して発生する可能性があります。

ストレージのプロビジョニング

コンソールを使用すると、ディスクを購入し、アグリゲートを管理することで、Cloud Volumes ONTAPのストレージ プロビジョニングが簡単になります。ボリュームを作成するだけです。必要に応じて、高度な割り当てオプションを使用して、集約を自分でプロビジョニングすることもできます。

簡素化されたプロビジョニング

アグリゲートはボリュームにクラウド ストレージを提供します。インスタンスを起動するとき、および追加のボリュームをプロビジョニングするときに、コンソールによってアグリゲートが作成されます。

ボリュームを作成すると、コンソールは次の 3 つのうちのいずれかを実行します。

- 十分な空き領域がある既存のアグリゲートにボリュームを配置します。
- 既存のアグリゲート用にさらにディスクを購入して、そのアグリゲートにボリュームを配置します。

+ Elastic Volumes をサポートする AWS のアグリゲートの場合、RAID グループ内のディスクのサイズも増加します。["エラスティックボリュームのサポートについて詳しくはこちら"](#)。

- 新しいアグリゲート用のディスクを購入し、そのアグリゲートにボリュームを配置します。

コンソールは、アグリゲートの最大サイズ、シン プロビジョニングが有効かどうか、アグリゲートの空き領域のしきい値など、いくつかの要素を考慮して、新しいボリュームを配置する場所を決定します。

AWS のアグリゲートのディスクサイズを選択

コンソールは、AWS で Cloud Volumes ONTAP の新しいアグリゲートを作成すると、アグリゲート数が増加するにつれてディスク サイズを徐々に増やし、AWS データのディスク制限に達する前にシステム容量を最大化します。

たとえば、コンソールは次のディスク サイズを選択する場合があります。

合計数	ディスク サイズ	最大総容量
1	500ギガバイト	3 TiB
4	1 TiB	6 TiB
6	2 TiB	12 TiB



この動作は、Amazon EBS Elastic Volumes 機能をサポートするアグリゲートには適用されません。エラスティック ボリュームが有効になっているアグリゲートは、1 つまたは 2 つの RAID グループで構成されます。各 RAID グループには、同じ容量を持つ 4 つの同一ディスクがあります。["エラスティックボリュームのサポートについて詳しくはこちら"](#)。

高度な割り当てオプションを使用して、ディスク サイズを自分で選択できます。

高度な割り当て

集計を管理することもできます。["*高度な割り当て*ページから"](#)、特定の数のディスクを含む新しいアグリゲートを作成したり、既存のアグリゲートにディスクを追加したり、特定のアグリゲートにボリュームを作成したりできます。

容量管理

組織またはアカウント管理者は、ストレージ容量の決定を通知したり、容量要件を自動的に管理するかどうかをコンソールで設定できます。

この動作は、コンソール エージェントの 容量管理モード によって決まります。容量管理モードは、そのコン

ソール エージェントによって管理されるすべてのCloud Volumes ONTAPシステムに影響します。別のコンソール エージェントがある場合は、別の方法で構成できます。

自動容量管理

容量管理モードは、デフォルトで自動に設定されています。このモードでは、コンソールは 15 分ごとに空き領域比率をチェックし、空き領域比率が指定されたしきい値を下回っているかどうかを判断します。さらに容量が必要な場合は、新しいディスクの購入を開始し、使用されていないディスクのコレクション (アグリゲート) を削除し、必要に応じてアグリゲート間でボリュームを移動し、ディスク障害を防止します。

次の例は、このモードがどのように動作するかを示しています。

- アグリゲートが容量しきい値に達し、さらにディスクを追加する余裕がある場合、コンソールはボリュームが引き続き拡張できるように、そのアグリゲート用に新しいディスクを自動的に購入します。

Elastic Volumes をサポートする AWS のアグリゲートの場合、RAID グループ内のディスクのサイズも増加します。"[エラスティックボリュームのサポートについて詳しくはこちら](#)"。

+ * アグリゲートが容量しきい値に達し、追加のディスクをサポートできない場合、コンソールはボリュームをそのアグリゲートから使用可能な容量を持つアグリゲートまたは新しいアグリゲートに自動的に移動します。

+ コンソールがボリュームの新しいアグリゲートを作成する場合、そのボリュームのサイズに対応するディスク サイズが選択されます。

+ 元のアグリゲートで空き領域が利用可能になったことに注意してください。既存のボリュームまたは新しいボリュームがそのスペースを使用できます。このシナリオでは、スペースをクラウド プロバイダーに返却することはできません。

- アグリゲートにボリュームが 12 時間以上含まれていない場合、コンソールはそれを削除します。

自動容量管理によるLUNの管理

コンソールの自動容量管理は LUN には適用されません。LUN を作成すると、自動拡張機能が無効になります。

手動容量管理

組織またはアカウント管理者が容量管理モードを手動に設定した場合、コンソールは容量の決定に対して適切なアクションを実行するように通知します。自動モードで説明したのと同じ例が手動モードにも当てはまりますが、アクションを受け入れるかどうかはユーザー次第です。

詳細情報

"[容量管理モードを変更する方法を学ぶ](#)"。

書き込み速度

NetAppコンソールを使用すると、ほとんどのCloud Volumes ONTAP構成で通常または高速の書き込み速度を選択できます。書き込み速度を選択する前に、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。

通常の書き込み速度

通常の書き込み速度を選択すると、データはディスクに直接書き込まれます。データがディスクに直接書き込まれると、予期しないシステム停止や、予期しないシステム停止を伴う連鎖障害が発生した場合にデータが失われる可能性が軽減されます (HA ペアのみ)。

通常の書き込み速度がデフォルトのオプションです。

高速書き込み

高速書き込み速度を選択すると、データはディスクに書き込まれる前にメモリにバッファリングされるため、書き込みパフォーマンスが高速化されます。このキャッシュにより、予期しないシステム停止が発生した場合にデータが失われる可能性があります。

予期しないシステム停止が発生した場合に失われる可能性があるデータの量は、最後の 2 つの整合性ポイントの範囲です。整合性ポイントとは、バッファリングされたデータをディスクに書き込む行為です。整合性ポイントは、書き込みログがいっぱいになったとき、または 10 秒経過したとき (いずれか早い方) に発生します。ただし、クラウド プロバイダーが提供するストレージのパフォーマンスは、整合性ポイントの処理時間に影響する可能性があります。

高速書き込み速度を使用する場合

ワークロードに高速な書き込みパフォーマンスが必要であり、予期しないシステム停止や予期しないシステム停止を伴う連鎖障害が発生した場合にデータ損失のリスクに耐えられる場合は、高速書き込みが適切な選択肢となります (HA ペアのみ)。

高速書き込みを使用する場合の推奨事項

高速書き込みを有効にする場合は、アプリケーション層での書き込み保護を確保するか、データ損失が発生した場合でもアプリケーションがデータ損失を許容できるようにする必要があります。

AWS の HA ペアによる高速書き込み

AWS の HA ペアで高速書き込みを有効にする予定の場合は、複数のアベイラビリティゾーン (AZ) 展開と単一の AZ 展開間の保護レベルの違いを理解する必要があります。複数の AZ にわたって HA ペアを展開すると、回復力が高まり、データ損失の可能性を軽減できます。

["AWSのHAペアについて詳しくはこちら"](#)。

高速書き込みをサポートする構成

すべてのCloud Volumes ONTAP構成が高速書き込み速度をサポートしているわけではありません。これらの構成では、デフォルトで通常の書き込み速度が使用されます。

AWS

単一ノード システムを使用する場合、Cloud Volumes ONTAP はすべてのインスタンス タイプで高速書き込み速度をサポートします。

9.8 リリース以降、Cloud Volumes ONTAP は、m5.xlarge と r5.xlarge を除く、サポートされているほぼすべての EC2 インスタンス タイプを使用する場合、HA ペアによる高速書き込みをサポートします。

["Cloud Volumes ONTAPがサポートする Amazon EC2 インスタンスの詳細"](#)。

Azure

単一ノード システムを使用する場合、Cloud Volumes ONTAP はすべての VM タイプで高速書き込み速度をサポートします。

HA ペアを使用する場合、Cloud Volumes ONTAP は、9.8 リリース以降、いくつかの VM タイプで高速書き込み速度をサポートします。に行く ["Cloud Volumes ONTAP リリースノート"](#) 高速書き込みをサポートする VM タイプを表示します。

Google Cloud

単一ノード システムを使用する場合、Cloud Volumes ONTAP はすべてのマシン タイプで高速書き込み速度をサポートします。

HA ペアを使用する場合、Cloud Volumes ONTAP は、9.13.0 リリース以降、いくつかの VM タイプで高速書き込み速度をサポートします。に行く ["Cloud Volumes ONTAP リリースノート"](#) 高速書き込みをサポートする VM タイプを表示します。

["Cloud Volumes ONTAP がサポートする Google Cloud マシンタイプの詳細"](#)。

書き込み速度の選択方法

新しい Cloud Volumes ONTAP システムを追加するときに書き込み速度を選択できます。["既存システムの書き込み速度を変更する"](#)。

データ損失が発生した場合に予想されること

書き込み速度が速いためにデータ損失が発生した場合、イベント管理システム (EMS) は次の 2 つのイベントを報告します。

- Cloud Volumes ONTAP 9.12.1 以降

```
NOTICE nv.data.loss.possible: An unexpected shutdown occurred while in
high write speed mode, which possibly caused a loss of data.
* Cloud Volumes ONTAP 9.11.0 から 9.11.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due
to dirty shutdown with High Write Speed mode"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might
have changed. Verify that all recent configuration changes are still in
effect..
* Cloud Volumes ONTAP 9.8 から 9.10.1
```

```
DEBUG nv.check.failed: NVRAM check failed with error "NVRAM disabled due to dirty shutdown"
```

```
ERROR wafl.root.content.changed: Contents of the root volume '' might have changed. Verify that all recent configuration changes are still in effect.
```

このような状況が発生すると、Cloud Volumes ONTAP はユーザーの介入なしに起動し、データの提供を継続できるようになります。

データ損失が発生した場合にデータアクセスを停止する方法

データ損失が懸念される場合、データ損失時にアプリケーションの実行を停止し、データ損失の問題が適切に解決された後にデータ アクセスを再開するには、CLI から NVFAIL オプションを使用してその目的を達成できます。

NVFAILオプションを有効にするには

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

NVFAIL設定を確認するには

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

NVFAILオプションを無効にするには

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

データ損失が発生すると、NVFAIL が有効になっている NFS または iSCSI ボリュームはデータの提供を停止します (ステートレス プロトコルである CIFS には影響はありません)。詳細については、["NFSボリュームまたはLUNへのアクセスに対するNVFAILの影響"](#)。

NVFAIL状態を確認するには

```
vol show -fields in-nvfailed-state
```

データ損失の問題が適切に解決されたら、NVFAIL 状態をクリアしてボリュームにデータ アクセスできるようになります。

NVFAIL状態をクリアするには

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

Flash Cache

一部のCloud Volumes ONTAP構成にはローカル NVMe ストレージが含まれており、Cloud Volumes ONTAP はこれを フラッシュ キャッシュ として使用してパフォーマンスを向上させます。

フラッシュキャッシュとは何ですか？

Flash Cache は、最近読み取られたユーザー データとNetAppメタデータをリアルタイムでインテリジェントにキャッシュすることで、データへのアクセスを高速化します。これは、データベース、電子メール、ファイル サービスなどのランダム読み取り集中型のワークロードに効果的です。

サポートされている構成

Flash Cache は、特定のCloud Volumes ONTAP構成でサポートされます。サポートされている構成については、"[Cloud Volumes ONTAPリリースノート](#)"

制限事項

- AWS でCloud Volumes ONTAP 9.12.0 以前の Flash Cache を構成する場合、Flash Cache のパフォーマンス向上を活用するには、すべてのボリュームで圧縮を無効にする必要があります。Cloud Volumes ONTAP 9.12.1 以降をデプロイまたはアップグレードする場合は、圧縮を無効にする必要はありません。

NetAppコンソールからボリュームを作成するときにストレージ効率設定の選択をスキップするか、ボリュームを作成してから "[CLIを使用してデータ圧縮を無効にする](#)"。

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

Cloud Volumes ONTAPの WORM ストレージについて学ぶ

Cloud Volumes ONTAPシステムでWrite Once Read Many (WORM) ストレージをアクティブ化すると、指定した保持期間中、変更されない状態でファイルを保管できます。Cloud WORMストレージはSnapLockテクノロジーを使用しているため、WORMファイルはファイル レベルで保護されます。

WORM 機能は、BYOL (お客様独自のライセンスの持ち込み) およびライセンスのマーケットプレイス サブスクリプションで追加料金なしで使用できます。現在のライセンスに WORM を追加するには、NetApp の営業担当者にお問い合わせください。

WORMストレージの仕組み

ファイルが WORM ストレージに保存されると、保持期間が経過しても変更することはできません。WORM ファイルの保持期間が経過したかどうかは、改ざん防止クロックによって判断されます。

保存期間が経過した後は、不要になったファイルを削除する責任はお客様にあります。

WORMストレージの有効化

WORM ストレージをアクティブ化する方法、それは使用しているCloud Volumes ONTAP のバージョンによって異なります。

バージョン**9.10.1**以降

Cloud Volumes ONTAP 9.10.1 以降では、ボリューム レベルで WORM を有効または無効にするオプションがあります。

Cloud Volumes ONTAPシステムを追加すると、WORM ストレージを有効または無効にするように求められます。

- システムを追加するときに WORM ストレージを有効にすると、NetAppコンソールから作成するすべてのボリュームで WORM が有効になります。ただし、ONTAP System Manager またはONTAP CLI を使用して、WORM が無効になっているボリュームを作成することはできません。
- システムを追加するときに WORM ストレージを無効にすると、コンソール、ONTAP System Manager、またはONTAP CLI から作成するすべてのボリュームで WORM が無効になります。

バージョン **9.10.0** 以前

新しいシステムを追加するときに、Cloud Volumes ONTAPシステムで WORM ストレージをアクティブ化できます。コンソールから作成するすべてのボリュームでは WORM が有効になっています。個々のボリュームで WORM ストレージを無効にすることはできません。

ファイルの**WORM**状態へのコミット

アプリケーションを使用して NFS または CIFS 経由でファイルを WORM にコミットすることも、ONTAP CLI を使用してファイルを自動的に WORM にコミットすることもできます。また、ログ情報のように増分的に書き込まれるデータを保持するために、WORM 追加可能ファイルを使用することもできます。

Cloud Volumes ONTAPシステムで WORM ストレージをアクティブ化した後は、WORM ストレージのすべての管理にONTAP CLI を使用する必要があります。手順については、"[SnapLockに関するONTAPドキュメント](#)"。

Cloud Volumes ONTAPシステムで **WORM** を有効にする

コンソールでCloud Volumes ONTAPシステムを作成するときに、WORM ストレージを有効にできます。作成時にシステムで WORM が有効になっていない場合でも、システムで WORM を有効にできます。有効にした後は、WORM を無効にすることはできません。

タスク概要

- WORM はONTAP 9.10.1 以降でサポートされています。
- バックアップ付き WORM は、ONTAP 9.11.1 以降でサポートされています。

手順

1. システム ページで、WORM を有効にするシステムの名前をダブルクリックします。
2. [概要] タブで [機能] パネルをクリックし、[WORM] の横にある鉛筆アイコンをクリックします。

システムで WORM がすでに有効になっている場合、鉛筆アイコンは無効になります。

3. **WORM** ページで、クラスターのコンプライアンス クロックの保持期間を設定します。

詳細については、"[ONTAPドキュメント: コンプライアンスクロックの初期化](#)"。

4. *設定*をクリックします。

終了後の操作

WORM のステータスは機能パネルで確認できます。WORM を有効にすると、SnapLockライセンスがクラスターに自動的にインストールされます。SnapLockライセンスはONTAP System Manager で確認できます。

WORMファイルの削除

特権削除機能を使用して、保持期間中に WORM ファイルを削除できます。

手順については、["ONTAPのドキュメント"](#)。

WORMとデータ階層化

新しいCloud Volumes ONTAP 9.8 以降のシステムを作成するときに、データ階層化と WORM ストレージの両方を一緒に有効にすることができます。WORM ストレージによるデータ階層化を有効にすると、クラウド内のオブジェクトストアにデータを階層化できます。

データ階層化と WORM ストレージの両方を有効にする場合、次の点を理解する必要があります。

- オブジェクトストレージに階層化されたデータには、ONTAP WORM 機能は含まれません。エンドツーエンドの WORM 機能を確認するには、バケットの権限を正しく設定する必要があります。
- オブジェクトストレージに階層化されたデータには WORM 機能がないため、技術的にはバケットとコンテナへのフルアクセス権を持つユーザーであれば誰でも、ONTAPによって階層化されたオブジェクトを削除できます。
- 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。

制限事項

- Cloud Volumes ONTAPの WORM ストレージは、「信頼できるストレージ管理者」モデルに基づいて動作します。WORM ファイルは変更や修正から保護されていますが、ボリュームに有効期限内の WORM データが含まれている場合でも、クラスター管理者によってボリュームが削除される可能性があります。
- 信頼できるストレージ管理者モデルに加えて、Cloud Volumes ONTAPの WORM ストレージも暗黙的に「信頼できるクラウド管理者」モデルの下で動作します。クラウド管理者は、クラウドプロバイダーから直接クラウドストレージを削除または編集することで、有効期限前に WORM データを削除できます。

関連リンク

- ["WORMストレージ用の改ざん防止スナップショットコピーを作成する"](#)

ハイアベイラビリティ ペア

AWS のCloud Volumes ONTAP HA ペアについて学ぶ

Cloud Volumes ONTAP の高可用性 (HA) 構成は、中断のない運用とフォールトトレランスを実現します。AWS では、データは 2 つのノード間で同期的にミラーリングされます。

HA コンポーネント

AWS では、Cloud Volumes ONTAP HA 構成には次のコンポーネントが含まれます。

- データが相互に同期してミラーリングされる 2 つのCloud Volumes ONTAPノード。
- ストレージの引き継ぎとギブバックのプロセスを支援するためにノード間の通信チャンネルを提供するメディアエーター インスタンス。

メディエーター

AWS のメディエーターインスタンスに関する重要な詳細は次のとおりです。

インスタンスタイプ

t3-マイクロ

ディスク

8 GiB と 4 GiB の 2 つの st1 ディスク

オペレーティング システム

Debian 11



Cloud Volumes ONTAP 9.10.0 以前では、Debian 10 がメディエーターにインストールされていました。

アップグレード

Cloud Volumes ONTAPをアップグレードすると、NetAppコンソールは必要に応じてメディエーター インスタンスも更新します。

インスタンスへのアクセス

コンソールからCloud Volumes ONTAP HA ペアを作成すると、メディエーター インスタンスのキー ペアを指定するように求められます。このキーペアはSSHアクセスに使用できます。`admin`ユーザー。

サードパーティエージェント

サードパーティ エージェントまたは VM 拡張機能は、メディエーター インスタンスではサポートされません。

ストレージの引き継ぎと返却

1 つのノードがダウンした場合、他のノードがパートナーにデータを提供して、継続的なデータ サービスを提供します。データはパートナーに同期的にミラーリングされているため、クライアントはパートナー ノードから同じデータにアクセスできます。

ノードが再起動した後、パートナーはストレージを返す前にデータを再同期する必要があります。データの再同期にかかる時間は、ノードがダウンしている間に変更されたデータの量によって異なります。

ストレージのテイクオーバー、再同期、ギブバックはすべてデフォルトで自動で行われます。ユーザーの操作は必要ありません。

RPOおよびRTO

HA 構成では、次のようにデータの高可用性が維持されます。

- Recovery Point Objective (RPO;目標復旧時点) は0秒です。データはトランザクションの整合性が確保されており、データ損失はありません。
- Recovery Time Objective (RTO;目標復旧時間) は120秒です。障害が発生した場合、データは120秒以内に使用可能になります。

HA展開モデル

複数のアベイラビリティゾーン (AZ) 全体または単一のアベイラビリティゾーン (AZ) に HA 構成を展開することで、データの高可用性を確保できます。それぞれの構成の詳細を確認して、ニーズに最適なものを選択してください。

複数のアベイラビリティゾーン

複数のアベイラビリティゾーン (AZ) に HA 構成を展開すると、AZ または Cloud Volumes ONTAP ノードを実行するインスタンスで障害が発生した場合でも、データの高可用性が保証されます。NAS IP アドレスがデータ アクセスとストレージ フェイルオーバーにどのような影響を与えるかを理解する必要があります。

NFS および CIFS データ アクセス

HA 構成が複数のアベイラビリティゾーンに分散されている場合、フローティング IP アドレス によって NAS クライアント アクセスが可能になります。フローティング IP アドレスは、リージョン内のすべての VPC の CIDR ブロックの外側にある必要があり、障害が発生するとノード間で移行できます。VPC 外のクライアントからはネイティブにアクセスできません。["AWS トランジットゲートウェイを設定する"](#)。

トランジットゲートウェイを設定できない場合は、VPC 外の NAS クライアントでプライベート IP アドレスを使用できます。ただし、これらの IP アドレスは静的であり、ノード間でフェイルオーバーすることはできません。

複数のアベイラビリティゾーンにわたって HA 構成を展開する前に、フローティング IP アドレスとルートテーブルの要件を確認する必要があります。構成を展開するときに、フローティング IP アドレスを指定する必要があります。プライベート IP アドレスは自動的に作成されます。

詳細については、["複数の AZ における Cloud Volumes ONTAP HA の AWS ネットワーク要件"](#)。

iSCSI データ アクセス

iSCSI はフローティング IP アドレスを使用しないため、VPC 間のデータ通信は問題になりません。

iSCSI のテイクオーバーとギブバック

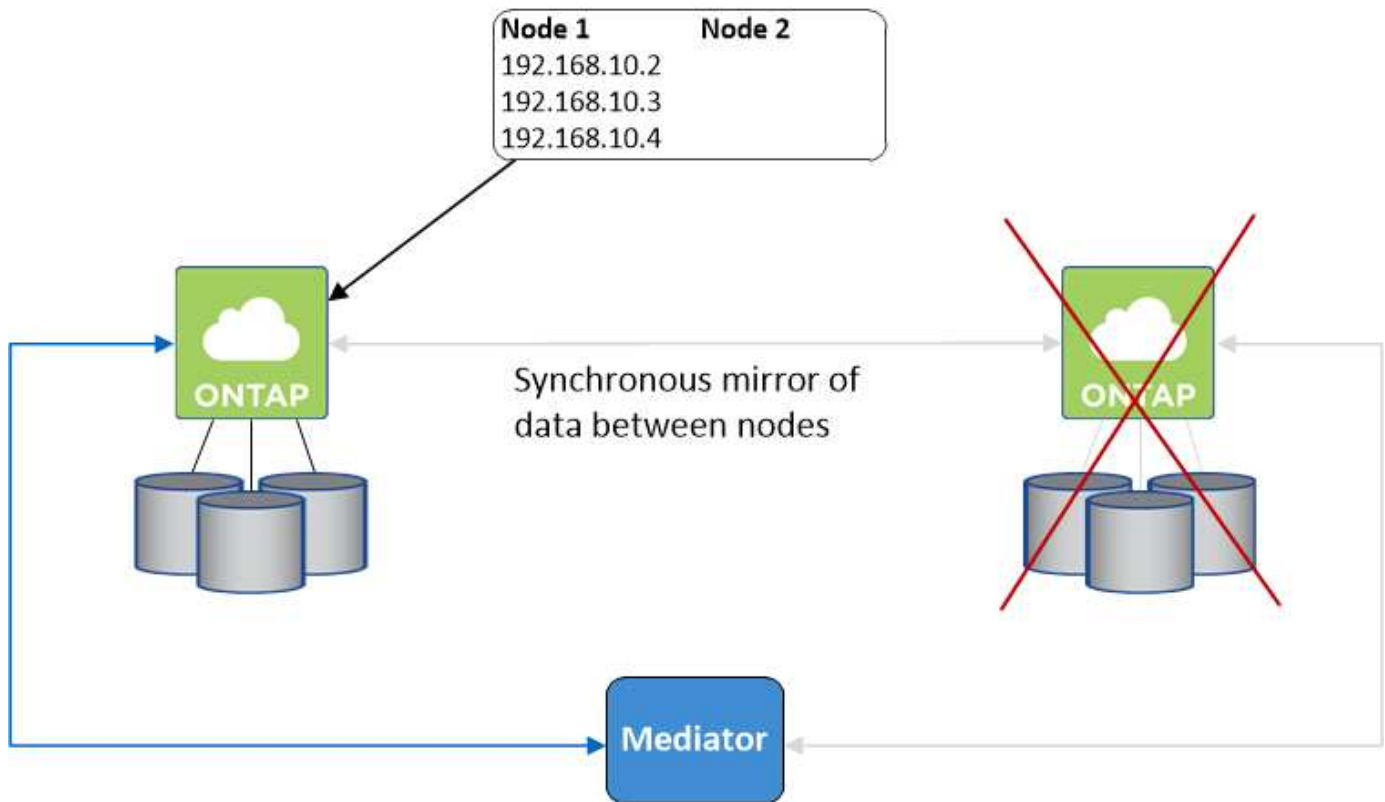
iSCSI の場合、Cloud Volumes ONTAP はマルチパス I/O (MPIO) と非対称論理ユニット アクセス (ALUA) を使用して、アクティブに最適化されたパスと最適化されていないパス間のパス フェイルオーバーを管理します。



ALUA をサポートする特定のホスト構成については、["NetApp Interoperability Matrix Tool"](#) そして ["SAN ホストとクラウドクライアントガイド"](#) ホスト オペレーティング システム用。

NAS の買収と返還

フローティング IP を使用する NAS 構成でテイクオーバーが発生すると、クライアントがデータにアクセスするために使用するノードのフローティング IP アドレスが他のノードに移動します。次の図は、フローティング IP を使用した NAS 構成でのストレージのテイクオーバーを示しています。ノード 2 がダウンした場合、ノード 2 のフローティング IP アドレスはノード 1 に移動します。



障害が発生した場合、外部 VPC アクセスに使用される NAS データ IP はノード間で移行できません。ノードがオフラインになった場合は、他のノードの IP アドレスを使用して、VPC 外部のクライアントにボリュームを手動で再マウントする必要があります。

障害が発生したノードがオンラインに戻ったら、元の IP アドレスを使用してクライアントをボリュームに再マウントします。この手順は、パフォーマンスと安定性に重大な影響を与える可能性のある、2 つの HA ノード間での不要なデータの転送を回避するために必要です。

ボリュームを選択し、*マウント コマンド*をクリックすると、コンソールから正しい IP アドレスを見つけることができます。

単一のアベイラビリティゾーン

単一のアベイラビリティゾーン (AZ) に HA 構成を展開すると、Cloud Volumes ONTAP ノードを実行するインスタンスに障害が発生した場合でも、データの高可用性を確保できます。すべてのデータは VPC の外部からネイティブにアクセスできます。

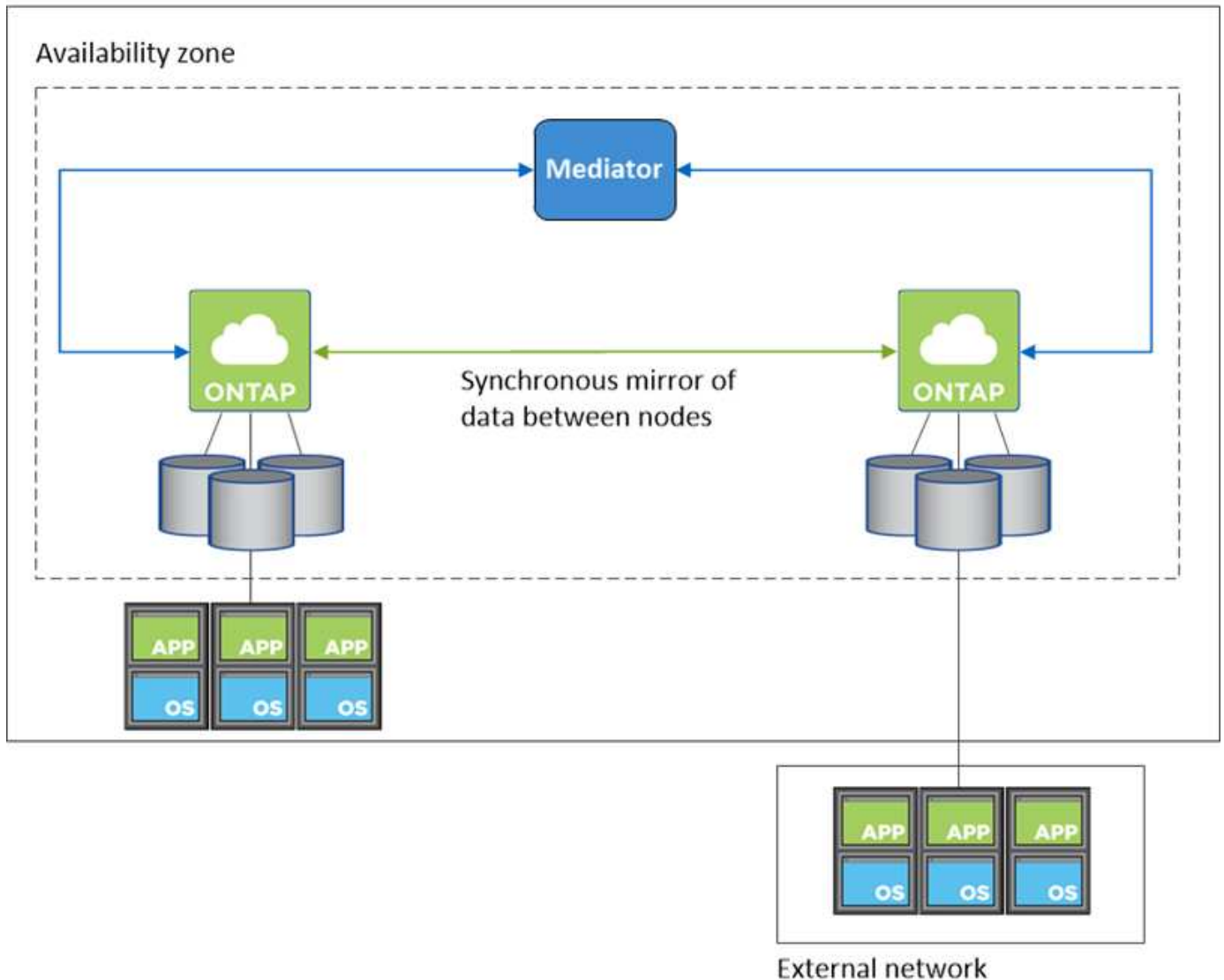


コンソールは ["AWS ドキュメント: AWS スプレッド配置グループ"](#) として、その配置グループ内の 2 つの HA ノードを起動します。配置グループは、インスタンスを異なる基盤ハードウェアに分散させることで、同時障害のリスクを軽減します。この機能は、ディスク障害の観点ではなく、コンピューティングの観点から冗長性を向上させます。

データ アクセス

この構成は単一のアベイラビリティゾーン (AZ) 内にあるため、フローティング IP アドレスは必要ありません。VPC 内からのデータアクセスと VPC 外からのデータアクセスに同じ IP アドレスを使用できます。

次の図は、単一のアベイラビリティゾーン (AZ) での HA 構成を示しています。データは VPC 内からも VPC 外からもアクセスできます。



買収と返還

iSCSI の場合、Cloud Volumes ONTAP はマルチパス I/O (MPIO) と非対称論理ユニット アクセス (ALUA) を使用して、アクティブに最適化されたパスと最適化されていないパス間のパス フェイルオーバーを管理します。



ALUAをサポートする特定のホスト構成については、"[NetApp Interoperability Matrix Tool](#)"そして"[SANホストとクラウドクライアントガイド](#)"ホスト オペレーティング システム用。

NAS 構成の場合、障害が発生した場合、データ IP アドレスは HA ノード間で移行できます。これにより、クライアントのストレージへのアクセスが保証されます。

AWS ローカルゾーン

AWS ローカルゾーンは、ストレージ、コンピューティング、データベース、およびその他の厳選された AWS サービスが大都市や産業地域の近くに配置されているインフラストラクチャ展開です。AWS Local Zones を使用すると、AWS のサービスをお客様の近くに配置できるため、ワークロードのレイテンシーが改善され、データベースがローカルで維持されます。Cloud Volumes ONTAPでは、

AWS ローカルゾーンに単一の AZ または複数の AZ 構成をデプロイできます。



コンソールを標準モードおよびプライベートモードで使用する場合、AWS ローカルゾーンがサポートされます。現時点では、AWS ローカルゾーンは制限モードではサポートされていません。

AWS ローカルゾーンの設定例

AWS のCloud Volumes ONTAPは、単一のアベイラビリティゾーンで高可用性 (HA) モードのみをサポートします。単一ノードの展開はサポートされていません。

Cloud Volumes ONTAP は、AWS ローカルゾーンのデータ階層化、クラウド階層化、および非適格インスタンスをサポートしていません。

以下に構成例を示します。

- 単一の可用性ゾーン: クラスター ノードとメディアエーターは両方とも同じローカル ゾーンにあります。
- 複数の可用性ゾーン 複数の可用性ゾーン構成では、3 つのインスタンス、2 つのノード、および 1 つのメディアエーターが存在します。3 つのインスタンスのうち 1 つは別のゾーンに存在する必要があります。どのように設定するか選択できます。

以下に 3 つの構成例を示します。

- 各クラスター ノードは異なるローカル ゾーンにあり、メディアエーターはパブリック アベイラビリティ ゾーンにあります。
- 1 つのクラスター ノードはローカル ゾーンにあり、メディアエーターはローカル ゾーンにあり、2 番目のクラスター ノードはアベイラビリティ ゾーンにあります。
- 各クラスター ノードとメディアエーターは別々のローカル ゾーンにあります。

サポートされているディスクとインスタンスタイプ

サポートされているディスク タイプは GP2 のみです。現在、xlarge から 4xlarge までのサイズの次の EC2 インスタンス タイプ ファミリがサポートされています。

- M5
- C5
- C5d
- R5
- R5d



Cloud Volumes ONTAP はこれらの構成のみをサポートします。AWS ローカルゾーン構成でサポートされていないディスクタイプまたは不適格なインスタンスを選択すると、デプロイメントが失敗する可能性があります。接続性がないため、AWS S3 へのデータ階層化はAWS ローカルゾーンでは利用できません。

["AWS ドキュメント: ローカルゾーンの EC2 インスタンスタイプ"](#)。

HAペアにおけるストレージの仕組み

ONTAPクラスターとは異なり、Cloud Volumes ONTAP HA ペアのストレージはノード間で共有されません。代わりに、データはノード間で同期的にミラーリングされるため、障害発生時にもデータを利用できます。

ストレージ割り当て

新しいボリュームを作成し、追加のディスクが必要になった場合、コンソールは両方のノードに同じ数のディスクを割り当て、ミラー化されたアグリゲートを作成してから、新しいボリュームを作成します。たとえば、ボリュームに2つのディスクが必要な場合、コンソールはノードごとに2つのディスクを割り当て、合計4つのディスクを割り当てます。

ストレージ構成

HA ペアは、両方のノードがクライアントにデータを提供するアクティブ/アクティブ構成として使用することも、アクティブ ノードのストレージを引き継いだ場合にのみパッシブ ノードがデータ要求に応答するアクティブ/パッシブ構成として使用することもできます。



アクティブ/アクティブ構成を設定できるのは、ストレージ システム ビューのコンソールを使用する場合のみです。

パフォーマンスの期待

Cloud Volumes ONTAP HA 構成では、ノード間でデータが同期的に複製されるため、ネットワーク帯域幅が消費されます。その結果、単一ノードのCloud Volumes ONTAP構成と比較して、次のパフォーマンスが期待できます。

- 1つのノードからのみデータを提供する HA 構成の場合、読み取りパフォーマンスは単一ノード構成の読み取りパフォーマンスに匹敵しますが、書き込みパフォーマンスは低くなります。
- 両方のノードからデータを提供する HA 構成の場合、読み取りパフォーマンスは単一ノード構成の読み取りパフォーマンスよりも高く、書き込みパフォーマンスは同じかそれ以上になります。

Cloud Volumes ONTAPのパフォーマンスの詳細については、以下を参照してください。"[パフォーマンス](#)"。

ストレージへのクライアントアクセス

クライアントは、ボリュームが存在するノードのデータ IP アドレスを使用して NFS および CIFS ボリュームにアクセスする必要があります。NAS クライアントがパートナー ノードの IP アドレスを使用してボリュームにアクセスすると、トラフィックが両方のノード間で行われ、パフォーマンスが低下します。



HA ペアのノード間でボリュームを移動する場合は、他のノードの IP アドレスを使用してボリュームを再マウントする必要があります。そうしないと、パフォーマンスが低下する可能性があります。クライアントが NFSv4 参照または CIFS のフォルダー リダイレクトをサポートしている場合は、Cloud Volumes ONTAPシステムでこれらの機能を有効にして、ボリュームの再マウントを回避できます。詳細については、ONTAP のドキュメントを参照してください。

ボリューム管理パネルの下にある マウント コマンド オプションを使用して、正しい IP アドレスを簡単に識別できます。

Volume Actions

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

Protection Actions

Advanced Actions

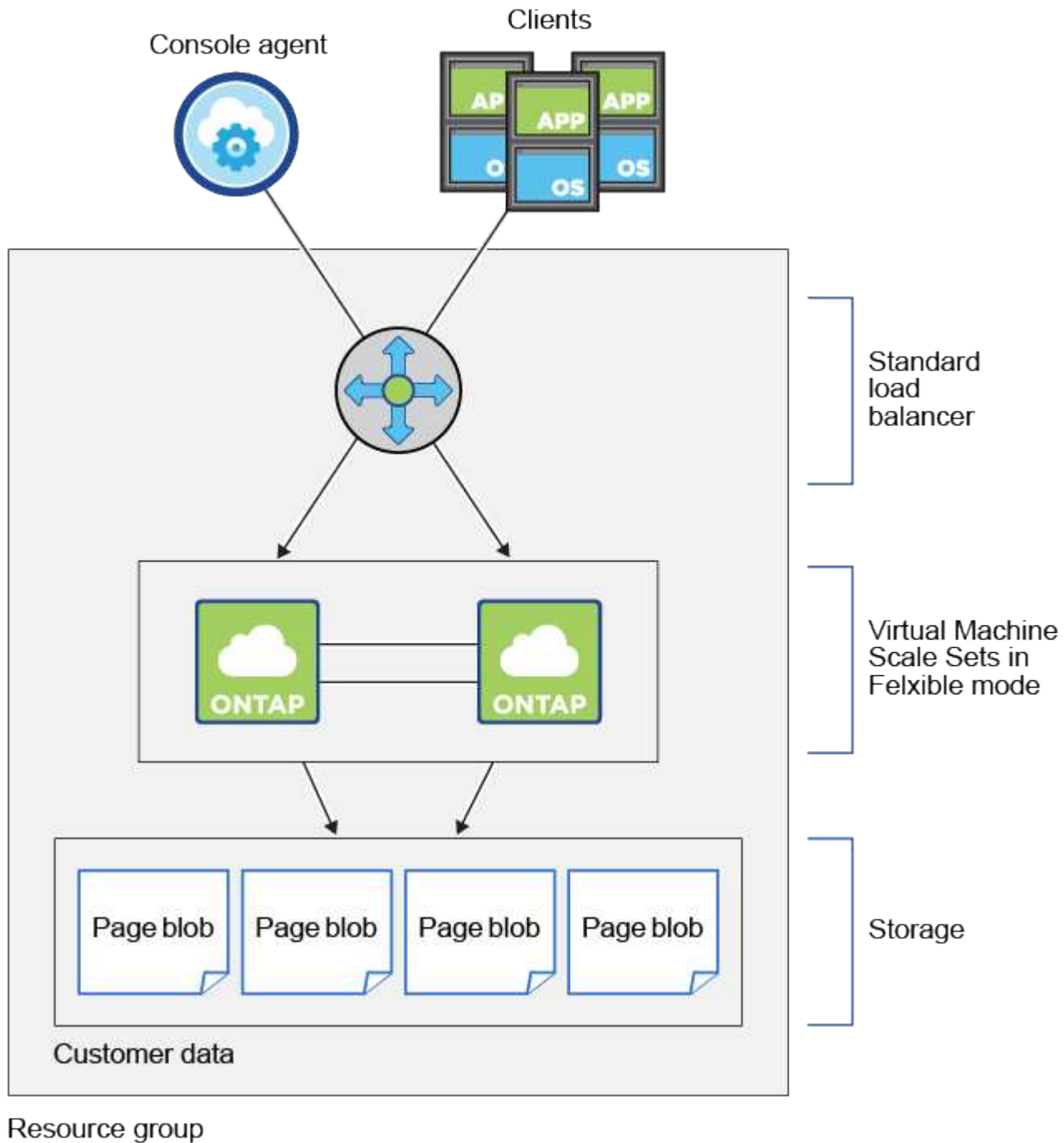
Azure のCloud Volumes ONTAP HA ペアについて学ぶ

Cloud Volumes ONTAP の高可用性 (HA) ペアは、クラウド環境で障害が発生した場合でも、エンタープライズの信頼性と継続的な運用を実現します。Azure では、ストレージは 2 つのノード間で共有されます。

HA コンポーネント

ページ BLOB を使用した HA 単一アベイラビリティゾーン構成

Azure のCloud Volumes ONTAP HA ページ BLOB 構成には、次のコンポーネントが含まれます。



NetAppコンソールによって展開される Azure コンポーネントについては、次の点に注意してください。

Azure 標準ロードバランサー

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

単一のアベイラビリティゾーン内のVM

Cloud Volumes ONTAP 9.15.1 以降では、単一のアベイラビリティゾーン (AZ) で異機種仮想マシン (VM) を作成および管理できます。同じ AZ 内の別々の障害ドメインに高可用性 (HA) ノードを展開して、最適な

可用性を保証できます。この機能を可能にする柔軟なオーケストレーションモードの詳細については、["Microsoft Azure ドキュメント: 仮想マシン スケール セット"](#)。

ディスク

顧客データは Premium Storage ページ BLOB に保存されます。各ノードは他のノードのストレージにアクセスできます。追加のストレージも必要です"[ブート、ルート、コアデータ](#)"。

ストレージアカウント

- マネージド ディスクには 1 つのストレージ アカウントが必要です。
- ストレージ アカウントあたりのディスク容量制限に達したため、Premium Storage ページ BLOB には 1 つ以上のストレージ アカウントが必要です。

["Microsoft Azure ドキュメント: Azure Storage のスケーラビリティとストレージ アカウントのパフォーマンス ターゲット"](#)。

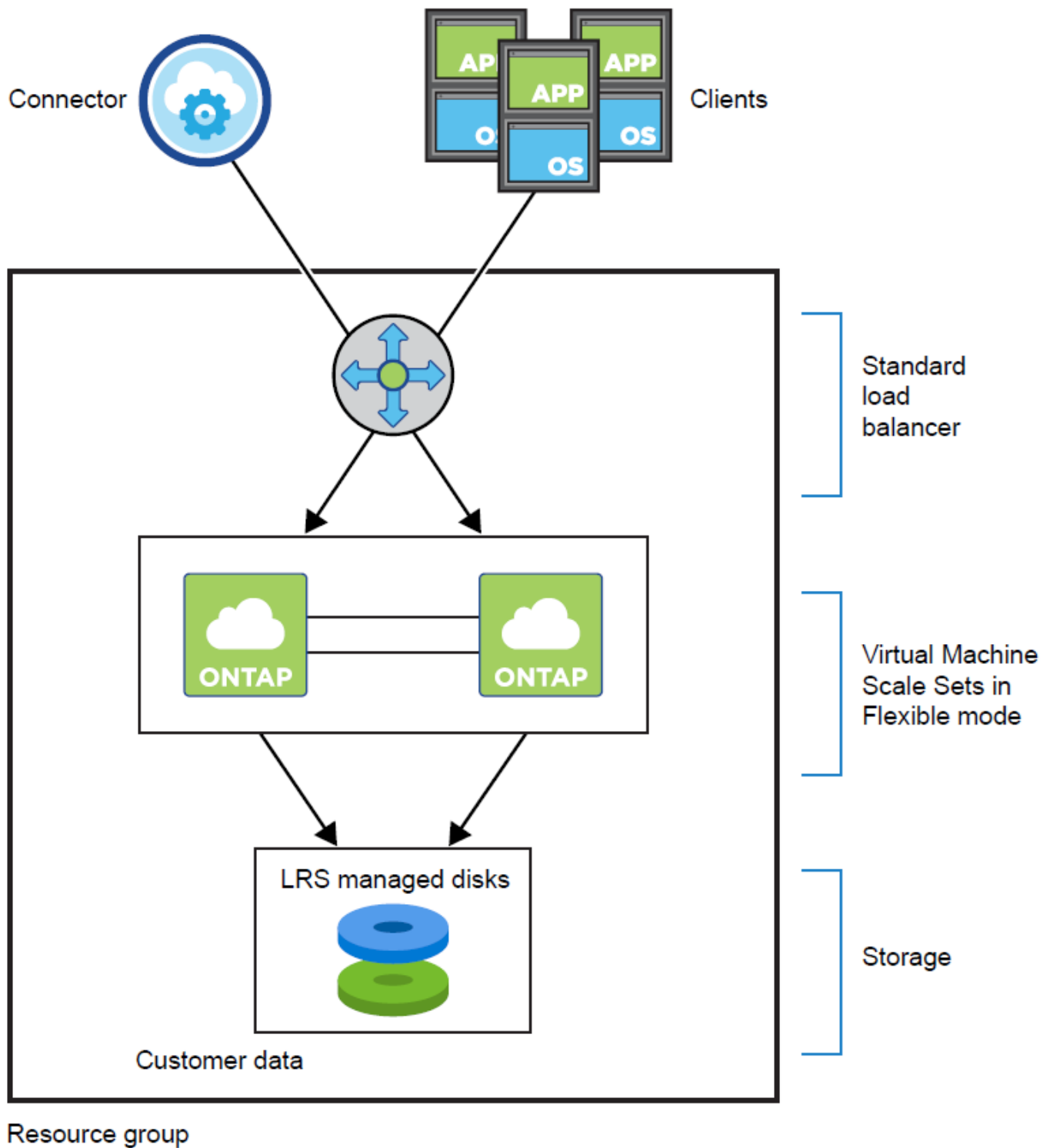
- Azure Blob ストレージへのデータ階層化には 1 つのストレージ アカウントが必要です。
- Cloud Volumes ONTAP 9.7 以降、コンソールが HA ペア用に作成するストレージ アカウントは、汎用 v2 ストレージ アカウントです。
- Cloud Volumes ONTAP システムを追加するときに、Cloud Volumes ONTAP 9.7 HA ペアから Azure ストレージ アカウントへの HTTPS 接続を有効にできます。このオプションを有効にすると書き込みパフォーマンスに影響する可能性があることに注意してください。システムを作成した後は設定を変更できません。



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"](#)。

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

共有管理ディスク上で実行される Cloud Volumes ONTAP HA 単一アベイラビリティゾーン構成には、次のコンポーネントが含まれます。



コンソールによってデプロイされる Azure コンポーネントについては、次の点に注意してください。

Azure 標準ロードバランサー

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

単一のアベイラビリティゾーン内のVM

Cloud Volumes ONTAP 9.15.1 以降では、単一のアベイラビリティゾーン (AZ) で異機種仮想マシン (VM) を作成および管理できます。同じ AZ 内の別々の障害ドメインに高可用性 (HA) ノードを展開して、最適な可用性を保証できます。この機能を可能にする柔軟なオーケストレーションモードの詳細については、

["Microsoft Azure ドキュメント: 仮想マシン スケール セット"](#)。

ゾーン展開では、次の条件が満たされている場合に Premium SSD v2 マネージド ディスクが使用されません。

- Cloud Volumes ONTAPのバージョンは 9.15.1 以降です。
- 選択したリージョンとゾーンは、Premium SSD v2 マネージド ディスクをサポートしています。サポートされている地域については、以下を参照してください。 ["Microsoft Azure Web サイト: 地域別に利用可能な製品"](#)。
- サブスクリプションはMicrosoftに登録されています["Microsoft.Compute/VMOrchestratorZonalMultiFD 機能"](#)。

ディスク

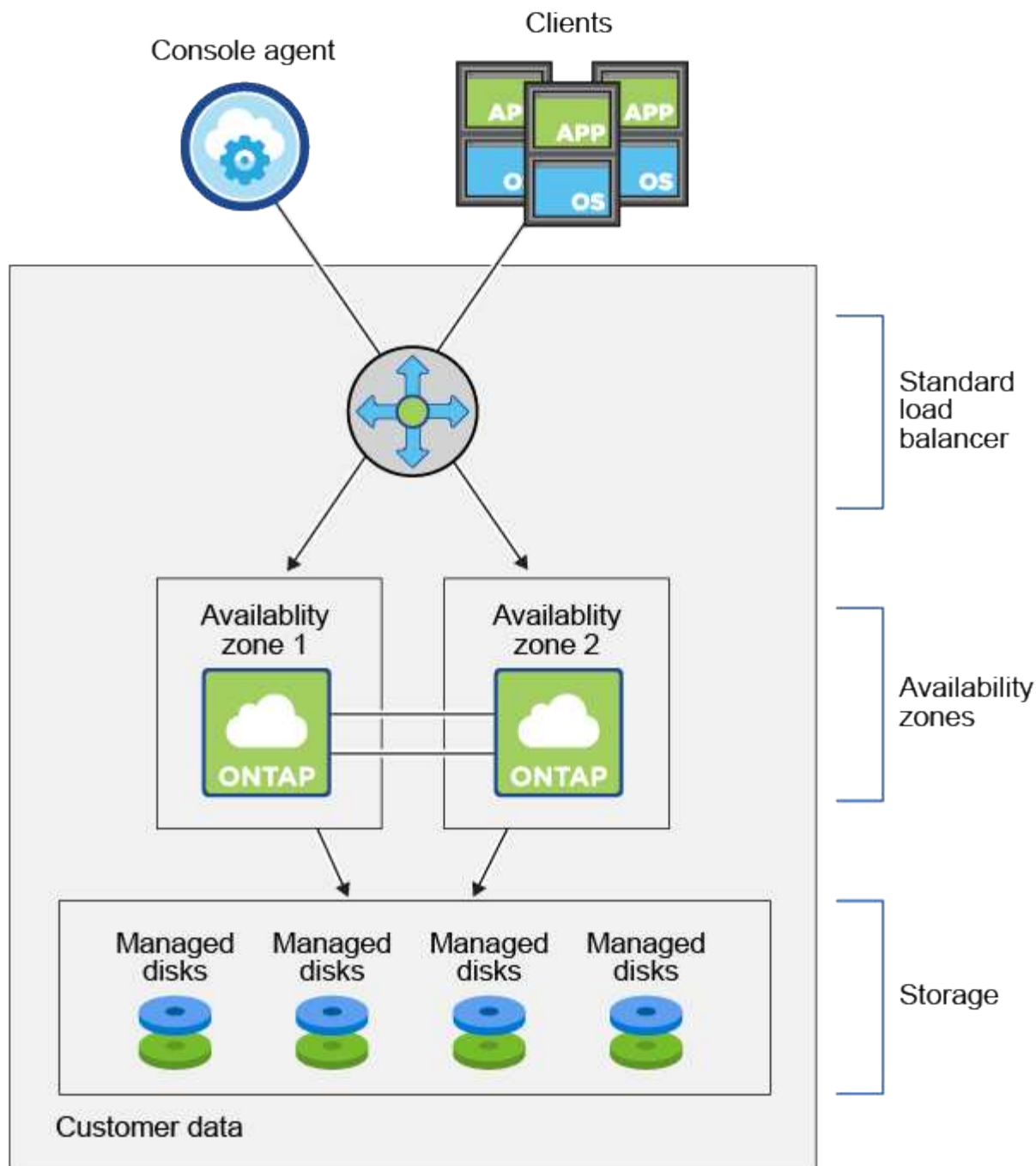
顧客データは、ローカル冗長ストレージ (LRS) 管理ディスクに保存されます。各ノードは他のノードのストレージにアクセスできます。追加のストレージも必要です["ブート、ルート、パートナールート、コア、NVRAMデータ"](#)。

ストレージアカウント

ストレージ アカウントは、診断ログと BLOB ストレージへの階層化を処理するために、マネージド ディスク ベースの展開に使用されます。

HA マルチアベイラビリティゾーン構成

Azure のCloud Volumes ONTAP HA 複数可用性ゾーン構成には、次のコンポーネントが含まれます。



Resource group

コンソールによってデプロイされる Azure コンポーネントについては、次の点に注意してください。

Azure 標準ロードバランサー

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

アベイラビリティ ゾーン

HA マルチアベイラビリティゾーン構成では、2 つのCloud Volumes ONTAPノードが異なるアベイラビリティゾーンにデプロイされるデプロイメント モデルが利用され、ノードが異なる障害ドメインに配置されることで冗長性と可用性が確保されます。フレキシブルオーケストレーションモードの仮想マシンスケールセットがAzureの可用性ゾーンをどのように使用できるかについては、["Microsoft Azure ドキュメント: 可用性ゾーンを使用する仮想マシン スケール セットを作成する"](#)。

ディスク

顧客データは、ゾーン冗長ストレージ (ZRS) マネージド ディスクに保存されます。各ノードは他のノードのストレージにアクセスできます。追加のストレージも必要です"[ブート、ルート、パートナールート、コアデータ](#)"。

ストレージアカウント

ストレージ アカウントは、診断ログと BLOB ストレージへの階層化を処理するために、マネージド ディスク ベースの展開に使用されます。

RPOおよびRTO

HA 構成では、次のようにデータの高可用性が維持されます。

- Recovery Point Objective (RPO;目標復旧時点) は0秒です。データはトランザクションの整合性が確保されており、データ損失はありません。
- Recovery Time Objective (RTO;目標復旧時間) は120秒です。障害が発生した場合、データは120秒以内に使用可能になります。

ストレージの引き継ぎと返却

物理的なONTAPクラスターと同様に、Azure HA ペアのストレージはノード間で共有されます。パートナーのストレージに接続すると、[_テイクオーバー_](#)の際に各ノードが他のノードのストレージにアクセスできるようになります。ネットワーク パスのフェイルオーバー メカニズムにより、クライアントとホストは稼働しているノードと引き続き通信することが可能です。ノードがオンラインに戻ると、パートナーはストレージを返却します。

NAS 構成の場合、障害が発生すると、データ IP アドレスは HA ノード間で自動的に移行されます。

iSCSI の場合、Cloud Volumes ONTAP はマルチパス I/O (MPIO) と非対称論理ユニット アクセス (ALUA) を使用して、アクティブに最適化されたパスと最適化されていないパス間のパス フェイルオーバーを管理します。



ALUAをサポートする特定のホスト構成については、"[NetApp Interoperability Matrix Tool](#)"そして "[SANホストとクラウドクライアントガイド](#)"ホスト オペレーティング システム用。

ストレージのテイクオーバー、再同期、ギブバックはすべてデフォルトで自動で行われます。ユーザーの操作は必要ありません。

ストレージ構成

HA ペアは、両方のノードがクライアントにデータを提供するアクティブ/アクティブ構成として使用することも、アクティブ ノードのストレージを引き継いだ場合にのみパッシブ ノードがデータ要求に応答するアクティブ/パッシブ構成として使用することもできます。

Google Cloud のCloud Volumes ONTAP HA ペアについて学ぶ

Cloud Volumes ONTAP の高可用性 (HA) 構成は、中断のない運用とフォールト トレランスを実現します。Google Cloud では、データは 2 つのノード間で同期的にミラーリングされます。

HA コンポーネント

Google Cloud のCloud Volumes ONTAP HA 構成には、次のコンポーネントが含まれます。

- データが相互に同期してミラーリングされる 2 つのCloud Volumes ONTAPノード。
- ストレージの引き継ぎとギブバックのプロセスを支援するためにノード間の通信チャンネルを提供するメディアエーター インスタンス。
- 1 つのゾーンまたは 3 つのゾーン (推奨)。

3 つのゾーンを選択した場合、2 つのノードとメディアエーターは別々の Google Cloud ゾーンに配置されます。

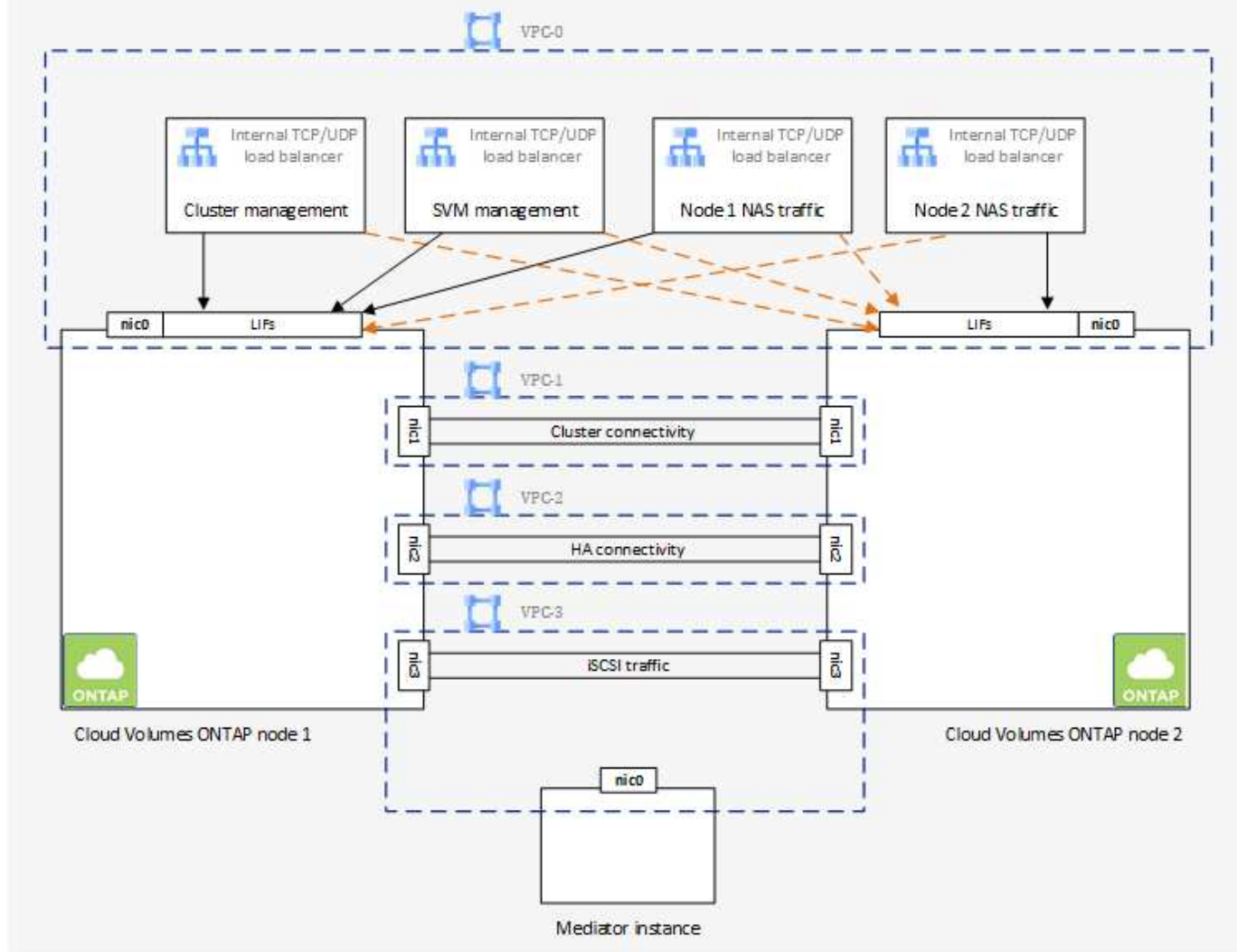
- 4 つの仮想プライベート クラウド (VPC)。

GCP では各ネットワーク インターフェースが個別の VPC ネットワークに存在する必要があるため、この構成では 4 つの VPC が使用されます。

- Cloud Volumes ONTAP HA ペアへの受信トラフィックを管理する 4 つの Google Cloud 内部ロードバランサ (TCP/UDP) 。

["ネットワーク要件について学ぶ"](#)ロードバランサー、VPC、内部 IP アドレス、サブネットなどの詳細が含まれます。

次の概念図は、Cloud Volumes ONTAP HA ペアとそのコンポーネントを示しています。



メディエーター

Google Cloud のメディエーター インスタンスに関する重要な詳細は次のとおりです。

インスタンスタイプ

e2-micro（以前はf1-microインスタンスが使用されていました）

ディスク

それぞれ 10 GiB の標準永続ディスク 2 つ

オペレーティング システム

Debian 11



Cloud Volumes ONTAP 9.10.0 以前では、Debian 10 がメディエーターにインストールされていました。

アップグレード

Cloud Volumes ONTAPをアップグレードすると、NetAppコンソールは必要に応じてメディエーター イン

スタンスも更新します。

インスタンスへのアクセス

Debianの場合、デフォルトのクラウドユーザーは `admin`。Google Cloudは、`admin` Google Cloud コンソールまたは `gcloud` コマンドラインから SSH アクセスが要求された場合のユーザー。指定できます ``sudo`` ルート権限を取得します。

サードパーティエージェント

サードパーティ エージェントまたは VM 拡張機能は、メディアエーター インスタンスではサポートされません。

ストレージの引き継ぎと返却

1 つのノードがダウンした場合、他のノードがパートナーにデータを提供して、継続的なデータ サービスを提供します。データはパートナーに同期的にミラーリングされているため、クライアントはパートナー ノードから同じデータにアクセスできます。

ノードが再起動した後、パートナーはストレージを返す前にデータを再同期する必要があります。データの再同期にかかる時間は、ノードがダウンしている間に変更されたデータの量によって異なります。

ストレージのテイクオーバー、再同期、ギブバックはすべてデフォルトで自動で行われます。ユーザーの操作は必要ありません。

RPOおよびRTO

HA 構成では、次のようにデータの高可用性が維持されます。

- Recovery Point Objective (RPO;目標復旧時点) は0秒です。

データはトランザクションの整合性が確保されており、データ損失はありません。

- Recovery Time Objective (RTO;目標復旧時間) は120秒です。

障害が発生した場合、データは120秒以内に使用可能になります。

HA展開モデル

複数のゾーンまたは単一のゾーンに HA 構成を展開することで、データの高可用性を確保できます。

複数のゾーン（推奨）

3 つのゾーンにわたって HA 構成を展開すると、ゾーン内で障害が発生した場合でも継続的なデータ可用性が確保されます。書き込みパフォーマンスは単一ゾーンを使用する場合と比べてわずかに低下しますが、最小限であることに注意してください。

単一ゾーン

単一のゾーンにデプロイされる場合、Cloud Volumes ONTAP HA 構成では、スプレッド配置ポリシーが使用されます。このポリシーにより、障害の分離を実現するために個別のゾーンを使用する必要がなく、ゾーン内の単一障害点から HA 構成が保護されます。

このデプロイメント モデルでは、ゾーン間のデータ送信料金が発生しないため、コストが削減されます。

HAペアにおけるストレージの仕組み

ONTAPクラスターとは異なり、GCP のCloud Volumes ONTAP HA ペアのストレージはノード間で共有されません。代わりに、障害発生時にデータが利用できるように、データはノード間で同期的にミラーリングされます。

ストレージ割り当て

新しいボリュームを作成し、追加のディスクが必要になった場合、コンソールは両方のノードに同じ数のディスクを割り当て、ミラー化されたアグリゲートを作成してから、新しいボリュームを作成します。たとえば、ボリュームに 2 つのディスクが必要な場合、コンソールはノードごとに 2 つのディスクを割り当て、合計 4 つのディスクを割り当てます。

ストレージ構成

HA ペアは、両方のノードがクライアントにデータを提供するアクティブ/アクティブ構成として使用することも、アクティブ ノードのストレージを引き継いだ場合にのみパッシブ ノードがデータ要求に応答するアクティブ/パッシブ構成として使用することもできます。

HA構成のパフォーマンス期待値

Cloud Volumes ONTAP HA 構成では、ノード間でデータが同期的に複製されるため、ネットワーク帯域幅が消費されます。その結果、単一ノードのCloud Volumes ONTAP構成と比較して、次のパフォーマンスが期待できます。

- 1 つのノードからのみデータを提供する HA 構成の場合、読み取りパフォーマンスは単一ノード構成の読み取りパフォーマンスに匹敵しますが、書き込みパフォーマンスは低くなります。
- 両方のノードからデータを提供する HA 構成の場合、読み取りパフォーマンスは単一ノード構成の読み取りパフォーマンスよりも高く、書き込みパフォーマンスは同じかそれ以上になります。

Cloud Volumes ONTAPのパフォーマンスの詳細については、以下を参照してください。"[パフォーマンス](#)"。

ストレージへのクライアントアクセス

クライアントは、ボリュームが存在するノードのデータ IP アドレスを使用して NFS および CIFS ボリュームにアクセスする必要があります。NAS クライアントがパートナー ノードの IP アドレスを使用してボリュームにアクセスすると、トラフィックが両方のノード間で行われ、パフォーマンスが低下します。



HA ペアのノード間でボリュームを移動する場合は、他のノードの IP アドレスを使用してボリュームを再マウントする必要があります。そうしないと、パフォーマンスが低下する可能性があります。クライアントが NFSv4 参照または CIFS のフォルダー リダイレクトをサポートしている場合は、Cloud Volumes ONTAPシステムでこれらの機能を有効にして、ボリュームの再マウントを回避できます。詳細については、ONTAP のドキュメントを参照してください。

ボリュームを選択し、*マウント コマンド*をクリックすると、コンソールから正しい IP アドレスを見つけることができます。

Volume Actions

View volume details

Mount command

Clone volume

Edit volume tags

Edit volume settings

Delete volume

Protection Actions

Advanced Actions

関連リンク

- ["ネットワーク要件について学ぶ"](#)
- ["GCP を使い始める方法を学ぶ"](#)

Cloud Volumes ONTAP HAペアのノードがオフラインの場合、操作は利用できません

HA ペアの一方向のノードが利用できない場合、もう一方のノードがパートナーにデータを提供して、継続的なデータ サービスを提供します。これは、ストレージ テイクオーバ

ーと呼ばれます。ストレージ内のギブバックが完了するまで、いくつかのアクションは利用できません。



HA ペアのノードが使用できない場合、NetAppコンソールのシステムの状態は「*Degraded*」になります。

ストレージのテイクオーバーでは、次のアクションは使用できません。

- サポート登録
- ライセンスの変更
- インスタンスまたはVMタイプの変更
- 書き込み速度の変化
- CIFSのセットアップ
- 構成バックアップの場所の変更
- クラスターパスワードの設定
- ディスクとアグリゲートの管理（高度な割り当て）

ストレージのギブバックが完了し、システムの状態が正常に戻った後、これらのアクションは再び利用可能になります。

Cloud Volumes ONTAP のデータ暗号化とランサムウェア保護について学ぶ

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

保存中のデータを暗号化

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

- NetApp暗号化ソリューション (NVE および NAE)
- AWS Key Management Service
- Azure Storage Service Encryption
- Google Cloud Platformのデフォルトの暗号化

NetApp暗号化ソリューションは、ハイパーバイザー レベルでデータを暗号化するクラウド プロバイダーのネイティブ暗号化と組み合わせて使用できます。こうすることで二重暗号化が実現され、非常に機密性の高いデータには望ましいものとなる可能性があります。暗号化されたデータにアクセスすると、そのデータは 2 回暗号化解除されます。1 回目はハイパーバイザー レベルで (クラウド プロバイダーのキーを使用)、2 回目はNetApp暗号化ソリューションを使用して (外部キー マネージャーのキーを使用) です。

NetApp暗号化ソリューション (NVE および NAE)

Cloud Volumes ONTAPは以下をサポートします ["NetAppボリューム暗号化 \(NVE\) とNetAppアグリゲート暗号化 \(NAE\)"](#)。NVE と NAE は、ボリュームの (FIPS) 140-2 準拠の保存データ暗号化を可能にするソフトウェア

ベースのソリューションです。NVE と NAE はどちらも AES 256 ビット暗号化を使用します。

- NVE は保存中のデータをボリュームごとに暗号化します。各データ ボリュームには独自の暗号化キーがあります。
- NAE は NVE の拡張機能であり、各ボリュームのデータを暗号化し、ボリュームはアグリゲート全体でキーを共有します。NAE では、アグリゲート内のすべてのボリュームにわたる共通ブロックの重複排除も可能になります。

Cloud Volumes ONTAP は、Fortanix などのサードパーティ ソリューションを含む、AWS、Azure、Google Cloud が提供する外部キー管理サービス (EKM) を使用して、NVE と NAE の両方をサポートします。ONTAP とは異なり、Cloud Volumes ONTAP の場合、暗号化キーは ONTAP ではなくクラウド プロバイダー側で生成されます。

Cloud Volumes ONTAP は、ONTAP が使用する標準の Key Management Interoperability Protocol (KMIP) サービスを使用します。サポートされているサービスの詳細については、"[Interoperability Matrix Tool](#)"。

NVE を使用する場合は、クラウド プロバイダーのキー ボールトを使用して ONTAP 暗号化キーを保護するオプションがあります。

- AWS キー管理サービス (KMS)
- Azure キー コンテナ (AKV)
- Google Cloud Key Management Service

外部キー マネージャーを設定すると、新しいアグリゲートでは NetApp Aggregate Encryption (NAE) がデフォルトで有効になります。NAE アグリゲートの一部ではない新しいボリュームでは、NVE がデフォルトで有効になっています (たとえば、外部キー マネージャーを設定する前に作成された既存のアグリゲートがある場合)。

サポートされているキー マネージャーを設定することだけが、必要な手順です。セットアップ手順については、"[NetApp 暗号化ソリューションでボリュームを暗号化](#)"。

AWS Key Management Service

AWS で Cloud Volumes ONTAP システムを起動すると、"[AWS キー管理サービス \(KMS\)](#)"。NetApp コンソールは、カスタマー マスター キー (CMK) を使用してデータ キーを要求します。



Cloud Volumes ONTAP システムを作成した後、AWS データ暗号化方法を変更することはできません。

この暗号化オプションを使用する場合は、AWS KMS が適切に設定されていることを確認する必要があります。詳細については、"[AWS KMS の設定](#)"。

Azure Storage Service Encryption

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

必要に応じて独自の暗号化キーを使用することもできます。"[Azure で顧客管理キーを使用するために Cloud Volumes ONTAP を設定する方法を学びます](#)"。

Google Cloud Platformのデフォルトの暗号化

"[Google Cloud Platform の保存データ暗号化](#)" Cloud Volumes ONTAPではデフォルトで有効になっています。セットアップは必要ありません。

Google Cloud Storage では、データがディスクに書き込まれる前に常に暗号化されますが、コンソール API を使用して、顧客管理の暗号化キー を使用するCloud Volumes ONTAPシステムを作成できます。これらは、Cloud Key Management Service を使用して GCP で生成および管理するキーです。"[詳細情報](#)"。

ONTAPウイルススキャン

ONTAPシステムに統合されたウイルス対策機能を使用すると、ウイルスやその他の悪意のあるコードによるデータの侵害から保護できます。

ONTAPウイルス スキャン (Vscan と呼ばれる) は、クラス最高のサードパーティ製ウイルス対策ソフトウェアとONTAP の機能を組み合わせて、スキャンするファイルとそのタイミングを制御するために必要な柔軟性を実現します。

Vscanでサポートされているベンダー、ソフトウェア、バージョンの詳細については、"[NetApp Interoperability Matrix](#)"。

ONTAPシステムでウイルス対策機能を設定および管理する方法については、"[ONTAP 9 アンチウイルス設定ガイド](#)"。

ランサムウェア対策

ランサムウェア攻撃は、企業の時間、リソース、評判に損害を与える可能性があります。コンソールを使用すると、可視性、検出、修復のための効果的なツールを提供する、ランサムウェアに対するNetAppソリューションを実装できます。

- コンソールは、スナップショット ポリシーによって保護されていないボリュームを識別し、それらのボリュームでデフォルトのスナップショット ポリシーをアクティブ化できるようにします。

スナップショット コピーは読み取り専用であるため、ランサムウェアによる破損を防ぎます。また、単一のファイルコピーまたは完全な災害復旧ソリューションのイメージを作成するための細分性も提供できます。

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

Ransomware Protection

Ransomware attacks can cost a business time, resources, and reputation. The NetApp solution for ransomware provides effective tools for visibility, detection, and remediation. [Learn More](#)

1 Enable Snapshot Copy Protection

50 %
Protection

1 Volumes without a Snapshot Policy

To protect your data, activate the default Snapshot policy for these volumes

Activate Snapshot Policy

2 Block Ransomware File Extensions



ONTAP's native FPolicy configuration monitors and blocks file operations based on a file's extension.

[View Denied File Names](#)

Activate FPolicy

"ランサムウェア対策のためのNetAppソリューションの実装方法を学ぶ"。

Cloud Volumes ONTAPワークロードのパフォーマンス監視について学ぶ

パフォーマンス結果を確認することで、どのワークロードがCloud Volumes ONTAPに適しているかを判断できます。

パフォーマンス技術レポート

- Cloud Volumes ONTAP for AWS

["NetAppテクニカルレポート4383：Amazon Web Servicesにおけるアプリケーションワークロードを用いたCloud Volumes ONTAPのパフォーマンス特性"](#)

- Microsoft Azure 向けCloud Volumes ONTAP

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

- Cloud Volumes ONTAP for Google Cloud

["NetAppテクニカル レポート 4816: Google Cloud 向けCloud Volumes ONTAPのパフォーマンス特性"](#)

CPUパフォーマンス

Cloud Volumes ONTAPノードは、クラウド プロバイダーの監視ツールから、高い使用率 (90% 以上) として表示されます。これは、ONTAP が仮想マシンに提供されるすべての vCPU を予約し、必要なときに使用できるようにするためです。

詳細については、["CLI を使用してONTAP CPU 使用率を監視する方法に関するNetAppナレッジベースの記事"](#)

ノードベースBYOLのライセンス管理

ノードベースの BYOL (個人ライセンス持ち込み) を持つ各Cloud Volumes ONTAPシステムには、アクティブなサブスクリプションとともにシステム ライセンスがインストールされている必要があります。 NetAppコンソールは、ライセンスを管理し、有効期限が切れる前に警告を表示することで、プロセスを簡素化します。



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せん。

["Cloud Volumes ONTAPのライセンスオプションの詳細"](#)。

["ノードベースのライセンスの管理方法について詳しくは、こちらをご覧ください。"](#)。

BYOLシステムライセンス

ノードベースのライセンスはNetAppから入手できます。単一ノードシステムまたはHAペアに対して購入できるライセンスの数に制限はありません。



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"](#)。

ノードベースのライセンスでは、単一ノードまたはHAペアに最大368TiBの容量が提供されます。CloudCloud Volumes ONTAP BYOLシステムで368TiBを超える容量を割り当てるために、複数のライセンスをご購入いただいた場合があります。例えば、2つのライセンスで最大736TiBの容量をCloud Volumes ONTAPに割り当てることができます。あるいは、4つのライセンスで最大1.4TiBの容量を確保することも可能です。

ディスク制限により、ディスクのみを使用すると容量制限に到達できなくなる可能性があることに注意してください。ディスク制限を超えるには["非アクティブなデータをオブジェクトストレージに階層化する"](#)。ディスク制限の詳細については、["Cloud Volumes ONTAPリリースノートのストレージ制限"](#)。

新しいシステムのライセンス管理

ノードベースの BYOL システムを作成すると、コンソールにライセンスのシリアル番号とNetAppサポート サイト アカウントの入力が求められます。コンソールは、アカウントを使用してNetAppからライセンス ファイルをダウンロードし、Cloud Volumes ONTAPシステムにインストールします。

["NetAppサポートサイトアカウントをコンソールに追加する方法を学びます"](#)。

コンソールが安全なインターネット接続経由でライセンスファイルにアクセスできない場合は、["ファイルを自分で入手し、手動でコンソールにアップロードする"](#)。

ライセンスの有効期限

コンソールには、ノードベースのライセンスの有効期限が切れる 30 日前と、ライセンスの有効期限が切れたときに再度警告が表示されます。次の画像は、ユーザー インターフェースに表示される 30 日間の有効期限の警告を示しています。



メッセージを確認するシステムを選択できます。

組織またはアカウント管理者であり、オプションを有効にしている場合、コンソールには、メールで送信されるCloud Volumes ONTAPレポートにライセンス有効期限の警告が含まれます。電子メールで送信されるレポートには、2週間ごとのライセンス有効期限の警告が含まれます。

ライセンスを期限内に更新しないと、Cloud Volumes ONTAPシステムは自動的にシャットダウンします。再起動すると、再びシャットダウンします。

ライセンスの更新

NetApp の担当者に連絡してノードベースの BYOL サブスクリプションを更新すると、コンソールはNetApp から新しいライセンスを自動的に取得し、Cloud Volumes ONTAPシステムにインストールします。

コンソールが安全なインターネット接続経由でライセンスファイルにアクセスできない場合は、["ファイルを自分で入手し、手動でコンソールにアップロードする"](#)。

新しいシステムへのライセンスの移行

既存のシステムを削除し、同じライセンスを使用して新しいシステムを作成すると、ノードベースの BYOL ライセンスはCloud Volumes ONTAPシステム間で転送可能になります。

たとえば、既存のライセンス システムを削除し、別の VPC/VNet またはクラウド プロバイダーの新しい BYOL システムでそのライセンスを使用する場合があります。どのクラウド プロバイダーでも機能するのは、クラウドに依存しないシリアル番号のみであることに注意してください。クラウドに依存しないシリアル番号は、908xxxx というプレフィックスで始まります。

BYOL ライセンスは会社と特定のNetAppサポート サイトの認証情報に関連付けられていることに注意することが重要です。

Cloud Volumes ONTAPでAutoSupportとDigital Advisor がどのように使用されるかを学びます

ONTAPのAutoSupportコンポーネントは、計測データを収集して分析用に送信します。Active IQ Digital Advisor (Digital Advisorとも呼ばれます) は、 AutoSupportからのデータを分析し、プロアクティブなケアと最適化を提供します。Digital Advisorは人工知能を使用して潜在的な問題を特定し、業務に影響が及ぶ前に解決できるように支援します。

Digital Advisorはクラウドベースのポータルとモバイル アプリで構成されます。実用的な予測分析とプロアクティブなサポートを提供することで、グローバル ハイブリッド クラウド全体でのデータ インフラの最適化を実現します。NetAppと有効なSupportEdge契約を締結しているお客様であれば、Digital Advisorからデータ主

体の分析情報と推奨事項を受け取ることができます（機能は製品およびサポート レベルによって異なります）。

以下は、Digital Advisorで実行できる機能の一例です。

- アップグレードを計画する。

Digital Advisorは新しいバージョンのONTAPにアップグレードすることで解決できる環境内の問題を特定し、Upgrade Advisorがアップグレードの計画を支援します。

- システムの健全性を表示する。

Digital Advisorダッシュボードに健全性に関する問題が報告され、問題の解決方法が提示されます。ストレージ スペースが不足しないようにシステム容量を監視できます。システムのサポート ケースが表示されます。

- パフォーマンスを管理する。

Digital Advisor は、ONTAP System Manager で確認できるよりも長い期間にわたるシステム パフォーマンスを表示します。パフォーマンスに影響を与えている構成やシステムの問題を特定できます。効率を最大化する。ストレージ効率の指標を確認し、より多くのデータをより少ないスペースに格納する方法を特定できます。

- インベントリと構成を表示する。

Digital Advisorでは、すべてのインベントリおよびソフトウェアとハードウェアの構成情報が表示されます。サービス契約の期限を確認し、サポートが中断されないようサービス契約を更新してください。

関連リンク

- ["NetAppドキュメント: Digital Advisor"](#)
- ["Digital Advisorのリリース"](#)
- ["SupportEdgeサービス"](#)

Cloud Volumes ONTAPでサポートされているデフォルト構成

Cloud Volumes ONTAPがデフォルトでどのように構成されているかを理解しておく、システムのセットアップと管理に役立ちます。特に、Cloud Volumes ONTAPのデフォルトのセットアップはONTAPとは異なるため、ONTAPに精通している場合は役立ちます。

デフォルト設定

- NetAppコンソールは、Cloud Volumes ONTAPを展開するときに、1つのデータ提供ストレージ VM を作成します。一部の構成では追加のストレージ VM がサポートされます。["ストレージVMの管理について詳しくはこちら"](#)。

3.9.5 リリース以降、初期ストレージ VM で論理スペース レポートが有効になります。スペースが論理的に報告される場合、ONTAP は、ストレージ効率機能によって節約されたすべての物理スペースも使用済みとして報告されるようにボリューム スペースを報告します。インラインストレージ効率化機能の詳細については、ナレッジベースの記事を参照してください。 ["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?"

- コンソールは、Cloud Volumes ONTAPに次のONTAP機能ライセンスを自動的にインストールします。
 - CIFS
 - FlexCache
 - FlexClone
 - iSCSI
 - Cloud Volumes ONTAP 9.12.1 GA から開始されるマルチテナント暗号化キー管理 (MTEKM)
 - NetAppボリューム暗号化 (BYOL (ライセンス持ち込み) または登録済みの従量課金制 (PAYGO) システムのみ)
 - NFS `ifdef::aws[] endif::aws[] ifdef::azure[] endif::azure[]`
 - SnapMirror
 - SnapRestore
 - SnapVault
 - デフォルトでは、いくつかのネットワーク インターフェイスが作成されます。
 - クラスタ管理LIF
 - クラスタ間LIF
 - Azure の HA システム上の SVM 管理 LIF
 - Google Cloud の HA システム上の SVM 管理 LIF
 - AWS の単一ノードシステム上の SVM 管理 LIF
 - ノード管理LIF
- + Google Cloud では、この LIF はクラスタ間 LIF と組み合わせられます。
- iSCSIデータLIF
 - CIFSおよびNFSデータLIF



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

- Cloud Volumes ONTAP は、HTTP を使用して構成バックアップをコンソール エージェントに送信します。

バックアップは `http://ipaddress/occm/offboxconfig/` からアクセスできます。ここで、*ipaddress* はコンソール エージェントのホストの IP アドレスです。

バックアップを使用して、Cloud Volumes ONTAPシステムを再構成できます。設定バックアップの詳細については、"[ONTAPのドキュメント](#)"。

- コンソールは、他の管理ツール (たとえば、ONTAP System Manager やONTAP CLI) とは異なる方法でいくつかのボリューム属性を設定します。

次の表は、デフォルトとは異なる設定のボリューム属性を示しています。

属性	コンソールが設定する値
オートサイズモード	育つ
最大オートサイズ	1,000パーセント  組織またはアカウント管理者は、[設定] ページからこの値を変更できません。
セキュリティ形式	CIFSボリュームの場合はNTFS、NFSボリュームの場合はUNIX
スペース ガランティ形式	なし
UNIX 権限 (NFS のみ)	777

+
これらの属性の詳細については、"[ONTAP volume create マニュアルページ](#)"。

システムデータ用の内部ディスク

コンソールは、ユーザー データ用のストレージに加えて、システム データ用のクラウド ストレージも購入します。

AWS

- ブート、ルート、コア データ用にノードごとに 3 つのディスク:
 - ブートデータ用の47 GiB io1ディスク
 - ルートデータ用の140 GiB gp3ディスク
 - コアデータ用の540 GiB gp2ディスク
- HA ペアの場合:
 - メディエーターインスタンス用の st1 EBS ボリューム 2 つ (ルートディスクとして約 8 GiB のボリューム 1 つとデータディスクとして 4 GiB のボリューム 1 つ)
 - 各ノードに140 GiBのgp3ディスクを1つずつ用意し、他のノードのルートデータのコピーを保存します。



一部のゾーンでは、使用可能な EBS ディスク タイプは gp2 のみです。

- ブートディスクとルートディスクごとに 1 つの EBS スナップショット



スナップショットは再起動時に自動的に作成されます。

- Key Management Service (KMS) を使用して AWS でデータ暗号化を有効にすると、Cloud Volumes ONTAPのブートディスクとルートディスクも暗号化されます。これには、HA ペアのメディエーター イン

スタンスのブート ディスクが含まれます。ディスクは、Cloud Volumes ONTAPシステムを追加するときに選択した CMK を使用して暗号化されます。



AWS では、NVRAMはブートディスク上にあります。

Azure (単一ノード)

- 3 つのプレミアム SSD ディスク:
 - ブートデータ用の10 GiBディスク1台
 - ルートデータ用の140 GiBディスク1台
 - NVRAM用の512 GiBディスク1台

Cloud Volumes ONTAP用に選択した仮想マシンが Ultra SSD をサポートしている場合、システムは Premium SSD ではなく、NVRAMに 32 GiB Ultra SSD を使用します。

- コアを節約するための 1024 GiB 標準 HDD ディスク 1 台
- ブート ディスクとルート ディスクごとに 1 つの Azure スナップショット
- Azure のすべてのディスクは、デフォルトで保存時に暗号化されます。

Cloud Volumes ONTAP用に選択した仮想マシンがデータ ディスクとして Premium SSD v2 マネージド ディスクをサポートしている場合、システムはNVRAM用に 32 GiB の Premium SSD v2 マネージド ディスクを使用し、ルート ディスクとしてもう 1 つを使用します。

Azure (HAペア)

ページブロッブとHAペア

- ブートボリューム用の 10 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- ルート ボリューム用の 140 GiB の Premium Storage ページ BLOB が 2 つ (ノードごとに 1 つ)
- コア保存用の 1024 GiB 標準 HDD ディスク 2 台 (ノードごとに 1 台)
- NVRAM用の 512 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- ブート ディスクとルート ディスクごとに 1 つの Azure スナップショット



スナップショットは再起動時に自動的に作成されます。

- Azure のすべてのディスクは、デフォルトで保存時に暗号化されます。

複数のアベイラビリティゾーンにある共有マネージドディスクを備えた HA ペア

- ブートボリューム用の 10 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- ルートボリューム用の 512 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- コア保存用の 1024 GiB 標準 HDD ディスク 2 台 (ノードごとに 1 台)
- NVRAM用の 512 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- ブート ディスクとルート ディスクごとに 1 つの Azure スナップショット



スナップショットは再起動時に自動的に作成されます。

- Azure のすべてのディスクは、デフォルトで保存時に暗号化されます。

単一のアベイラビリティゾーン内の共有マネージドディスクを使用した **HA** ペア

- ブートボリューム用の 10 GiB プレミアム SSD ディスク 2 台 (ノードごとに 1 台)
- ルート ボリューム用の 512 GiB プレミアム SSD 共有マネージド ディスク 2 つ (ノードごとに 1 つ)
- コア保存用の 1024 GiB 標準 HDD ディスク 2 台 (ノードごとに 1 台)
- NVRAM用の 512 GiB プレミアム SSD マネージド ディスク 2 台 (ノードごとに 1 台)

仮想マシンがデータ ディスクとして Premium SSD v2 マネージド ディスクをサポートしている場合、NVRAMには 32 GiB の Premium SSD v2 マネージド ディスクが使用され、ルート ボリュームには 512 GiB の Premium SSD v2 共有マネージド ディスクが使用されます。

次の条件が満たされている場合は、単一の可用性ゾーンに HA ペアをデプロイし、Premium SSD v2 マネージド ディスクを使用できます。

- Cloud Volumes ONTAPのバージョンは 9.15.1 以降です。
- 選択したリージョンとゾーンは、Premium SSD v2 マネージド ディスクをサポートしています。サポートされている地域については、以下を参照してください。"[Microsoft Azure Web サイト: 地域別に利用可能な製品](#)"。
- サブスクリプションはMicrosoftに登録されています"[Microsoft.Compute/VMOrchestratorZonalMultiFD 機能](#)"。

Google Cloud (単一ノード)

- ブートデータ用の 10 GiB SSD 永続ディスク 1 台
- ルートデータ用の 64 GiB SSD 永続ディスク 1 台
- NVRAM用の 500 GiB SSD 永続ディスク 1 台
- コア保存用の 315 GiB 標準永続ディスク 1 台
- ブートおよびルートデータのスナップショット



スナップショットは再起動時に自動的に作成されます。

- ブート ディスクとルート ディスクはデフォルトで暗号化されます。

Google Cloud (HAペア)

- ブートデータ用の 10 GiB SSD 永続ディスク 2 台
- ルートデータ用の 64 GiB SSD 永続ディスク 4 台
- NVRAM用の 500 GiB SSD 永続ディスク 2 台
- コア保存用の 315 GiB 標準永続ディスク 2 台
- メディエーターデータ用の 10 GiB 標準永続ディスク 1 台

- メディエーターブートデータ用の 10 GiB 標準永続ディスク 1 台
- ブートおよびルートデータのスナップショット



スナップショットは再起動時に自動的に作成されます。

- ブート ディスクとルート ディスクはデフォルトで暗号化されます。

ディスクが存在する場所

ストレージレイアウト:

- ブート データは、インスタンスまたは仮想マシンに接続されたディスク上に存在します。
ブート イメージを含むこのディスクは、Cloud Volumes ONTAPでは使用できません。
- システム構成とログを含むルート データは aggr0 にあります。
- ストレージ仮想マシン (SVM) のルート ボリュームは aggr1 にあります。
- データ ボリュームも aggr1 に存在します。

知識とサポート

サポートに登録する

BlueXPおよびそのストレージソリューションとサービスに固有のテクニカルサポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウドプロバイダーファイルサービスに対するNetAppサポートは有効になりません。クラウドプロバイダーのファイルサービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカルサポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- ["Amazon FSx for ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

サポート登録の概要

サポート資格を有効にするには、次の2つの登録形式があります。

- BlueXPアカウントのシリアル番号を登録します (BlueXPのサポートリソースページにある20桁の960xxxxxxxxxシリアル番号)。

これは、BlueXP内のすべてのサービスに対する単一のサポートサブスクリプションIDとして機能します。各BlueXPアカウントレベルのサポートサブスクリプションを登録する必要があります。

- クラウドプロバイダーのマーケットプレイスで、サブスクリプションに関連付けられたCloud Volumes ONTAPシリアル番号を登録します (これらは20桁の909201xxxxxxxxシリアル番号です)。

これらのシリアル番号は一般にPAYGOシリアル番号と呼ばれ、Cloud Volumes ONTAPの展開時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録すると、サポートチケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppサポートサイト (NSS) アカウントをBlueXPに追加することで完了します。

NetAppサポートのためにBlueXPに登録する

サポートに登録し、サポート資格を有効にするには、BlueXP組織 (またはアカウント) 内の1人のユーザーがNetAppサポートサイトアカウントをBlueXPログインに関連付ける必要があります。NetAppサポートに登録する方法は、NetAppサポートサイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

NSSアカウントをお持ちの既存顧客

NSSアカウントをお持ちのNetAppのお客様の場合は、BlueXPを通じてサポートに登録するだけです。

手順

1. BlueXPコンソールの右上にある設定アイコンを選択し、*資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. **NSS** 資格情報の追加 を選択し、NetAppサポート サイト (NSS) の認証プロンプトに従います。
4. 登録プロセスが成功したことを確認するには、[ヘルプ] アイコンを選択し、[サポート] を選択します。

リソース ページには、BlueXP組織がサポートに登録されていることが表示されます。



他のBlueXPユーザーは、NetAppサポート サイト アカウントをBlueXPログインに関連付けていない場合、同じサポート登録ステータスを表示しないことに注意してください。ただし、これはBlueXP組織がサポートに登録されていないことを意味するものではありません。組織内の 1 人のユーザーがこれらの手順を実行すれば、組織は登録されます。

既存の顧客だが**NSS**アカウントがない

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをBlueXPログインに関連付ける必要があります。

手順

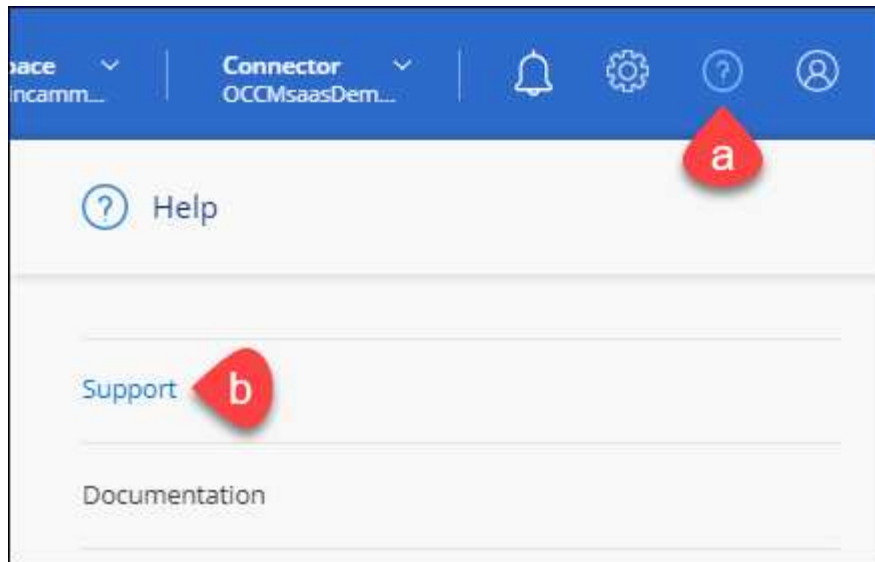
1. NetAppサポートサイトのアカウントを作成するには、"[NetAppサポートサイト ユーザー登録フォーム](#)"
 - a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
 - b. 上記で使ったBlueXPアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を完了して、新しいNSSアカウントをBlueXPログインに関連付けます。NSSアカウントをお持ちの既存顧客。

NetAppの新着情報

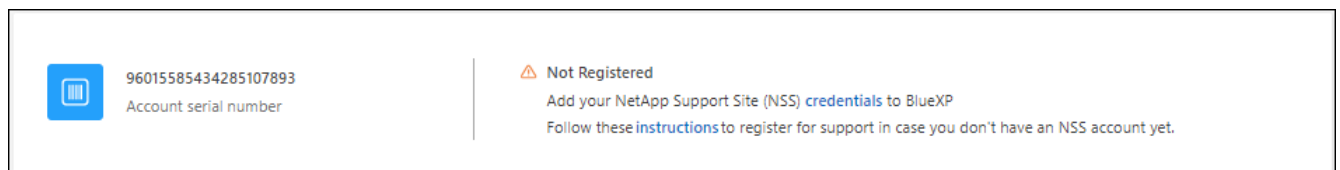
NetAppを初めて使用し、NSS アカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. サポート登録ページからアカウント ID シリアル番号を見つけます。



3. 移動先 "[NetAppのサポート登録サイト](#)"私は登録済みの**NetApp**顧客ではありません を選択します。
4. 必須フィールド（赤いアスタリスクが付いているフィールド）に入力します。
5. 製品ライン フィールドで、**Cloud Manager** を選択し、該当する請求プロバイダーを選択します。
6. 上記の手順 2 からアカウントのシリアル番号をコピーし、セキュリティ チェックを完了して、NetApp のグローバル データ プライバシー ポリシーを読んだことを確認します。

この安全な取引を完了するために、指定されたメールボックスに電子メールが直ちに送信されます。検証メールが数分以内に届かない場合は、必ずスパム フォルダーを確認してください。

7. メール内からアクションを確認します。

確認すると、リクエストがNetAppに送信され、NetAppサポート サイトのアカウントを作成することが推奨されます。

8. NetAppサポートサイトのアカウントを作成するには、"[NetAppサポートサイト ユーザー登録フォーム](#)"
 - a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
 - b. 上記で使用了アカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより処理速度が向上します。

終了後の操作

このプロセス中に、NetAppから連絡が来るはずですが、これは、新規ユーザー向けの 1 回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行してアカウントをBlueXPログインに関連付けます。[NSSアカウントをお持ちの既存顧客](#)。

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける

Cloud Volumes ONTAPの次の主要なワークフローを有効にするには、NetAppサポート サイトの認証情報をBlueXP組織に関連付ける必要があります。

- 従量課金制のCloud Volumes ONTAPシステムをサポート対象として登録する

システムのサポートを有効にし、NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

BlueXP がライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

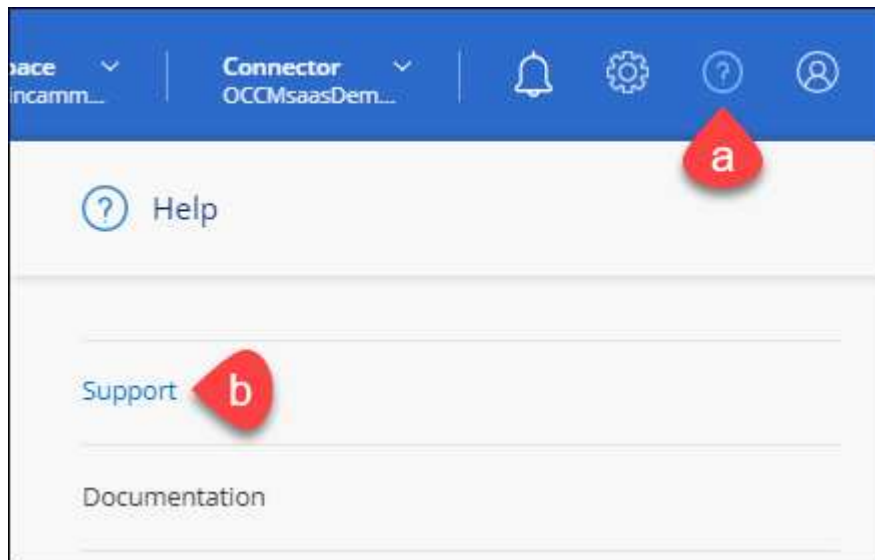
NSS 資格情報をBlueXP組織に関連付けることは、BlueXPユーザー ログインに関連付けられている NSS アカウントとは異なります。

これらの NSS 資格情報は、特定のBlueXP組織 ID に関連付けられています。BlueXP組織に属するユーザーは、サポート > **NSS 管理** からこれらの資格情報にアクセスできます。

- 顧客レベルのアカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できます。
- パートナー アカウントまたは再販業者アカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できますが、顧客レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. *NSS管理 > NSSアカウントの追加*を選択します。
3. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

4. ログイン ページで、NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力して、認証プロセスを実行します。

これらのアクションにより、BlueXP はライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などに NSS アカウントを使用できるようになります。

次の点に注意してください。

- NSS アカウントは顧客レベルのアカウントである必要があります (ゲスト アカウントや一時アカウントではありません)。顧客レベルの NSS アカウントを複数持つことができます。
- パートナー レベルのアカウントの場合、NSS アカウントは 1 つだけ存在できます。顧客レベルの NSS アカウントを追加しようとしたときにパートナー レベルのアカウントが存在する場合は、次のエラー メッセージが表示されます。

「異なるタイプの NSS ユーザーがすでに存在するため、このアカウントでは NSS 顧客タイプは許可されません。」

既存の顧客レベルの NSS アカウントがあり、パートナー レベルのアカウントを追加しようとする場合も同様です。

- ログインが成功すると、NetApp はNSS ユーザー名を保存します。

これは、メールにマッピングされるシステム生成の ID です。*NSS管理*ページでは、... メニュー。

- ログイン認証トークンを更新する必要がある場合は、... メニュー。

このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

ヘルプを受ける

NetAppは、BlueXPとそのクラウドサービスに対して、様々なサポートを提供しています。ナレッジベース (KB) 記事やコミュニティフォーラムなど、充実した無料のセルフサポートオプションを24時間365日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

クラウドプロバイダーのファイルサービスのサポートを受ける

クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- ["Amazon FSx for ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

BlueXPとそのストレージ ソリューションおよびサービスに固有のテクニカル サポートを受けるには、以下に説明するサポート オプションを使用してください。

セルフサポートオプションを使用する

以下のオプションは、24 時間 365 日無料でご利用いただけます。

- ドキュメント

現在表示しているBlueXPドキュメント。

- ["ナレッジベース"](#)

BlueXPナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- ["コミュニティ"](#)

BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりしてください。

NetAppサポートでケースを作成する

上記のセルフ サポート オプションに加えて、サポートを有効にした後は、NetAppサポート スペシャリストと協力して問題を解決することもできます。

始める前に

- *ケースの作成*機能を使用するには、まずNetAppサポート サイトの資格情報をBlueXPログインに関連付ける必要があります。 ["BlueXPログインに関連付けられた資格情報を管理する方法を学びます"](#)。
- シリアル番号を持つONTAPシステムのケースを開く場合は、NSS アカウントがそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *リソース*ページで、テクニカル サポートの下にある利用可能なオプションのいずれかを選択します。
 - a. 電話で誰かと話したい場合は、「電話する」を選択してください。電話をかけることができる電話番号をリストした netapp.com のページに移動します。
 - b. NetAppサポート スペシャリストとのチケットを開くには、[ケースを作成] を選択します。
 - サービス: 問題が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能に関するテクニカル サポートの問題に固有の場合はBlueXP。
 - 作業環境: ストレージに該当する場合は、* Cloud Volumes ONTAP* または * On-Prem* を選択し、関連する作業環境を選択します。

作業環境のリストは、サービスのトップバナーで選択したBlueXP組織 (またはアカウント)、プロジェクト (またはワークスペース)、およびコネクタの範囲内にあります。
 - ケースの優先度: ケースの優先度 (低、中、高、重大) を選択します。

これらの優先順位の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスを置きます。
 - 問題の説明: 該当するエラー メッセージや実行したトラブルシューティング手順など、問題の詳細

な説明を入力します。

- 追加のメールアドレス:この問題を他の人に知らせたい場合は、追加のメールアドレスを入力してください。
- 添付ファイル (オプション): 一度に 1 つずつ、最大 5 つの添付ファイルをアップロードします。

添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。

The screenshot shows a web form titled "ntapitdemo" and "NetApp Support Site Account". It contains several sections: "Service" and "Working Enviroment" (sic) dropdown menus, both currently set to "Select"; a "Case Priority" dropdown menu set to "Low - General guidance"; an "Issue Description" text area with placeholder text "Provide detailed description of problem, applicable error messages and troubleshooting steps taken."; an "Additional Email Addresses (Optional)" text input field with placeholder text "Type here"; and an "Attachment (Optional)" section with a file selection area showing "No files selected", an "Upload" button, and a trash icon. Information icons (i) are present next to the Case Priority, Additional Email Addresses, and Attachment sections.

終了後の操作

サポート ケース番号を示すポップアップが表示されます。NetAppサポート スペシャリストがお客様のケースを確認し、すぐにご連絡いたします。

サポート ケースの履歴については、設定 > タイムライン を選択し、「サポート ケースの作成」というアクションを探します。右端のボタンを使用すると、アクションを展開して詳細を表示できます。

ケースを作成しようとする、次のエラー メッセージが表示される場合があります。

「選択したサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、BlueXPアカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、960xxxx) または作業環境のシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 製品内チャットを使用する
- 非技術的なケースを提出する <https://mysupport.netapp.com/site/help>

サポートケースを管理する（プレビュー）

アクティブおよび解決済みのサポート ケースをBlueXPから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして利用できます。今後のリリースでは、このエクスペリエンスを改良し、機能強化を追加する予定です。製品内チャットを使用してフィードバックをお送りください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の 2 つのビューがあります。
 - 左側のビューには、指定したユーザー NSS アカウントによって過去 3 か月間に開かれたケースの合計が表示されます。
 - 右側のビューには、ユーザーの NSS アカウントに基づいて、会社レベルで過去 3 か月間に開かれたケースの合計が表示されます。

表の結果には、選択したビューに関連するケースが反映されます。

- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は並べ替え機能のみを提供します。

詳細については、以下の手順をご覧ください。

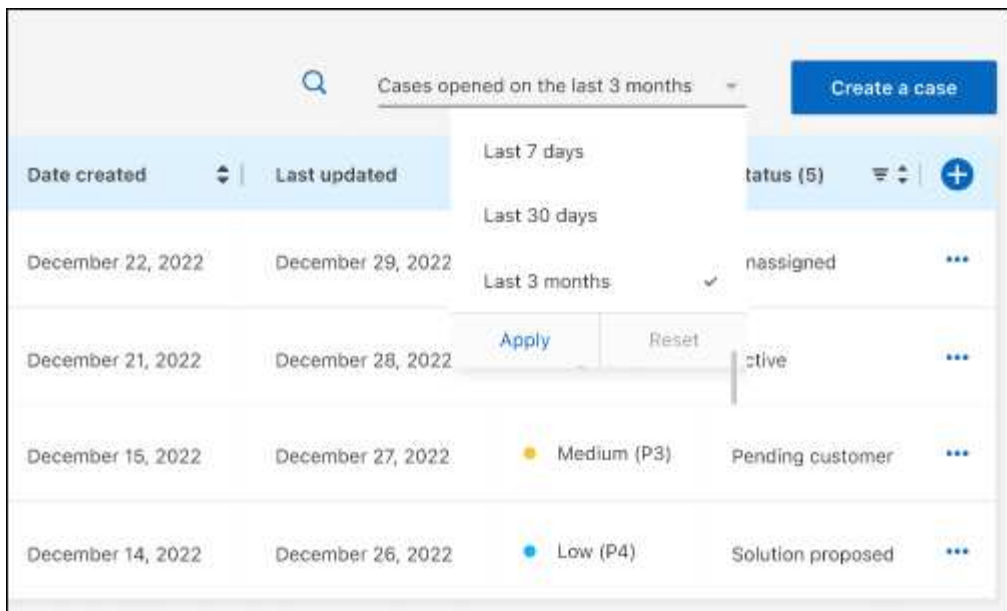
- ケースごとに、ケースメモを更新したり、まだ「クローズ」または「クローズ保留中」ステータスになっていないケースをクローズしたりする機能を提供します。

手順

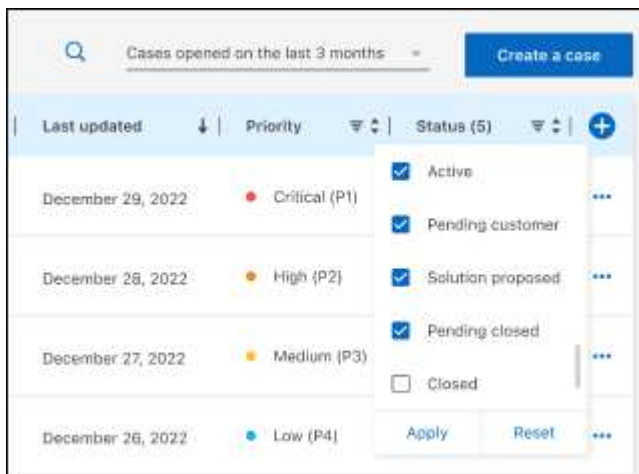
1. BlueXPで、*ヘルプ> サポート*を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをBlueXPに追加します。

ケース管理 ページには、BlueXPユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS 管理** ページの上部に表示される NSS アカウントと同じです。

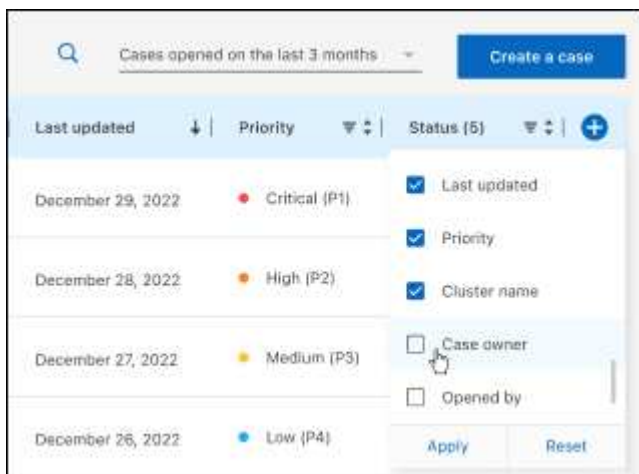
3. 必要に応じて、テーブルに表示される情報を変更します。
 - *組織のケース*の下で*表示*を選択すると、会社に関連付けられているすべてのケースが表示されます。
 - 正確な日付範囲を選択するか、別の期間を選択して日付範囲を変更します。



- 。列の内容をフィルタリングします。



- 。表に表示される列を変更するには、**+** 次に、表示する列を選択します。

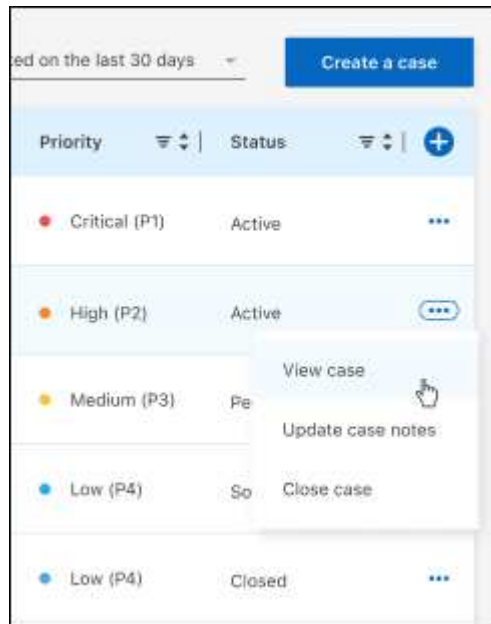


4. 既存のケースを管理するには、**...**利用可能なオプションのいずれかを選択します。

- ケースを表示: 特定のケースに関する詳細をすべて表示します。
- ケースノートを更新: 問題に関する追加の詳細を入力するか、*ファイルのアップロード*を選択して最大 5 つのファイルを添付します。

添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。

- ケースを閉じる: ケースを閉じる理由の詳細を入力し、[ケースを閉じる] を選択します。



法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

プライバシー ポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

通知ファイルには、NetAppソフトウェアで使用するサードパーティの著作権およびライセンスに関する情報が提供されます。

- ["NetAppコンソールに関するお知らせ"](#)
- ["Cloud Volumes ONTAPに関するお知らせ"](#)
- ["ONTAPに関するお知らせ"](#)

著作権に関する情報

Copyright © 2025 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。