



# Cloud Backup のドキュメント

## Cloud Backup

NetApp  
June 20, 2022

# 目次

Cloud Backup のドキュメント .....	1
Cloud Backup の新機能 .....	2
2022年6月14日 .....	2
2022年6月8日 .....	2
2022年5月2日 .....	3
2022 年 4 月 4 日 .....	4
2022 年 3 月 3 日 .....	4
2022 年 2 月 14 日 .....	5
2022 年 1 月 2 日 .....	5
2021 年 11 月 28 日 .....	5
2021 年 11 月 5 日 .....	6
2021 年 10 月 4 日 .....	6
2021 年 9 月 2 日 .....	7
2021 年 8 月 1 日 .....	7
2021 年 7 月 7 日 .....	8
2021 年 6 月 7 日 .....	8
2021 年 5 月 5 日 .....	8
はじめに .....	10
Cloud Backup の詳細をご確認ください .....	10
Cloud Backup のライセンスをセットアップします .....	12
ONTAP データのバックアップとリストア .....	18
Cloud Backup を使用して ONTAP クラスタのデータを保護します .....	18
Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ .....	24
オンプレミスの ONTAP データを Azure BLOB ストレージにバックアップする .....	30
オンプレミスの ONTAP データの StorageGRID へのバックアップ .....	39
ONTAP システムのバックアップの管理 .....	45
バックアップファイルからの ONTAP データのリストア .....	62
Kubernetes データのバックアップとリストア .....	79
Cloud Backup を使用して Kubernetes クラスタのデータを保護 .....	79
Kubernetes の永続ボリュームのデータを Azure BLOB ストレージにバックアップする .....	83
Kubernetes システムのバックアップの管理 .....	88
バックアップファイルからの Kubernetes データのリストア .....	99
オンプレミスのアプリケーションデータのバックアップとリストア .....	102
オンプレミスアプリケーションのデータを保護 .....	102
オンプレミスアプリケーションのデータをクラウドにバックアップ .....	104
アプリケーションの保護を管理します .....	106
アプリケーションデータをリストアする .....	109
仮想マシンのデータのバックアップとリストア .....	113
仮想マシンのデータを保護 .....	113

データストアをクラウドにバックアップ.....	115
仮想マシンの保護を管理します.....	116
クラウドから仮想マシンをリストアします.....	118
Cloud Backup API .....	120
はじめに.....	120
APIを使用した例 .....	122
API リファレンス.....	125
参照 .....	126
AWS S3 アーカイブストレージクラスおよびリストアの読み出し時間 .....	126
Azure のアーカイブ階層およびリストアの読み出し時間 .....	127
知識とサポート .....	129
サポートに登録します.....	129
ヘルプを表示します.....	130
法的通知.....	132
著作権.....	132
商標 .....	132
特許 .....	132
プライバシーポリシー.....	132
オープンソース .....	132

# Cloud Backup のドキュメント

# Cloud Backup の新機能

Cloud Backup の新機能をご確認ください。

## 2022年6月14日

インターネットにアクセスできないサイトのオンプレミス**ONTAP** クラスタデータをバックアップするサポートが追加されました

オンプレミスのONTAP クラスタが、インターネットにアクセスできないサイト（ダークサイトまたはオフラインサイトとも呼ばれます）にある場合は、Cloud Backupを使用して、同じサイトにあるNetApp StorageGRID システムにボリュームデータをバックアップできるようになりました。この機能を使用するには、Cloud Manager Connector（バージョン3.9.19以降）もオフラインサイトに導入する必要があります。

"コネクタをオフラインサイトにインストールする方法を参照してください"。 <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html>["オフラインサイトのStorageGRIDにONTAP データをバックアップする方法を参照してください"]。

## 2022年6月8日

### Cloud Backup for Virtual Machines 1.1.0のGA版になりました

SnapCenter Plug-in for VMware vSphereとCloud Managerを統合することで、仮想マシン上のデータを保護できます。データストアをクラウドにバックアップし、仮想マシンをオンプレミスのSnapCenter Plug-in for VMware vSphereにリストアする作業は簡単です。

"仮想マシンをクラウドに保護する方法については、こちらをご覧ください"。

クラウドのリストアインスタンスは、**ONTAP** の参照とリストア機能では必要ありません

S3およびBLOBストレージからのファイルレベルの参照およびリストア処理に必要な、別のCloud Restoreインスタンス/仮想マシン。このインスタンスは使用していないときにシャットダウンされますが、ファイルのリストアに時間とコストがかかります。この機能は、必要に応じてコネクタに導入される無償のコンテナに置き換えられました。これには、次の利点があります。

- ファイルレベルのリストア処理のための追加コストは不要です
- ファイルレベルのリストア処理が高速化されます
- Connectorがオンプレミスにインストールされている場合のクラウドからのファイルの参照とリストアの処理がサポートされます

以前に使用していた場合は、Cloud Restoreインスタンス/VMが自動的に削除されることに注意してください。Cloud Backupプロセスが1日に1回実行され、古いCloud Restoreインスタンスがすべて削除されます。この変更は完全に透過的に行われます。データへの影響はなく、バックアップジョブやリストアジョブの変更は通知されません。

## Google CloudおよびStorageGRID ストレージからのファイルのサポートを参照してリストアできます

前述のように、参照および復元操作のコンテナが追加されたことで、Google CloudおよびStorageGRID システムに保存されているバックアップファイルからファイルの復元操作を実行できるようになりました。現在は、参照とリストアを使用して、すべてのパブリッククラウドプロバイダとStorageGRID からファイルをリストアできます。"[参照リストアを使用してONTAP バックアップからボリュームとファイルをリストアする方法を参照してください](#)"。

## ドラッグアンドドロップして、Cloud Backup to S3ストレージを有効にします

バックアップのAmazon S3デスティネーションがキャンバス上の作業環境として存在する場合、オンプレミスのONTAP クラスタまたはCloud Volumes ONTAP システム（AWSにインストール）をAmazon S3作業環境にドラッグしてセットアップウィザードを開始できます。

## Kubernetesクラスタ内に新しく作成されたボリュームにバックアップポリシーを自動的に適用します

Cloud Backupをアクティブ化したあとにKubernetesクラスタに新しい永続ボリュームを追加した場合は、以前にそれらのボリュームのバックアップを忘れずに設定する必要があります。新しく作成したボリュームに自動的に適用するポリシーを選択できます "[\[バックアップ設定ページから選択します\]](#)" Cloud Backupをすでにアクティブ化しているクラスタの場合

## Cloud Backup APIを使用して、バックアップとリストアの処理を管理できるようになりました

APIにはあります <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>。を参照してください "[このページです](#)" を参照してください。

## 2022年5月2日

## Google Cloud Storageのバックアップファイルで検索とリストアがサポートされるようになりました

ボリュームとファイルをリストアするための検索とリストアの方法は、AWSにバックアップファイルを格納するユーザ向けに4月に導入されました。Google Cloud Storageにバックアップファイルを保存するユーザーがこの機能を使用できるようになりました。"[Search & Restoreを使用してボリュームとファイルをリストアする方法を参照してください](#)"。

## Kubernetesクラスタ内に新しく作成されたボリュームにバックアップポリシーが自動的に適用されるように設定します

Cloud Backupをアクティブ化したあとにKubernetesクラスタに新しい永続ボリュームを追加した場合は、以前にそれらのボリュームのバックアップを忘れずに設定する必要があります。新しく作成したボリュームに自動的に適用するポリシーを選択できます。このオプションは、新しいKubernetesクラスタに対してCloud Backupをアクティブ化するときにセットアップウィザードで使用できます。

## Cloud Backupを作業環境でアクティブ化するには、ライセンスが必要になります

Cloud Backupのライセンスの実装方法には、次の点が変更されています。

- Cloud Backupをアクティブ化するには、クラウドプロバイダからPAYGO Marketplaceサブスクリプションに登録するか、ネットアップからBYOLライセンスを購入する必要があります。
- 30日間無償トライアルは、クラウドプロバイダがPAYGOサブスクリプションを使用している場合にのみ利用できます。BYOLライセンスを使用している場合は利用できません。
- 無料トライアルは、Marketplaceのサブスクリプションが開始された日から開始されます。たとえば、Cloud Volumes ONTAP システムのMarketplaceサブスクリプションを30日間使用した後で無料トライアルを有効にした場合、クラウドバックアップトライアルは利用できません。

["使用可能なライセンスモデルの詳細については、こちらをご覧ください"](#)。

## 2022 年 4 月 4 日

### Cloud Backup for Applications 1.1.0 （ SnapCenter 搭載）の GA 版になりました

新しいCloud Backup for Applications機能を使用すると、OracleおよびMicrosoft SQLの既存のアプリケーション整合性スナップショット（バックアップ）を、オンプレミスのプライマリストレージからAmazon S3またはAzure Blobのクラウドオブジェクトストレージにオフロードできます。

必要に応じて、クラウドからオンプレミスヘデータをリストアできます。

["オンプレミスアプリケーションのデータをクラウドで保護する方法については、こちらをご覧ください"](#)。

### すべての ONTAP バックアップファイルでボリュームまたはファイルを検索するための新しい検索とリストア機能

ボリューム名またはフルボリューム名、部分的またはフルファイル名、サイズ範囲、および追加の検索フィルタを使用して、すべての ONTAP バックアップファイル \* にまたがるボリュームまたはファイルを検索できるようになりました。これは、どのクラスタまたはボリュームがデータのソースであるかがわからない場合に、リストアするデータを見つけるための新しい優れた方法です。 ["検索とリストアの使用方法を説明します"](#)。

## 2022 年 3 月 3 日

### GKE Kubernetes クラスタから Google Cloud ストレージに永続ボリュームをバックアップする機能

ネットアップ Astra Trident がインストールされている GKE クラスタで、Cloud Volumes ONTAP for GCP をクラスタのバックエンドストレージとして使用している場合は、Google Cloud ストレージとの間で永続的ボリュームのバックアップとリストアを行うことができます。 ["詳細については、こちらをご覧ください"](#)。

Cloud Data Sense を使用して Cloud Backup ファイルをスキャンするベータ機能は、本リリースでは廃止されました

## 2022 年 2 月 14 日

バックアップポリシーを単一クラスタ内の個々のボリュームに割り当てることができるようになりました

これまでは、クラスタ内のすべてのボリュームに割り当てることができるバックアップポリシーは 1 つだけでした。1 つのクラスタに複数のバックアップポリシーを作成し、異なるボリュームに異なるポリシーを適用できるようになりました。"[クラスタの新しいバックアップポリシーを作成し、選択したボリュームに割り当てる方法を参照してください](#)"。

新しいオプションを使用すると、新規に作成されたボリュームにデフォルトのバックアップポリシーを自動的に適用できます

以前は、Cloud Backup をアクティブ化したあとに作業環境で作成した新しいボリュームには、バックアップポリシーを手動で適用する必要がありました。これで、Cloud Manager、System Manager、CLI、または API を使用してボリュームを作成したかどうかに関係なく、Cloud Backup はボリュームを検出し、デフォルトポリシーとして選択したバックアップポリシーを適用します。

このオプションは、新しい作業環境でバックアップを有効にする場合、または既存の作業環境で \_ ボリュームの管理 \_ ページから有効にする場合に使用できます。

すべてのバックアップジョブとリストアジョブの処理中ステータスを確認するには、新しいジョブモニタを使用できます

ジョブモニタは、バックアップポリシーの変更やバックアップの削除など、複数のボリュームに対して処理を開始した場合に非常に役立ちます。そのため、すべてのボリュームで処理が完了したことを確認できます。  
"[「ジョブモニタの使用法」を参照してください](#)"。

## 2022 年 1 月 2 日

**AKS Kubernetes クラスタから Azure BLOB ストレージに永続ボリュームをバックアップする機能**

AKS クラスタに NetApp Astra Trident がインストールされていて、クラスタのバックエンドストレージとして Cloud Volumes ONTAP for Azure を使用している場合、Azure BLOB ストレージとのボリュームをバックアップおよびリストアできます。["詳細については、こちらをご覧ください"](#)。

このリリースでは、業界標準に合わせて **Cloud Backup Service** の料金に変更されています

バックアップファイルのサイズに基づいてネットアップに容量を支払う代わりに、バックアップ対象のソース ONTAP ボリュームの論理使用容量（ONTAP の効率化前）で計算された、保護対象のデータにのみ料金が発生します。この容量はフロントエンドテラバイト（FETB）とも呼ばれます。

## 2021 年 11 月 28 日



## EKS Kubernetes クラスタから Amazon S3 に永続ボリュームをバックアップできます

EKS クラスタに NetApp Astra Trident がインストールされていて、クラスタのバックエンドストレージとして Cloud Volumes ONTAP for AWS を使用している場合、Amazon S3 との間でボリュームをバックアップおよびリストアできます。"詳細については、[こちらをご覧ください](#)"。

## DP ボリュームのバックアップ機能が強化されました

Cloud Backup で、SVM-DR 関係のターゲット ONTAP システムに存在する DP ボリュームのバックアップの作成がサポートされるようになりました。いくつかの制限事項があります。を参照してください "[制限事項](#)" を参照してください。

## 2021 年 11 月 5 日

### オンプレミスの ONTAP システムにボリュームをリストアする際にプライベートエンドポイントを選択できます

Amazon S3 または Azure Blob にあるバックアップファイルからオンプレミスの ONTAP システムにボリュームをリストアする場合、オンプレミスシステムに接続するプライベートかつセキュアなプライベートエンドポイントを選択できるようになりました。

### 古いバックアップファイルを数日後にアーカイブストレージに階層化してコストを削減できるようになりました

クラスタで ONTAP 9.10.1 以降が実行されており、AWS または Azure クラウドストレージを使用している場合に、アーカイブストレージへのバックアップの階層化を有効にすることができます。詳細については、を参照してください "[AWS S3 アーカイブストレージクラス](#)" および "[Azure BLOB アーカイブアクセス層](#)"。

### Cloud Backup BYOL ライセンスが、Digital Wallet の Data Services Licenses タブに移動しました

Cloud Backup の BYOL ライセンスが、Cloud Manager Digital Wallet の Cloud Backup Licenses タブから Data Services Licenses タブに移動しました。

## 2021 年 10 月 4 日

### ボリュームまたはファイルのリストアを実行するときに、バックアップページでバックアップファイルのサイズを確認できるようになりました

これは、不要な大容量のバックアップファイルを削除する場合や、バックアップファイルのサイズを比較して、悪意のあるソフトウェア攻撃の結果として発生する可能性のある異常なバックアップファイルを特定する場合に便利です。

### クラウドバックアップのコストを比較するための TCO 計算ツールが用意されています

総所有コスト計算ツールを使用すると、Cloud Backup の総所有コストを把握し、これらのコストを従来のバックアップソリューションと比較して、削減可能なコストを見積もることができます。ご確認ください <https://cloud.netapp.com/cloud-backup-service-tco-calculator>["[こちらをご覧ください](#)"]。

## 作業環境に対する **Cloud Backup** の登録を解除する機能

これで、簡単に実現できます ["作業環境での Cloud Backup の登録を解除します"](#) その作業環境でバックアップ機能を使用しない（または課金される）場合。

## 2021 年 9 月 2 日

### ボリュームのオンデマンドバックアップを作成する機能

オンデマンドバックアップをいつでも作成して、ボリュームの現在の状態をキャプチャできるようになりました。これは、ボリュームに重要な変更が加えられており、次のスケジュールされたバックアップがそのデータを保護するのを待つ必要がない場合に便利です。

["オンデマンドバックアップの作成方法を参照してください"](#)。

### プライベートインターフェイス接続を定義して、**Amazon S3** へのセキュアなバックアップを実現できる

オンプレミスの ONTAP システムから Amazon S3 へのバックアップを設定する際に、アクティブ化ウィザードでプライベートインターフェイスエンドポイントへの接続を定義できるようになりました。これにより、オンプレミスシステムをプライベートかつセキュアに接続するネットワークインターフェイスを、AWS PrivateLink を基盤とするサービスに使用できるようになります。 ["このオプションの詳細を参照してください"](#)。

### **Amazon S3** にデータをバックアップする際に、お客様が管理する独自のキーをデータ暗号化用に選択できるようになりました

セキュリティと制御を強化するために、デフォルトの Amazon S3 暗号化キーを使用する代わりに、アクティブ化ウィザードでお客様が管理するデータ暗号化キーを選択できます。オンプレミスの ONTAP システムまたは AWS の Cloud Volumes ONTAP システムからバックアップを設定する場合に使用できます。

### **30、000** を超えるファイルを含むディレクトリからファイルをリストアできるようになりました

## 2021 年 8 月 1 日

### **Azure Blob** へのセキュアなバックアップを実現するためのプライベートエンドポイント接続を定義する機能

オンプレミスの ONTAP システムから Azure Blob へのバックアップを設定する場合は、アクティブ化ウィザードで Azure プライベートエンドポイントへの接続を定義できます。これにより、プライベートかつセキュアに Azure Private Link を搭載したサービスに接続するネットワークインターフェイスを使用できます。

### 毎時バックアップポリシーがサポートされるようになりました

この新しいポリシーは、既存の Daily、Weekly、および Monthly ポリシーに追加されています。毎時バックアップポリシーは、最小限の目標復旧時点（RPO）を提供します。

## 2021 年 7 月 7 日

これで、さまざまなアカウントとリージョンを使用してバックアップを作成できるようになりました

Cloud Backup で、Cloud Volumes ONTAP システムに使用するアカウントやサブスクリプションとは異なるものを使用してバックアップを作成できるようになりました。Cloud Volumes ONTAP システムの導入リージョンとは異なるリージョンにバックアップファイルを作成することもできます。

この機能は、AWS または Azure を使用している場合にのみ使用できます。既存の作業環境でバックアップを有効にする場合にのみ使用できます。新しい Cloud Volumes ONTAP 作業環境を作成する場合は使用できません。

**Azure Blob** にデータをバックアップする際のデータ暗号化に使用する、お客様が管理する独自のキーを選択できるようになりました

セキュリティと制御を強化するために、Microsoft が管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで、お客様が管理する独自のキーを選択してデータを暗号化できます。オンプレミスの ONTAP システムまたは Azure の Cloud Volumes ONTAP システムからバックアップを設定する場合に使用できます。

単一ファイルのリストアを使用する場合、一度に最大 **100** 個のファイルをリストアできるようになりました

## 2021 年 6 月 7 日

**ONTAP 9.8** 以降を使用している場合は、**DP** ボリュームの制限が解除されました

データ保護（DP）ボリュームのバックアップに関する 2 つの既知の制限事項が解決されました。

- ・カスケードバックアップは、SnapMirror 関係のタイプがミラーバックアップまたはバックアップの場合にのみ機能します。関係のタイプが MirrorAllSnapshots の場合は、バックアップを作成できるようになりました。
- ・Cloud Backup で、SnapMirror ポリシーに設定されているかぎり、バックアップに任意のラベルを使用できるようになりました。名前が daily、weekly、または monthly のラベルを要求するという制限はなくなりました。

## 2021 年 5 月 5 日

オンプレミスのクラスタデータを **Google Cloud Storage** または **NetApp StorageGRID** システムにバックアップ

オンプレミスの ONTAP システムから Google Cloud Storage や NetApp StorageGRID システムへのバックアップを作成できるようになりました。を参照してください ["Google Cloud Storage へのバックアップ"](#) および ["StorageGRID にバックアップしています"](#) を参照してください。

## System Manager を使用して Cloud Backup の処理を実行できるようになりました

ONTAP 9.9.1 の新機能では、System Manager を使用して、オンプレミスの ONTAP のバックアップを Cloud Backup で設定したオブジェクトストレージに送信できます。"[Cloud Backup を使用してボリュームをクラウドにバックアップする方法については、System Manager の説明を参照してください。](#)"

## いくつかの機能拡張により、バックアップポリシーが改善されました

- 次に、日単位、週単位、月単位のバックアップを組み合わせたカスタムポリシーを作成します。
- バックアップポリシーを変更すると、元のバックアップポリシーを使用してすべてのボリュームに環境のすべての新しいバックアップ \* および \* が変更されます。これまでは、新しいボリュームバックアップにのみ適用されていました。

## その他のバックアップおよびリストアの改善

- バックアップファイルのクラウドのデスティネーションを設定する際に、Cloud Volumes ONTAP システムが配置されているリージョンとは異なるリージョンを選択できるようになりました。
- 単一のボリュームに作成できるバックアップファイルの数が 1、019 から 4、000 に増えました。
- 1 つのボリュームのすべてのバックアップファイルを先に削除できるようになったほか、ボリュームのバックアップファイルを 1 つだけ削除したり、作業環境全体のバックアップファイルを必要に応じてすべて削除したりできるようになりました。

# はじめに

## Cloud Backup の詳細をご確認ください

Cloud Backup は、Cloud Manager 作業環境向けのサービスで、データを保護し、長期間アーカイブするためのバックアップおよびリストア機能を提供します。バックアップは自動的に生成され、パブリックまたはプライベートクラウドアカウントのオブジェクトストアに格納されます。

必要に応じて、バックアップから同じ作業環境または別の作業環境に全面的に `_ ボリューム _` をリストアできます。ONTAP データをバックアップする場合は、バックアップから同じ作業環境または別の作業環境に 1 つ以上の `_ ファイル _` をリストアすることもできます。

"Cloud Backup の詳細については、こちらをご覧ください"。

バックアップとリストアは、次の目的で使用できます。

- Cloud Volumes ONTAP システムとオンプレミスの ONTAP システムから ONTAP ボリュームをバックアップおよびリストア "詳細な機能については、こちらをご覧ください"。
- Kubernetes の永続ボリュームのバックアップとリストア "詳細な機能については、こちらをご覧ください"。
- クラウドバックアップアプリケーションを使用して、アプリケーションと整合性のある Snapshot をオンプレミスの ONTAP からクラウドにバックアップできます。"詳細な機能については、こちらをご覧ください"。
- Cloud Backup for VMwareを使用して、データストアをクラウドにバックアップし、仮想マシンをオンプレミスのvCenterにリストアします。"詳細な機能については、こちらをご覧ください"。



Cloud Manager Connectorをクラウドの政府機関のリージョンまたはインターネットにアクセスできないサイト（ダークサイト）に導入した場合、Cloud BackupではONTAP システムからのバックアップとリストアの処理のみがサポートされます。これらの代替導入方法を使用する場合、Cloud BackupはKubernetesクラスタ、アプリケーション、または仮想マシンからのバックアップとリストアの処理をサポートしません。

## Cloud Backup の仕組み

Cloud Volumes ONTAP またはオンプレミスの ONTAP システムでクラウドバックアップを有効にすると、サービスはデータのフルバックアップを実行します。ボリューム Snapshot はバックアップイメージに含まれません。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。

ほとんどの場合、すべてのバックアップ処理に Cloud Manager UI を使用します。ただし、ONTAP 9.9.1 以降では、ONTAP System Manager を使用して、オンプレミスの ONTAP クラスタのボリュームバックアップ処理を開始できます。"Cloud Backup を使用してボリュームをクラウドにバックアップする方法については、System Manager の説明を参照してください。"

次の図は、各コンポーネント間の関係を示しています。



## バックアップの保管場所バックアップノバショ

バックアップコピーは、Cloud Manager がクラウドアカウントで作成するオブジェクトストアに格納されます。クラスター / 作業環境ごとに 1 つのオブジェクトストアがあり、Cloud Manager は「NetApp-backup-clusteruuid」のようにオブジェクトストアに名前を付けます。このオブジェクトストアは削除しないでください。

- Azure では、Cloud Manager は BLOB コンテナのストレージアカウントを持つ新規または既存のリソースグループを使用します。クラウドマネージャ **"BLOB データへのパブリックアクセスをブロックします"** デフォルトでは
- StorageGRID では、Cloud Manager はオブジェクトストアバケットに既存のストレージアカウントを使用します。

## バックアップは午前 0 時に作成されます

- 毎時バックアップは、毎時 5 分に開始されます。
- 日次バックアップは、毎日午前 0 時を過ぎた直後に開始されます。
- 週次バックアップは、日曜日の朝の午前 0 時を過ぎた直後に開始されます
- 月単位のバックアップは、毎月 1 日の午前 0 時を過ぎた直後に開始されます。

開始時間は、各ソース ONTAP システムで設定されているタイムゾーンに基づきます。ユーザーが指定した時



間に、UI からバックアップ操作をスケジュールすることはできません。詳細については、システムエンジニアにお問い合わせください。

バックアップコピーはネットアップアカウントに関連付けられています

バックアップコピーには関連付けられます **"ネットアップアカウント"** コネクタがある場所。

同じネットアップアカウントに複数のコネクタがある場合は、各コネクタに同じバックアップリストが表示されます。バックアップには、Cloud Volumes ONTAP インスタンスとオンプレミスの ONTAP インスタンスに関連付けられたバックアップが含まれます。

## Cloud Backup のライセンスをセットアップします

クラウドバックアップのライセンスを取得するには、クラウドプロバイダから従量課金制（PAYGO）のマーケットプレイスサブスクリプションを購入するか、ネットアップからお客様所有のライセンスを使用（BYOL）を購入します。作業環境でCloud Backupをアクティブ化し、本番環境のデータのバックアップを作成し、本番環境のシステムにバックアップデータをリストアするには、有効なライセンスが必要です。

さらに読む前に、いくつかのメモを記入してください。

- クラウドプロバイダの Cloud Volumes ONTAP システム市場で Cloud Manager の従量課金制（PAYGO）サブスクリプションにすでに登録している場合は、Cloud Backup にも自動的に登録されます。再度登録する必要はありません。
- Cloud Backup Bring Your Own License（BYOL；お客様所有のライセンス）は、Cloud Manager アカウントに関連付けられたすべてのシステムで使用できるフローティングライセンスです。したがって、既存のBYOLライセンスで使用できるバックアップ容量が十分にある場合、別のBYOLライセンスを購入する必要はありません。
- オンプレミスの ONTAP データを StorageGRID にバックアップする場合は、BYOL ライセンスが必要ですが、クラウドプロバイダのストレージスペースは無償です。

**"Cloud Backupの使用に関連するコストの詳細については、こちらをご覧ください。"**

### 30 日間の無償トライアルをご利用いただけます

クラウド・バックアップの30日間無料トライアルは、クラウド・プロバイダーのマーケットプレイスで従量課金制サブスクリプションから利用できます。無料トライアルは、マーケットプレイスのリストに登録した時点から開始されます。Cloud Volumes ONTAP システムの導入時にマーケットプレイスサブスクリプションの料金を支払い、クラウドバックアップの無償トライアルを10日後に開始した場合は、20日後に無償トライアルを利用できます。

無償トライアルが終了すると、自動的にPAYGOサブスクリプションに切り替えられます。Cloud Backupを引き続き使用しない場合は、のみを使用してください **"作業環境からCloud Backupの登録を解除します"** トライアルが終了する前に、請求は行われません。

### Cloud Backup 従量課金制を使用

従量課金制の場合、クラウドプロバイダにオブジェクトストレージのコストとネットアップのバックアップライセンスのコストを1時間単位で支払うことになります。無償トライアルを利用されている場合や、お客様が

独自のライセンスを使用（BYOL）されている場合も、サブスクリプションを設定する必要があります。

- 登録すると、無料トライアルの終了後にサービスが中断されることがなくなります。試用期間が終了すると、バックアップしたデータの量に応じて1時間ごとに課金されます。
- BYOL ライセンスで許可されている数を超えるデータをバックアップした場合、データバックアップは従量課金制サブスクリプションを使用して続行されます。たとえば、BYOL ライセンスが 10TiB の場合、10TiB を超える容量はすべて PAYGO サブスクリプションによって課金されます。

お客様は、無料トライアル期間中、または BYOL ライセンスを超えていない場合は、従量課金制サブスクリプションから料金を請求されることはありません。

Cloud Backupについては、次の2種類のPAYGOを計画しています。

- Cloud Volumes ONTAP データとオンプレミスのONTAP データをバックアップできる「クラウドバックアップ」パッケージ。
- Cloud Volumes ONTAP とクラウドバックアップをバンドルできる「CVO Professional」パッケージ。これには、このライセンスに基づいて Cloud Volumes ONTAP ボリュームのバックアップが無制限になることも含まれます（バックアップ容量はライセンスにはカウントされません）。このオプションでは、オンプレミスの ONTAP データをバックアップすることはできません。ifdef: Azure []

以下のリンクから、クラウドプロバイダのマーケットプレイスから Cloud Backup にサブスクライブできます。

- Azure ["価格の詳細については、Cloud Manager Marketplace のサービスを参照してください"](#)。

## Cloud Backup BYOL ライセンスを使用する

ネットアップが提供するお客様所有のライセンスには、1年、2年、3年の期間があります。バックアップ対象のソース ONTAP ボリュームの論理使用容量（\_Before\_any 効率化）で計算され、保護するデータに対してのみ料金が発生します。この容量はフロントエンドテラバイト（FETB）とも呼ばれます。

BYOL Cloud Backup ライセンスは、Cloud Manager アカウントに関連付けられたすべてのシステムで合計容量が共有されるフローティングライセンスです。ONTAP システムでは、バックアップするボリュームに対してCLIコマンド「volume show-space logical-used」を実行することで、必要な容量を概算できます。

Cloud Backup BYOL ライセンスがない場合は、Cloud Manager の右下にあるチャットアイコンをクリックしてライセンスを購入してください。

必要に応じて、使用しない 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、ドル同等かつ同じ有効期限で Cloud Backup ライセンスに変換できます。["詳細については、こちらをご覧ください"](#)。

BYOLライセンスを管理するには、Cloud ManagerのDigital Walletページを使用します。新しいライセンスの追加、既存のライセンスの更新、およびDigital Walletからのライセンスステータスの表示を行うことができます。

### Cloud Backup ライセンスファイルを取得します

Cloud Backupライセンスを購入したあと、Cloud Managerでライセンスをアクティブ化するには、Cloud Backupのシリアル番号とNSSアカウントを入力するか、NLFライセンスファイルをアップロードします。次の手順は、NLF ライセンスファイルを取得する方法を示しています。



インターネットにアクセスできないオンプレミスサイトで Cloud Backup を実行している場合は、オフラインのオンプレミスサイトのホストに Cloud Manager Connector を導入しているため、インターネットに接続されたシステムからライセンスファイルを取得する必要があります。シリアル番号と NSS アカウントを使用してライセンスをアクティブ化することは、オフライン（ダークサイト）でのインストールには利用できません。

#### 手順

1. にサインインします "ネットアップサポートサイト" [ システム ]、[ ソフトウェアライセンス ] の順にクリックします。
2. Cloud Backup ライセンスのシリアル番号を入力します。

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		CLOUD_BKP_SERVICE	Get NetApp License File		100	12/31/9998

3. [\* License Key] 列で、[\* Get NetApp License File\*] をクリックします。
4. Cloud Manager アカウント ID（サポートサイトではテナント ID と呼ばれます）を入力し、\* Submit \* をクリックしてライセンスファイルをダウンロードします。

**Get License**

SERIAL NUMBER: 4810

LICENSE: CLOUD\_BKP\_SERVICE

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

Cloud Manager アカウント ID は、Cloud Manager の上部にある「\* Account \*」ドロップダウンを選択し、アカウントの横にある「\* Manage Account \*」をクリックすると確認できます。アカウント ID は、[ 概要 ] タブにあります。

#### Cloud Backup BYOL ライセンスをアカウントに追加します

ネットアップアカウント用の Cloud Backup ライセンスを購入したら、Cloud Manager にライセンスを追加する必要があります。

#### 手順

1. [ すべてのサービス ]、[ デジタルウォレット ]、[ データサービスライセンス ] の順にクリックします。

2. [ ライセンスの追加 ] をクリックします。

3. ライセンスの追加 ダイアログで、ライセンス情報を入力し、\* ライセンスの追加 \* をクリックします。

- バックアップライセンスのシリアル番号があり、NSS アカウントを知っている場合は、\* シリアル番号を入力 \* オプションを選択してその情報を入力します。

お使いのネットアップサポートサイトのアカウントがドロップダウンリストにない場合は、"[NSS アカウントを Cloud Manager に追加します](#)"。

- バックアップライセンスファイル（ダークサイトにインストールする場合に必要な）がある場合は、\* ライセンスファイルのアップロード \* オプションを選択し、プロンプトに従ってファイルを添付します。

**Add Cloud Backup License**

A Backup License must be installed with an active subscription. A Backup license enables you to use Cloud Backup for a certain period of time and for a maximum amount of backup space.

☒ Enter Serial Number    ☐ Upload License File

Serial Number

Enter Serial Number

NetApp Support Site Account

Select Support Site Account

**Add Backup License**    Cancel

☐ Enter Serial Number    ☒ Upload License File

To install a license, follow these instructions:

- 1 Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- 2 Click Upload File and then select the file.

Upload License File

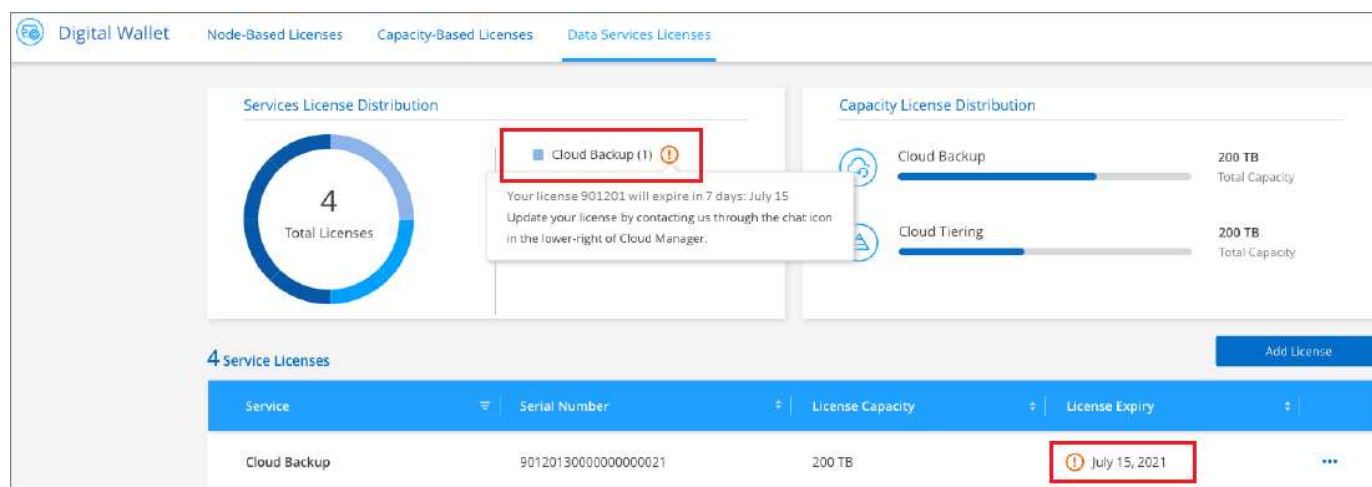
Upload License File    **Upload**

**Add Backup License**    Cancel

Cloud Manager でライセンスが追加されて、Cloud Backup がアクティブになります。

### Cloud Backup BYOL ライセンスを更新する

ライセンスで許可されている期間が終了期限に近づいている場合や、ライセンスで許可されている容量が上限に達している場合は、バックアップ UI に通知されます。このステータスは、[ デジタルウォレット ] ページ およびにも表示されます **"通知"**。



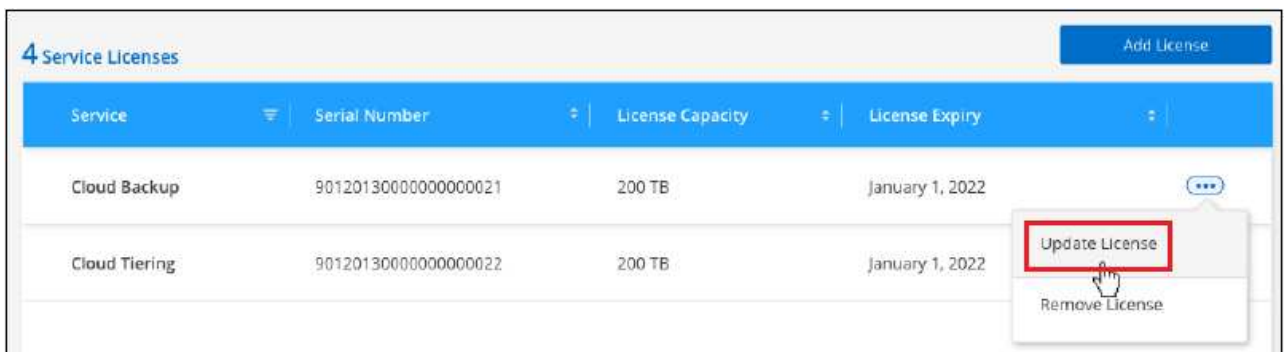
Cloud Backup のライセンスは有効期限が切れる前に更新できるため、データのバックアップとリストアを中断することなく実行できます。

#### 手順

1. Cloud Manager の右下にあるチャットアイコンをクリックするか、サポートにお問い合わせください。特定のシリアル番号について Cloud Backup ライセンスの期間延長または容量の追加を申請することができます。

ライセンスの支払いが完了し、ネットアップサポートサイトに登録されると、Cloud Manager はデジタルウォレットとデータサービスのライセンスページのライセンスを自動的に更新し、5 分から 10 分で変更が反映されます。

2. Cloud Manager がライセンスを自動更新できない場合（ダークサイトにインストールした場合など）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。
  - a. 可能です [ライセンスファイルをネットアップサポートサイトから入手します](#)。
  - b. [ デジタルウォレット ] ページの [ データサービスライセンス ] タブで、をクリックします ... アイコン"] 更新するサービスシリアル番号の場合は、 [ \* ライセンスの更新 \* ] をクリックします。



ボタンを選択するスクリーンショット。"]

- c. \_Update License\_page で、ライセンスファイルをアップロードし、 \* ライセンスの更新 \* をクリックします。

Cloud Manager によってライセンスが更新され、Cloud Backup は引き続きアクティブになります。

#### BYOL ライセンスに関する考慮事項

Cloud Backup BYOL ライセンスを使用している場合、バックアップするすべてのデータのサイズが容量の上限に近づいているかライセンスの有効期限に近づいているときに、Cloud Manager のユーザインターフェイスに警告が表示されます。次の警告が表示されます。

- バックアップがライセンスで許可された容量の 80% に達したとき、および制限に達したときに再度実行されます
- 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あとに再度有効になります

Cloud Manager インターフェイスの右下にあるチャットアイコンを使用して、警告が表示されたときにライセンスを更新してください。

BYOLライセンスの期限が切れると、次の2つのことが起こります。

- 使用しているアカウントにマーケットプレイスアカウントがある場合、バックアップサービスは引き続き

実行されますが、PAYGO ライセンスモデルに移行します。バックアップに使用されている容量に基づいて料金が発生します。

- 使用しているアカウントにMarketplaceアカウントがない場合、バックアップサービスは引き続き実行されますが、警告は引き続き表示されます。

BYOL サブスクリプションを更新すると、Cloud Manager によってライセンスが自動的に更新されます。Cloud Manager がセキュア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（ダークサイトにインストールされている場合など）は、手動でファイルを入手して Cloud Manager にアップロードできます。手順については、を参照してください ["Cloud Backup ライセンスを更新する方法"](#)。

PAYGO ライセンスに切り替えられたシステムは、自動的に BYOL ライセンスに戻されます。ライセンスなしで実行されていたシステムでは、警告が表示されなくなります。

# ONTAP データのバックアップとリストア

## Cloud Backup を使用して ONTAP クラスタのデータを保護します

Cloud Backup は、ONTAP クラスタデータを保護し、長期アーカイブするためのバックアップおよびリストア機能を提供します。バックアップは、ほぼ期間のリカバリやクローニングに使用されるボリューム Snapshot コピーとは関係なく、パブリックまたはプライベートのクラウドアカウントのオブジェクトストアに自動的に生成されて格納されます。

必要に応じて、バックアップから同じ作業環境または別の作業環境に、`volume_` 全体または 1 つ以上の `files` をリストアできます。

### の機能

バックアップ機能：

- データボリュームの独立したコピーを低コストのオブジェクトストレージにバックアップできます。
- クラスタ内のすべてのボリュームに単一のバックアップポリシーを適用するか、または一意のリカバリポイント目標が設定されたボリュームに異なるバックアップポリシーを割り当てます。
- 古いバックアップファイルをアーカイブストレージに階層化してコストを削減（ONTAP 9.10.1以降でサポート）
- クラウドからクラウドへ、オンプレミスシステムからパブリッククラウドやプライベートクラウドへバックアップできます。
- Cloud Volumes ONTAP システムの場合、バックアップは別のサブスクリプションやアカウントに配置することも、別のリージョンに配置することもできます。
- バックアップデータは、転送中の AES-256 ビット暗号化と TLS 1.2 HTTPS 接続によって保護されます。
- クラウドプロバイダのデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを使用してデータを暗号化します。
- 単一ボリュームで最大 4、000 個のバックアップがサポートされます。

リストア機能：

- 特定の時点からデータをリストアします。
- ボリュームまたは個々のファイルをソースシステムまたは別のシステムにリストアする。
- 別のサブスクリプション / アカウントを使用して、または別のリージョンにある作業環境にデータをリストアする。
- 元の ACL を維持したまま、指定した場所にデータを直接配置して、ブロックレベルでデータをリストアします。
- 単一ファイルのリストア用に個々のファイルを選択するための、参照可能および検索可能なファイルカタログ。

## サポート対象の **ONTAP** 作業環境およびオブジェクトストレージプロバイダ

Cloud Backup を使用すると、以下の作業環境から次のパブリックおよびプライベートクラウドプロバイダのオブジェクトストレージに ONTAP ボリュームをバックアップできます。

ソースの作業環境	バックアップファイルデスティネーション <code>ifdef : aws []</code>
AWS の Cloud Volumes ONTAP	Amazon S3 <code>endif : aws []ifdef : azure[]</code>
Azure の Cloud Volumes ONTAP	Azure Blob <code>endif : Azure[] ifdef : GCP []</code>
Google の Cloud Volumes ONTAP	Google Cloud Storage <code>endif : GCP []</code>
オンプレミスの ONTAP システム	<code>ifdef : aws [] Amazon S3 endif : aws [] ifdef : azure[] Azure Blob endif : azure [] ifdef : gcp [] Google Cloud Storage endif : GCP [] NetApp StorageGRID</code>

ONTAP バックアップファイルから次の作業環境にボリュームまたは個々のファイルをリストアできます。

バックアップファイル	デスティネーションの作業環境	
* 場所 *	* ボリュームの復元 *	ファイルのリストア <code>ifdef : aws []</code>
Amazon S3	オンプレミスの AWS ONTAP システムに Cloud Volumes ONTAP が導入されている	AWSオンプレミスONTAP システムのCloud Volumes ONTAP 。 <code>endif : aws [] ifdef : azure[]</code>
Azure Blob の略	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入	AzureオンプレミスONTAP システムのCloud Volumes ONTAP 。 <code>endif : azure[] ifdef : gCP[]</code>
Google クラウドストレージ	Google オンプレミス ONTAP システムの Cloud Volumes ONTAP	GoogleオンプレミスONTAP システムのCloud Volumes ONTAP : <code>GCP[]</code>
NetApp StorageGRID	オンプレミスの ONTAP システム	オンプレミスの ONTAP システム

「オンプレミス ONTAP システム」とは、FAS、AFF、ONTAP Select の各システムを指します。

インターネットに接続されていないサイトをサポート

インターネットに接続されていないサイト（「オフライン」または「ダーク」サイトとも呼ばれる）で Cloud Backup を使用して、ローカルのオンプレミス ONTAP システムからローカルの NetApp StorageGRID システムにボリュームデータをバックアップできます。この場合は、ダークサイトに Cloud Manager Connector（バージョン 3.9.19 以上）を導入する必要があります。を参照してください ["オンプレミスの ONTAP データの StorageGRID へのバックアップ"](#) を参照してください。

## コスト

ONTAP システムでクラウドバックアップを使用する場合、リソース料金とサービス料金の 2 種類のコストが発生します。

- リソース料金 \*

リソースの料金は、オブジェクトストレージの容量とクラウドでの仮想マシン / インスタンスの実行についてクラウドプロバイダに支払います。

- バックアップでは、クラウドプロバイダにオブジェクトストレージのコストを支払います。

クラウドバックアップではソースボリュームの Storage Efficiency が保持されるため、クラウドプロバイダ側で、data\_after\_ONTAP 効率化のコストを支払います（重複排除と圧縮が適用されたあとのデータ量が少ないほど）。

- 検索とリストアを使用したボリュームまたはファイルのリストアでは、特定のリソースがクラウドプロバイダによってプロビジョニングされ、検索要求でスキャンされるデータ量には1TiBあたりのコストが関連付けられます。
- アーカイブストレージに移動されたバックアップファイルからボリュームデータをリストアする必要がある場合は、GiB単位の読み出し料金とクラウドプロバイダからの要求ごとの料金が別途かかります。
- サービス料金 \*

サービス料金はネットアップに支払われ、バックアップの作成時とリストア時のボリューム、またはファイルに対する費用の両方が含まれます。保護するデータの料金は、オブジェクトストレージにバックアップされる ONTAP のソースの使用済み論理容量（\_Before\_ONTAP 効率化）で計算されます。この容量はフロントエンドテラバイト（FETB）とも呼ばれます。

バックアップサービスの料金を支払う方法は 3 通りあります。1 つ目は、クラウドプロバイダを利用して月額料金を支払う方法です。2 つ目のオプションは、年間契約を取得することです。3 つ目のオプションは、ネットアップからライセンスを直接購入することです。を参照してください [ライセンス](#) 詳細については、を参照してください

## ライセンス

Cloud Backupには、いくつかのライセンスオプションがあります。

- 従量課金制（PAYGO）のサブスクリプション
- お客様所有のライセンスを使用（BYOL）

PAYGOサブスクリプションに最初に登録したときに、30日間の無償トライアルを利用できます。

### 従量課金制のサブスクリプション

Cloud Backup は従量課金制モデルで、使用量に応じたライセンスを提供します。クラウドプロバイダの市場に登録した後は、バックアップされたデータに対して GiB 単位で料金が発生します。つまり、前払いによる支払いが発生しません。クラウドプロバイダから月額料金で請求されます。

["従量課金制サブスクリプションの設定方法について説明します"](#)。

### お客様所有のライセンスを使用

BYOL は期間ベース（12 カ月、24 カ月、36 カ月）の \_ 容量ベースであり、1TiB 単位で提供されます。ネットアップに料金を支払って、1 年分のサービスを使用し、最大容量を指定した場合は「10TiB」とします。

サービスを有効にするために、Cloud Manager のデジタルウォレットのページに入力したシリアル番号が表示されます。いずれかの制限に達すると、ライセンスを更新する必要があります。Backup BYOL ライセンス環境では、に関連付けられているすべてのソースシステムがライセンスされます ["Cloud Manager アカウント"](#)。



"BYOL ライセンスの管理方法について説明します"。

## Cloud Backup の仕組み

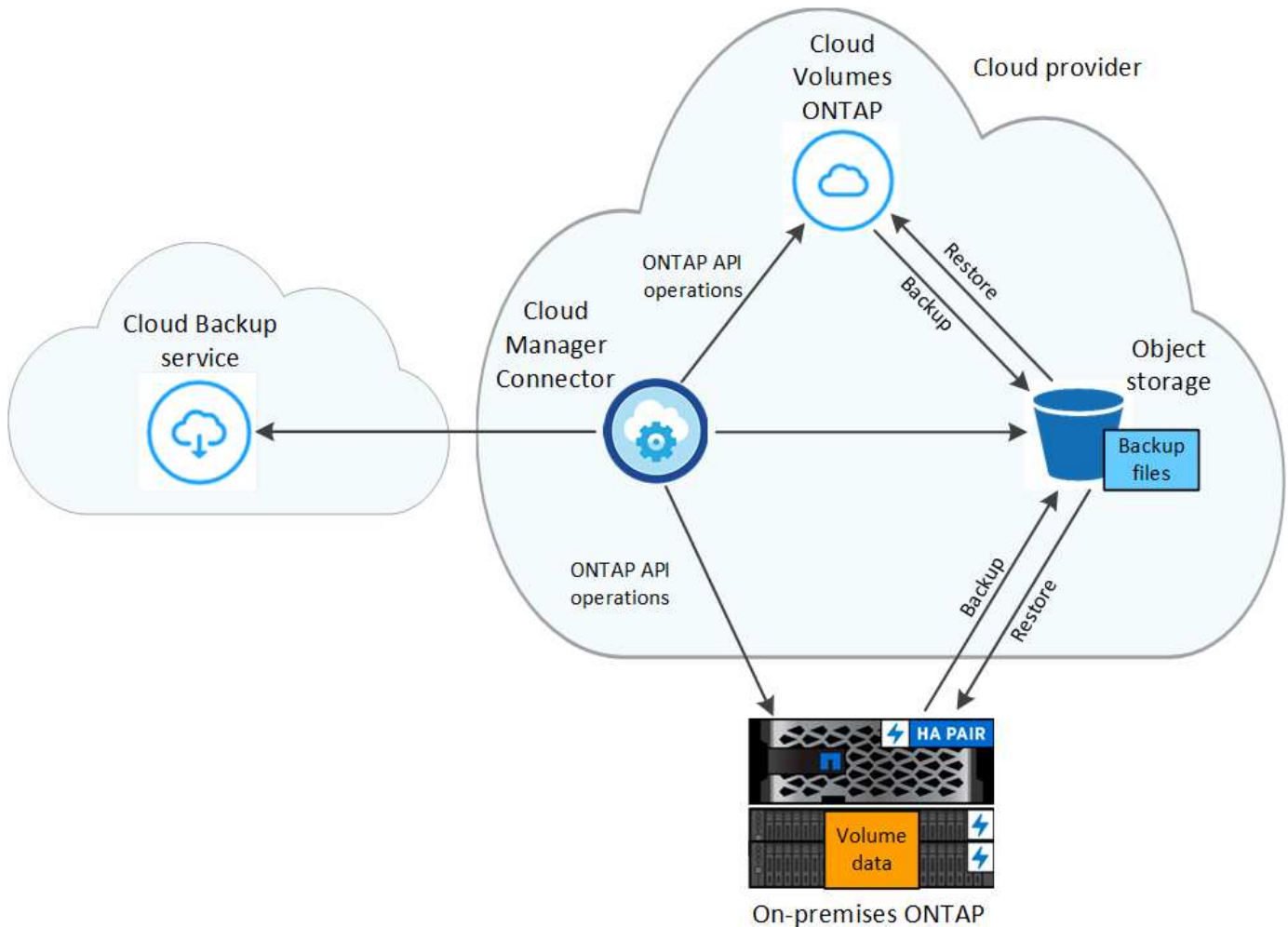
Cloud Volumes ONTAP またはオンプレミスの ONTAP システムでクラウドバックアップを有効にすると、サービスはデータのフルバックアップを実行します。ボリューム Snapshot はバックアップイメージに含まれません。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。

ほとんどの場合、すべてのバックアップ処理に Cloud Manager UI を使用します。ただし、ONTAP 9.9.1 以降では、ONTAP System Manager を使用して、オンプレミスの ONTAP クラスターのボリュームバックアップ処理を開始できます。"[Cloud Backup を使用してボリュームをクラウドにバックアップする方法については、System Manager の説明を参照してください。](#)"



クラウドプロバイダ環境からバックアップファイルの管理や変更を直接行くと、ファイルが破損してサポートされない構成になる可能性があります。

次の図は、各コンポーネント間の関係を示しています。





## バックアップの保管場所バックアップノバシヨ

バックアップコピーは、Cloud Manager がクラウドアカウントで作成するオブジェクトストアに格納されます。クラスタ / 作業環境ごとに 1 つのオブジェクトストアがあり、Cloud Manager は「NetApp-backup-clusteruuid」のようにオブジェクトストアに名前を付けます。このオブジェクトストアは削除しないでください。

- Azure では、Cloud Manager は BLOB コンテナのストレージアカウントを持つ新規または既存のリソースグループを使用します。クラウドマネージャ ["BLOB データへのパブリックアクセスをブロックします"](#) デフォルトでは
- StorageGRID では、Cloud Manager はオブジェクトストアバケットに既存のストレージアカウントを使用します。

あとでクラスタのデスティネーションオブジェクトストアを変更する場合は、が必要になります ["作業環境の Cloud Backup の登録を解除します"](#)をクリックし、新しいクラウドプロバイダ情報を使用して Cloud Backup を有効にします。

## サポートされるストレージクラスまたはアクセス階層

- Azure では、バックアップは \_COOL アクセス層に関連付けられます。

クラスタが ONTAP 9.10.1 以降を使用している場合は、特定の日数が経過した古いバックアップを Azure Archive\_storage に階層化して、コストをさらに最適化することができます。 ["Azure アーカイブストレージの詳細については、こちらをご覧ください"](#)。

- StorageGRID では、バックアップは \_Standard\_storage クラスに関連付けられます。

## クラスタごとにカスタマイズ可能なバックアップスケジュールと保持設定

作業環境で Cloud Backup を有効にすると、最初に選択したすべてのボリュームが、定義したデフォルトのバックアップポリシーを使用してバックアップされます。Recovery Point Objective（RPO；目標復旧時点）が異なるボリュームに対して異なるバックアップポリシーを割り当てる場合は、そのクラスタに追加のポリシーを作成し、そのポリシーを他のボリュームに割り当てることができます。

すべてのボリュームについて、毎時、毎日、毎週、および毎月のバックアップを組み合わせることで選択できます。また、システム定義のポリシーの中から、3 カ月、1 年、7 年のバックアップと保持を提供するポリシーを選択することもできます。ポリシーは次のとおりです。

バックアップポリシー名	間隔ごとのバックアップ ...			最大バックアップ
	* 毎日 *	* 毎週 *	* 毎月 *	
Netapp3MonthsRetention	30	13	3.	46
Netapp1YearRetention	30	13	12.	55
Netapp7YearsRetention	30	53	84	167

ONTAP System Manager または ONTAP CLI を使用してクラスタに作成したバックアップ保護ポリシーも選択内容として表示されます。

カテゴリまたは間隔のバックアップの最大数に達すると、古いバックアップは削除されるため、常に最新のバックアップが保持されます。

できることに注意してください ["ボリュームのオンデマンドバックアップを作成する"](#) スケジュールバックアップから作成されたバックアップファイルに加え、いつでも Backup Dashboard からアクセスできます。



データ保護ボリュームのバックアップの保持期間は、ソースの SnapMirror 関係の定義と同じです。API を使用して必要に応じてこの値を変更できます。

## FabricPool 階層化ポリシーに関する考慮事項

バックアップするボリュームが FabricPool アグリゲートに配置され、「none」以外のポリシーが割り当てられている場合に注意する必要がある点があります。

- FabricPool 階層化ボリュームの最初のバックアップでは、（オブジェクトストアからの）ローカルおよびすべての階層化データを読み取る必要があります。バックアップ処理では、オブジェクトストレージに階層化されたコールドデータは「再加熱」されません。

この処理を実行すると、クラウドプロバイダからデータを読み取るコストが 1 回だけ増加する可能性があります。

- 2 回目以降のバックアップは増分バックアップとなるため、影響はありません。
- ボリュームの作成時に階層化ポリシーが割り当てられていた場合、この問題は表示されません。
- ボリュームに「all」階層化ポリシーを割り当てる前に、バックアップの影響を考慮してください。データはすぐに階層化されるため、Cloud Backup はローカル階層からではなくクラウド階層からデータを読み取ります。バックアップの同時処理は、クラウドオブジェクトストレージへのネットワークリンクを共有するため、ネットワークリソースが最大限まで使用されなくなった場合にパフォーマンスが低下する可能性があります。この場合、複数のネットワークインターフェイス（LIF）をプロアクティブに設定して、この種類のネットワークの飽和を軽減することができます。

## サポートされるボリューム

Cloud Backup では、FlexVol の読み書き可能ボリュームと SnapMirror データ保護（DP）のデスティネーションボリュームがサポートされます。

FlexGroup ボリュームと SnapLock ボリュームは現在サポートされていません。

## 制限

- 古いバックアップファイルをアーカイブストレージに階層化するには、クラスタで ONTAP 9.10.1 以降が実行されている必要があります。アーカイブストレージにあるバックアップファイルからボリュームをリストアするには、デスティネーションクラスタで ONTAP 9.10.1 以降が実行されている必要もあります。
- ポリシーにボリュームが割り当てられていない場合にバックアップポリシーを作成または編集するときは、バックアップの保持数を 1018 以下にする必要があります。回避策では、ポリシーを作成するバックアップの数を減らすことができます。その後、ポリシーを編集して、ポリシーにボリュームを割り当てたあとで最大 4、000 個のバックアップを作成できます。
- データ保護（DP）ボリュームをバックアップする場合、次の SnapMirror ラベルが設定されている関係はクラウドにバックアップされません。
  - APP\_Consistent
  - all\_source\_snapshot
- SVM-DR ボリュームバックアップは、次の制限事項でサポートされます。

- バックアップは ONTAP セカンダリからのみサポートされます。
- ボリュームに適用される Snapshot ポリシーは、日単位、週単位、月単位など、クラウドバックアップで認識されるポリシーのいずれかである必要があります。デフォルトの「sm\_created」ポリシー（すべての Snapshot をミラー \* する場合に使用）が認識されず、バックアップ可能なボリュームのリストに DP ボリュームが表示されない。
- [今すぐバックアップ] ボタンを使用したアドホック・ボリューム・バックアップは 'データ保護ボリューム' ではありません。
- SM-BC 設定はサポートされません。
- MetroCluster（MCC）バックアップは、ONTAP セカンダリからのみサポートされます。  
MCC>SnapMirror > ONTAP > Cloud Backup > オブジェクトストレージ。
- ONTAP では、単一のボリュームから複数のオブジェクトストアへの SnapMirror 関係のファンアウトはサポートされていません。そのため、この構成は Cloud Backup ではサポートされていません。
- オブジェクトストアでの Worm/Compliance モードはサポートされません。

#### 単一ファイルのリストアに関する制限事項

これらの制限事項は、特に明記されていない限り、ファイルのリストアの検索とリストアおよび参照と復元の両方の方法に適用されます。

- ブラウズとリストアでは、一度に最大100個のファイルをリストアできます。
- 検索とリストアでは、一度に1つのファイルをリストアできます。
- 現在、フォルダ / ディレクトリのリストアはサポートされていません。
- リストアするファイルは、デスティネーションボリュームの言語と同じ言語を使用している必要があります。言語が異なる場合は、エラーメッセージが表示されます。
- 異なるサブネットにある異なる Cloud Manager で同じアカウントを使用する場合、ファイルレベルのリストアはサポートされません。
- バックアップファイルがアーカイブストレージにある場合は、個々のファイルをリストアできません。
- インターネットにアクセスできないサイト（ダークサイト）にコネクタがインストールされている場合は、検索とリストアを使用したファイルレベルのリストアはサポートされません。

## Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ

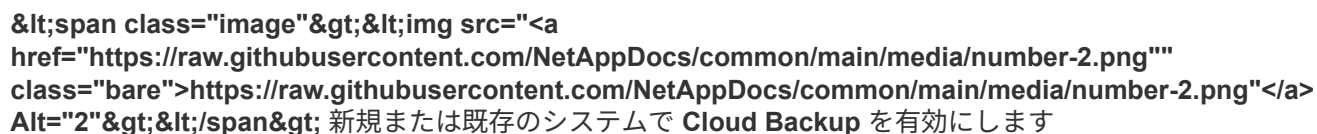
Cloud Volumes ONTAP から Azure Blob Storage へのデータのバックアップを開始するには、いくつかの手順を実行します。

### クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>  設定のサポートを確認します

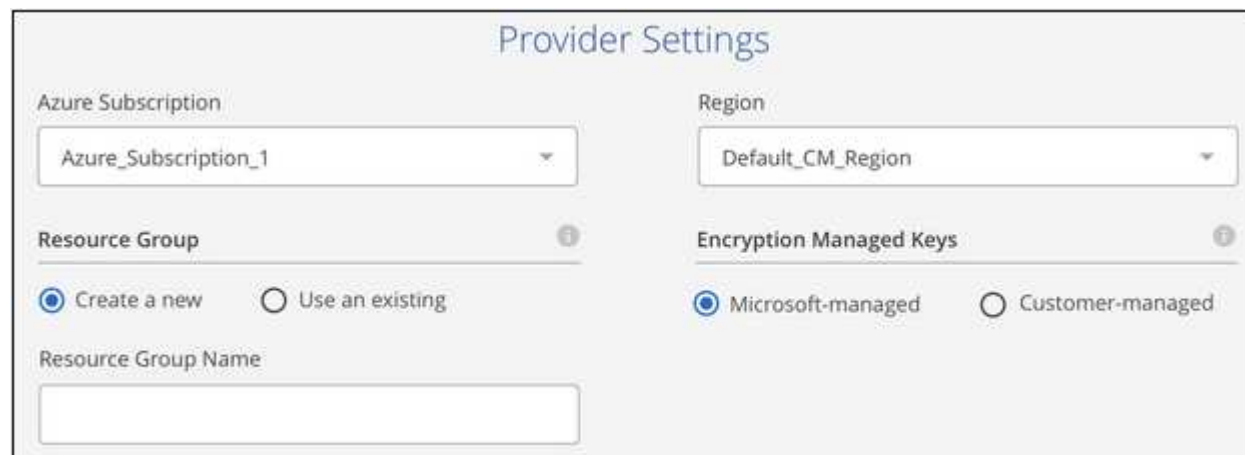
- Cloud Volumes ONTAP 9.7P5 以降を Azure で実行しています。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます ["Cloud Manager Marketplace のバックアップソリューション"](https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png)またはを購入したことが必要です ["アクティブ化されます"](https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png) NetApp の Cloud Backup BYOL ライセンス。

新規または既存のシステムで Cloud Backup を有効にします

- 新しいシステム：Cloud Backup は、作業環境ウィザードではデフォルトで有効になっています。このオプションは必ず有効にしておいてください。
- 既存のシステム：作業環境を選択し、右パネルのバックアップと復元サービスの横にある \* 有効化 \* をクリックして、セットアップウィザードに従います。



プロバイダのサブスクリプションとリージョンを選択し、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するかを選択します。また、Microsoft が管理するデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを選択してデータを暗号化することもできます。



デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

デフォルトでは、バックアップは Cool アクセス層に保存されます。クラスタが ONTAP 9.10.1 以降を使用している場合は、特定の日数が経過したあとに Azure Archive ストレージにバックアップを階層化してコストをさらに最適化することができます。

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

---

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data.  
Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)  Access Tier

---

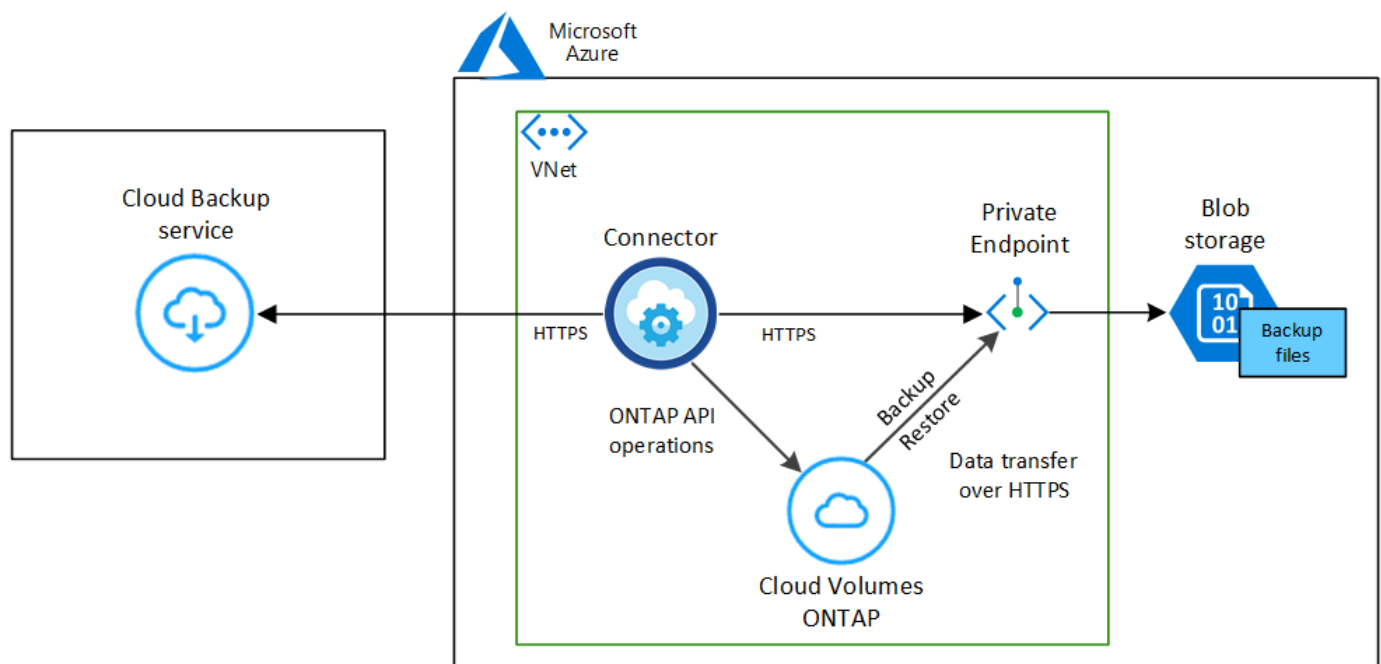
**Storage Account** Cloud Manager will create the storage account after you complete the wizard

Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを特定します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、あとから追加のポリシーを作成してボリュームに適用できます。

## 要件

Azure Blob Storage へのボリュームのバックアップを開始する前に、次の要件を確認し、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



## サポートされている ONTAP のバージョン

ONTAP 9.7P5以降が必要です。ONTAP 9.8P11以降が推奨されます。

## ライセンス要件

Cloud Backup 従量課金制のライセンスの場合は、Cloud Backup を有効にする前に Azure Marketplace でサブスクリプションを購入する必要があります。Cloud Backup の請求は、このサブスクリプションを通じて行われます。"[作業環境ウィザードの詳細 & 資格情報ページから購読できます](#)"。

Cloud Backup BYOL ライセンスを使用するには、ライセンスの期間と容量にサービスを使用できるように、ネットアップから提供されたシリアル番号が必要です。"[BYOL ライセンスの管理方法について説明します](#)"。

また、バックアップを格納するストレージスペースには、Microsoft Azure サブスクリプションが必要です。

## サポートされている Azure リージョン

Cloud Backup はすべての Azure リージョンでサポートされます "[Cloud Volumes ONTAP がサポートされている場合](#)" Azure Government リージョンを含む。

## データ暗号化にお客様が管理するキーを使用するために必要な情報

Microsoft が管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで、お客様が管理する独自のキーを使用してデータを暗号化できます。この場合、Azure サブスクリプション、キー・ボールド名、およびキーが必要です。"[独自のキーの使用方を参照してください](#)"。

## 新しいシステムでの Cloud Backup の有効化

Cloud Backup は、作業環境ウィザードではデフォルトで有効になっています。このオプションは必ず有効にしておいてください。

を参照してください "[Azure で Cloud Volumes ONTAP を起動します](#)" を Cloud Volumes ONTAP 参照してください。

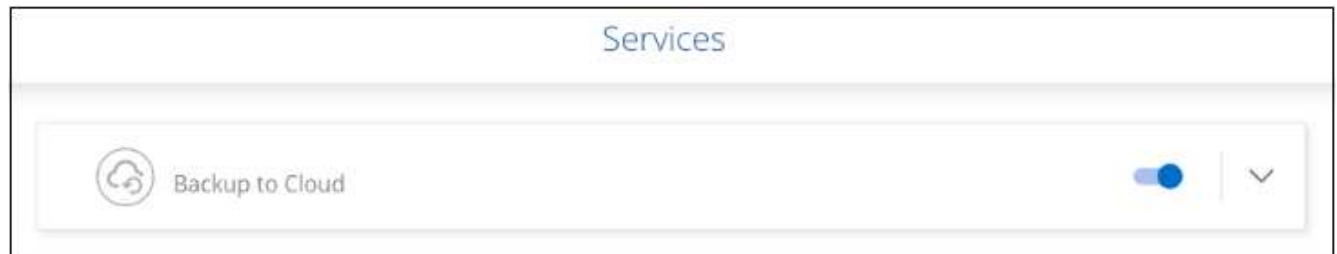


リソースグループの名前を選択する場合は、Cloud Volumes ONTAP を導入する際に \* disable \* Cloud Backup と入力します。の手順に従います [既存のシステムでの Cloud Backup の有効化](#) Cloud Backup を有効にしてリソースグループを選択します。

## 手順

1. [ Cloud Volumes ONTAP の作成 \* ] をクリックします。
2. クラウドプロバイダとして Microsoft Azure を選択し、シングルノードまたは HA システムを選択します。
3. Azure クレデンシャルの定義ページで、クレデンシャル名、クライアント ID、クライアントシークレット、およびディレクトリ ID を入力し、\* 続行 \* をクリックします。
4. 詳細とクレデンシャルページに必要事項を入力し、Azure Marketplace サブスクリプションが登録されていることを確認して、「\* Continue \*」をクリックします。
5. [ サービス ] ページで、サービスを有効のままにして、[\* 続行 ] をクリックします。





6. ウィザードの各ページを設定し、システムを導入します。

Cloud Backup はシステムで有効になり、ボリュームを毎日バックアップして、最新の 30 個のバックアップコピーを保持します。

可能です ["ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"](#)。また可能です ["ボリューム全体または個々のファイルをバックアップファイルからリストアする"](#) Azure 内の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムへの接続に使用できます。

## 既存のシステムでの **Cloud Backup** の有効化

作業環境から Cloud Backup をいつでも直接有効にできます。

### 手順

1. 作業環境を選択し、右パネルの [バックアップと復元] サービスの横にある [\*Enable] をクリックします。



2. プロバイダの詳細を選択し、\* 次へ \* :

- バックアップの格納に使用する Azure サブスクリプション。これは、Cloud Volumes ONTAP システムとは異なるサブスクリプションにすることもできます。
- バックアップを保存するリージョン。これは、Cloud Volumes ONTAP システムが配置されているリージョンとは異なるリージョンにすることもできます。
- BLOB コンテナを管理するリソースグループ - 新しいリソースグループを作成したり、既存のリソースグループを選択したりできます。
- Microsoft が管理するデフォルトの暗号化キーを使用する場合でも、お客様が管理する独自のキーを選択してデータの暗号化を管理する場合でも、(["独自のキーの使用方法を参照してください"](#))。

### Provider Settings

Azure Subscription

Azure\_Subscription\_1

Region

Default\_CM\_Region

Resource Group

☒ Create a new
☐ Use an existing

Resource Group Name

Encryption Managed Keys

☒ Microsoft-managed
☐ Customer-managed

3. デフォルトのバックアップポリシーの詳細を入力し、\* Next \* をクリックします。
- バックアップスケジュールを定義し、保持するバックアップの数を選択します。 ["選択可能な既存のポリシーのリストが表示されます"](#)。
  - ONTAP 9.10.1 以降を使用している場合は、特定の日数が経過したバックアップを Azure Archive ストレージに階層化して、コストをさらに最適化することができます。 ["アーカイブ階層の使用の詳細については、こちらをご覧ください"](#)。

### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	24	↑ ↓
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30	↑ ↓
<input type="checkbox"/> Weekly	Number of backups to retain	52	↑ ↓
<input type="checkbox"/> Monthly	Number of backups to retain	12	↑ ↓

---

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data.  
Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

30

Access Tier

Azure Archive

---

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

4. Select Volumes (ボリュームの選択) ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを選択します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、追加のポリシーを作成し、それらのボリュームにあとから適用できます。



Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy						

。すべてのボリュームをバックアップするには、タイトル行（☒ Volume Name）。

。個々のボリュームをバックアップするには、各ボリュームのボックス（☒ Volume\_1）。

5. 今後追加されるすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップ...」チェックボックスをオンのままにします。この設定を無効にした場合は、以降のボリュームのバックアップを手動で有効にする必要があります。

6. Activate Backup \* をクリックすると、選択した各ボリュームの初期バックアップの実行が開始されます。

Cloud Backup が起動し、選択した各ボリュームの初期バックアップの作成が開始されます。Volume Backup Dashboard が表示され、バックアップの状態を監視できます。

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"。また可能です "ボリューム全体または個々のファイルをバックアップファイルからリストアする" Azure 内の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムへの接続に使用できます。

## オンプレミスの ONTAP データを Azure BLOB ストレージにバックアップする

オンプレミスの ONTAP システムから Azure BLOB ストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

「オンプレミス ONTAP システム」には、FAS、AFF、ONTAP Select の各システムが含まれます。

### クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>  
Alt="one " 設定のサポートを確認します

- ・ オンプレミスクラスタを検出し、Cloud Manager の作業環境に追加しておきます。を参照してください

"ONTAP クラスタの検出" を参照してください。

- クラスタで ONTAP 9.7P5 以降が実行されています。
- クラスタには SnapMirror ライセンスがあります。このライセンスは、Premium Bundle または Data Protection Bundle に含まれています。
- クラスタは、BLOB ストレージとコネクタへの必要なネットワーク接続を備えている必要があります。
- コネクタは、BLOB ストレージとクラスタへの必要なネットワーク接続と、必要な権限を備えている必要があります。
- バックアップを配置するオブジェクトストレージスペース用の有効な Azure サブスクリプションが必要です。

作業環境を選択し、右パネルのバックアップと復元サービスの横にある \*Enable>Backup Volumes] をクリックして、セットアップ・ウィザードに従います。



ボタンを示すスクリーンショット"]

プロバイダとして Microsoft Azure を選択し、プロバイダの詳細を入力します。バックアップを作成する Azure サブスクリプションとリージョンを選択する必要があります。また、Microsoft が管理するデフォルトの暗号化キーを使用する代わりに、お客様が管理する独自のキーを選択してデータを暗号化することもできます。

ボリュームが配置されている ONTAP クラスタ内の IPspace を選択します。また、既存の Azure プライベートエンドポイントを使用して、オンプレミスのデータセンターから VNet へのよりセキュアな接続を実現することもできます。

The Networking configuration panel includes the following elements:

- IPspace:** A dropdown menu currently showing "IP\_Space\_1".
- Private Endpoint Configuration:** A toggle switch that is currently turned off.
- VNet:** A dropdown menu with the text "Select VNet".
- Subnet:** A dropdown menu with the text "Select Subnet".

デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

デフォルトでは、バックアップは Cool アクセス層に保存されます。クラスタが ONTAP 9.10.1 以降を使用している場合は、特定の日数が経過したあとに Azure Archive ストレージにバックアップを階層化してコストをさらに最適化することができます。

The Define Policy configuration panel includes the following sections:

- Policy - Retention & Schedule:**
  - Radio buttons for "Create a New Policy" (selected) and "Select an Existing Policy".
  - Four backup frequency options, each with a checkbox and a "Number of backups to retain" spinner:
    - ☐ Hourly (24)
    - ☒ Daily (30)
    - ☐ Weekly (52)
    - ☐ Monthly (12)
- Archival Policy:**
  - Text: "Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization."
  - ☒ Tier Backups to Archival
  - Archive after (Days): Input field with "30".
  - Access Tier: Dropdown menu showing "Azure Archive".
- Storage Account:**
  - Text: "Cloud Manager will create the storage account after you complete the wizard"

Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを特定します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、あとから追加のポリシーを作成してボリュームに適用できます。

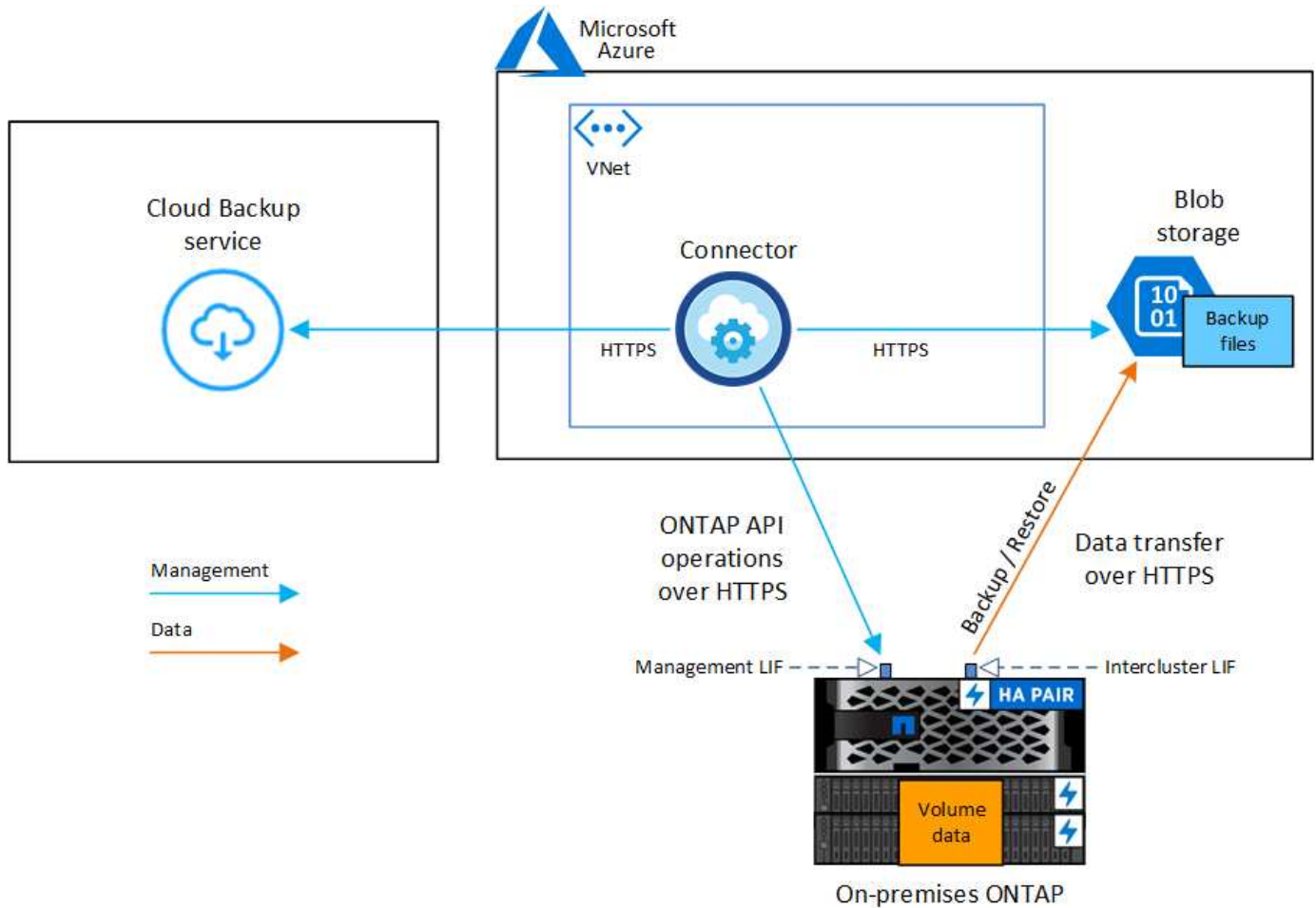
## 要件

オンプレミスボリュームを Azure BLOB ストレージにバックアップする前に、次の要件を読み、サポートされている構成であることを確認してください。

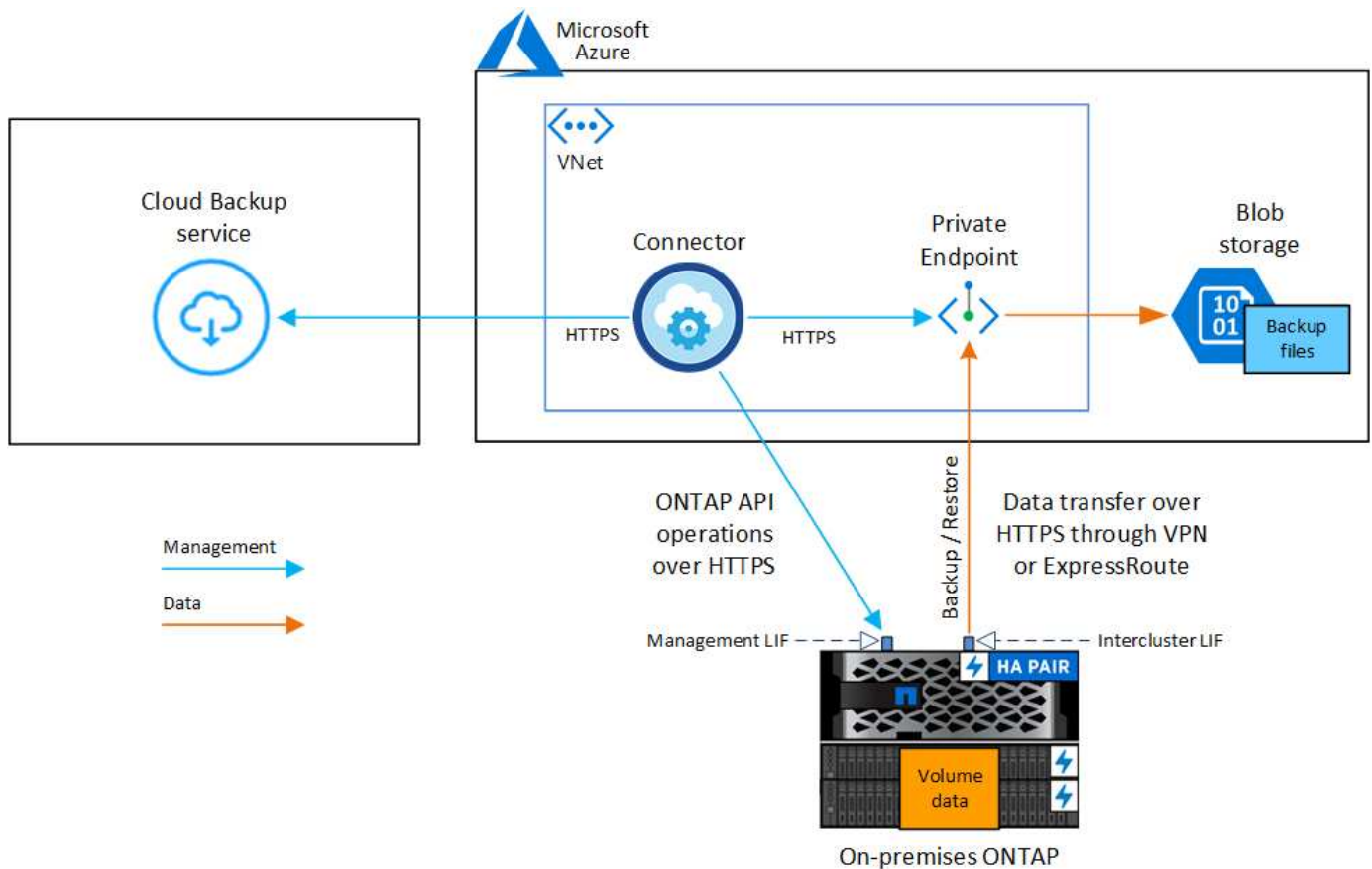
オンプレミスの ONTAP システムから Azure Blob へのバックアップを設定する場合は、2 つの接続方法を使用できます。

- パブリック接続 - パブリック Azure エンドポイントを使用して、ONTAP システムを Azure BLOB ストレージに直接接続します。
- プライベート接続 - VPN または ExpressRoute を使用し、プライベート IP アドレスを使用する vnet Private Endpoint を介してトラフィックをルーティングします。

次の図は、\*パブリック接続\*メソッドと、コンポーネント間の準備に必要な接続を示しています。



次の図は、\*プライベート接続\*メソッドと、コンポーネント間の準備に必要な接続を示しています。



## ONTAP クラスタの準備

ボリュームデータのバックアップを開始する前に、Cloud Manager でオンプレミスの ONTAP クラスタを検出する必要があります。

"[クラスタの検出方法について説明します](#)".

## ONTAP の要件

- ONTAP 9.7P5以降が必要です。ONTAP 9.8P11以降が推奨されます。
- SnapMirror ライセンス（Premium Bundle または Data Protection Bundle に含まれます）。
- 注：\* Cloud Backup を使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を参照してください "[クラスタライセンスを管理します](#)".

- 時間とタイムゾーンが正しく設定されている。

方法を参照してください "[クラスタ時間を設定します](#)".

## クラスタネットワークの要件

- ONTAP クラスタは、バックアップおよびリストア処理用に、クラスタ間 LIF から Azure Blob Storage へのポート 443 経由の HTTPS 接続を開始します。

ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。コネクタは Azure VNet 内に配置できます。
- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"[IPspace の詳細については、こちらをご覧ください](#)。

Cloud Backup をセットアップすると、IPspace で使用するように求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードとクラスタ間 LIF からオブジェクトストアにアクセスできます。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "[SVM 用に DNS サービスを設定](#)"。
- をデフォルトとは異なる IPspace を使用している場合は、オブジェクトストレージへのアクセスを取得するために静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新し、ONTAP からオブジェクトストレージへのポート 443 経由の Cloud Backup Service 接続と、ポート 53 （TCP / UDP）経由での Storage VM から DNS サーバへの名前解決トラフィックを許可します。

## コネクタの作成または切り替え

データをクラウドにバックアップするにはコネクタが必要です。Azure BLOB ストレージにデータをバックアップする場合は、コネクタが Azure VNet 内に存在する必要があります。オンプレミスに導入されているコネクタは使用できません。新しいコネクタを作成するか、現在選択されているコネクタが正しいプロバイダーにあることを確認する必要があります。

- "[コネクタについて説明します](#)"
- "[Azure でコネクタを作成する](#)"
- "[コネクタ間の切り替え](#)"

## コネクタのネットワークを準備しています

コネクタに必要なネットワーク接続があることを確認します。

### 手順

1. コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
  - Cloud Backup Service へのアウトバウンドインターネット接続 ポート 443 （HTTPS）
  - ポート 443 経由での BLOB オブジェクトストレージへの HTTPS 接続
  - ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
2. Azure ストレージへの VNet プライベートエンドポイントを有効化これは、ONTAP クラスタから VNet への ExpressRoute または VPN 接続があり、コネクタと BLOB ストレージ間の通信を仮想プライベートネットワークのままにする場合に必要です。

## サポートされている地域

すべての地域で、オンプレミスシステムから Azure Blob へのバックアップを作成できます "[Cloud Volumes ONTAP がサポートされている場合](#)" Azure Government リージョンを含む。サービスのセットアップ時にバッ



クアッブを保存するリージョンを指定します。

## ライセンス要件を確認

- クラスタでCloud Backupをアクティブ化するには、従量課金制（PAYGO）のCloud Manager Marketplace が提供するAzureのサービスをサブスクライブするか、ネットアップからCloud Backup BYOLライセンスを購入してアクティブ化する必要があります。これらのライセンスはアカウント用であり、複数のシステムで使用できます。
  - Cloud Backup PAYGO ライセンスの場合は、へのサブスクリプションが必要です ["Azure" Cloud Backup](#)を使用するためのCloud Manager Marketplaceのサービス。Cloud Backup の請求は、このサブスクリプションを通じて行われます。
  - Cloud Backup BYOL ライセンスを利用するには、ライセンスの期間と容量に応じてサービスを使用できるように、ネットアップから提供されたシリアル番号が必要です。 ["BYOL ライセンスの管理方法について説明します"](#)。
- バックアップを配置するオブジェクトストレージスペース用の Azure サブスクリプションが必要です。

すべての地域で、オンプレミスシステムから Azure Blob へのバックアップを作成できます ["Cloud Volumes ONTAP がサポートされている場合"](#)Azure Government リージョンを含む。サービスのセットアップ時にバックアップを保存するリージョンを指定します。

## バックアップ用に **Azure BLOB** ストレージを準備しています

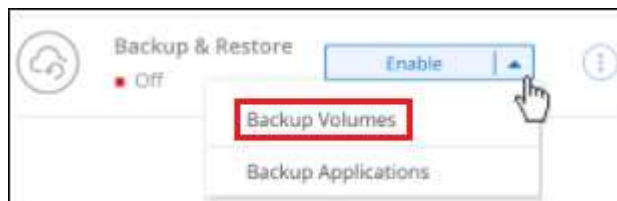
1. Microsoftが管理するデフォルトの暗号化キーを使用する代わりに、アクティベーションウィザードで独自のカスタム管理キーを使用して、データ暗号化を行うことができます。この場合、Azure サブスクリプション、キー・ボルト名、およびキーが必要です。 ["独自のキーの使用方法を参照してください"](#)。
2. オンプレミスのデータセンターから VNet へのパブリックインターネット経由での接続をより安全にするには、アクティベーションウィザードで Azure Private Endpoint を設定するオプションがあります。この場合、この接続用の VNet とサブネットについて理解しておく必要があります。 ["プライベートエンドポイントの使用の詳細を参照してください"](#)。

## Cloud Backup を有効にしています

Cloud Backup は、オンプレミスの作業環境からいつでも直接有効にできます。

### 手順

1. キャンバスから作業環境を選択し、右パネルのバックアップと復元サービスの横にある **\*Enable>Backup Volumes \*** をクリックします。



ボタンを示すスクリーンショット"]

2. プロバイダとして Microsoft Azure を選択し、**\* Next \*** をクリックします。
3. プロバイダの詳細を入力し、**\* 次へ \*** をクリックします。
  - a. バックアップおよびバックアップを格納する Azure リージョンで使用する Azure サブスクリプション。

- b. BLOB コンテナを管理するリソースグループ - 新しいリソースグループを作成したり、既存のリソースグループを選択したりできます。
- c. Microsoft が管理するデフォルトの暗号化キーを使用するか、お客様が管理する独自のキーを選択してデータの暗号化を管理するか。 ("[独自のキーの使用方法を参照してください](#)")。

- 4. アカウントにCloud Backupの既存のライセンスがない場合は、使用する課金方法を選択するよう求められます。Azureから従量課金制（PAYGO）のCloud Manager Marketplaceサービスにサブスクライブする（または複数のサブスクリプションを選択する必要がある場合）、またはネットアップからCloud Backup BYOLライセンスを購入してアクティブ化することができます。 "[Cloud Backupライセンスの設定方法について説明します。](#)"
- 5. ネットワークの詳細を入力し、\* 次へ \* をクリックします。
  - a. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンドのインターネットアクセスが必要です。
  - b. 必要に応じて、Azure プライベートエンドポイントを設定するかどうかを選択します。 "[プライベートエンドポイントの使用の詳細を参照してください](#)"。

- 6. デフォルトのバックアップポリシーの詳細を入力し、\* Next \* をクリックします。
  - a. バックアップスケジュールを定義し、保持するバックアップの数を選択します。 "[選択可能な既存のポリシーのリストが表示されます](#)"。
  - b. ONTAP 9.10.1 以降を使用している場合は、特定の日数が経過したバックアップを Azure Archive ストレージに階層化して、コストをさらに最適化することができます。 "[アーカイブ階層の使用の詳細については、こちらをご覧ください](#)"。



### Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

**Policy - Retention & Schedule** ☒ Create a New Policy ☐ Select an Existing Policy

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

**Archival Policy**

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Access Tier
 

Azure Archive

**Storage Account**

Cloud Manager will create the storage account after you complete the wizard

7. Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを選択します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、追加のポリシーを作成し、それらのボリュームにあとから適用できます。

- すべてのボリュームをバックアップするには、タイトル行（☒ Volume Name）。
- 個々のボリュームをバックアップするには、各ボリュームのボックス（☒ Volume\_1）。

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 <small>On</small>	DP	SVM_Name_2	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy

今後追加されるすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップ ...」チェックボックスをオンのままにします。この設定を無効にした場合は、以降のボリュームのバックアップを手動で有効にする必要があります。

8. Activate Backup \* をクリックすると、ボリュームの初期バックアップの作成が開始されます。

Cloud Backup が起動し、選択した各ボリュームの初期バックアップの作成が開始されます。Volume Backup

Dashboard が表示され、バックアップの状態を監視できます。

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"。また可能です "ボリューム全体または個々のファイルをバックアップファイルからリストアする" Azure 内の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムへの接続に使用できます。

## オンプレミスの ONTAP データの StorageGRID へのバックアップ

オンプレミスの ONTAP システムから NetApp StorageGRID システムのオブジェクトストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

「オンプレミス ONTAP システム」には、FAS、AFF、ONTAP Select の各システムが含まれます。

### クイックスタート

これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>   
Alt="one " & /span & 設定のサポートを確認します

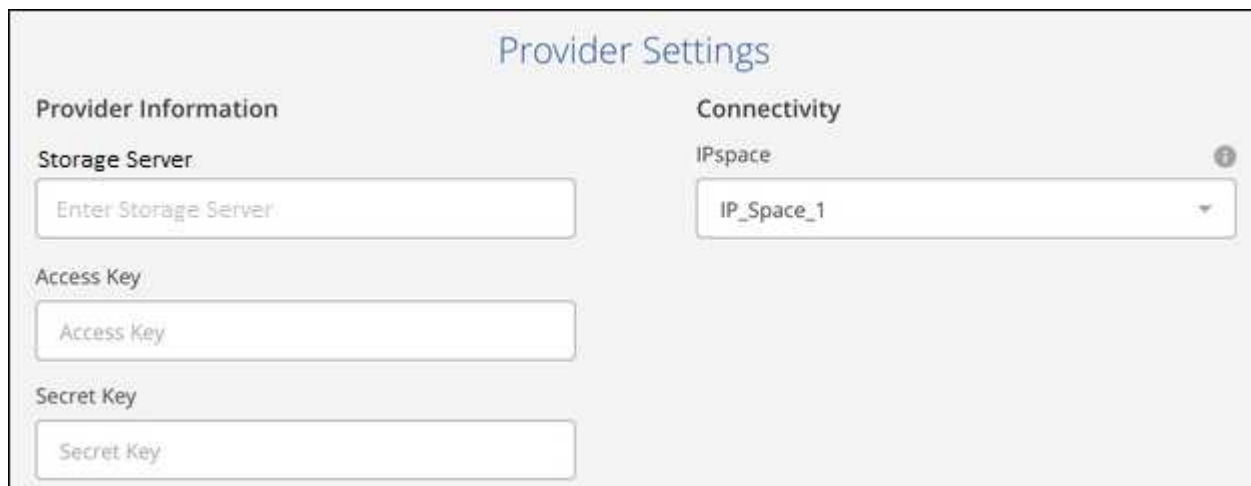
- オンプレミスクラスタを検出し、Cloud Manager の作業環境に追加しておきます。を参照してください ["ONTAP クラスタの検出"](#) を参照してください。
  - クラスタで ONTAP 9.7P5 以降が実行されています。
  - クラスタには SnapMirror ライセンスがあります。このライセンスは、Premium Bundle または Data Protection Bundle に含まれています。
  - クラスタから StorageGRID およびコネクタへの必要なネットワーク接続が確立されている必要があります。
- コネクタがオンプレミスにインストールされている。
  - コネクタは、インターネットに接続するかどうかに関係なく、サイトにインストールできます。
  - コネクタのネットワークを使用すると、ONTAP クラスタおよび StorageGRID へのアウトバウンド HTTPS 接続が可能になります。
- を購入済みである ["アクティブ化されます"](#) NetApp の Cloud Backup BYOL ライセンス。
- StorageGRID バージョン 10.3 以降では、S3 権限を持つアクセスキーが設定されています。

作業環境を選択し、右パネルのバックアップと復元サービスの横にある \*Enable>Backup Volumes] をクリックして、セットアップ・ウィザードに従います。



ボタンを示すスクリーンショット"]

プロバイダとして StorageGRID を選択し、StorageGRID サーバとサービスアカウントの詳細を入力します。また、ボリュームが配置されている ONTAP クラスタ内の IPspace を指定する必要があります。



デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。



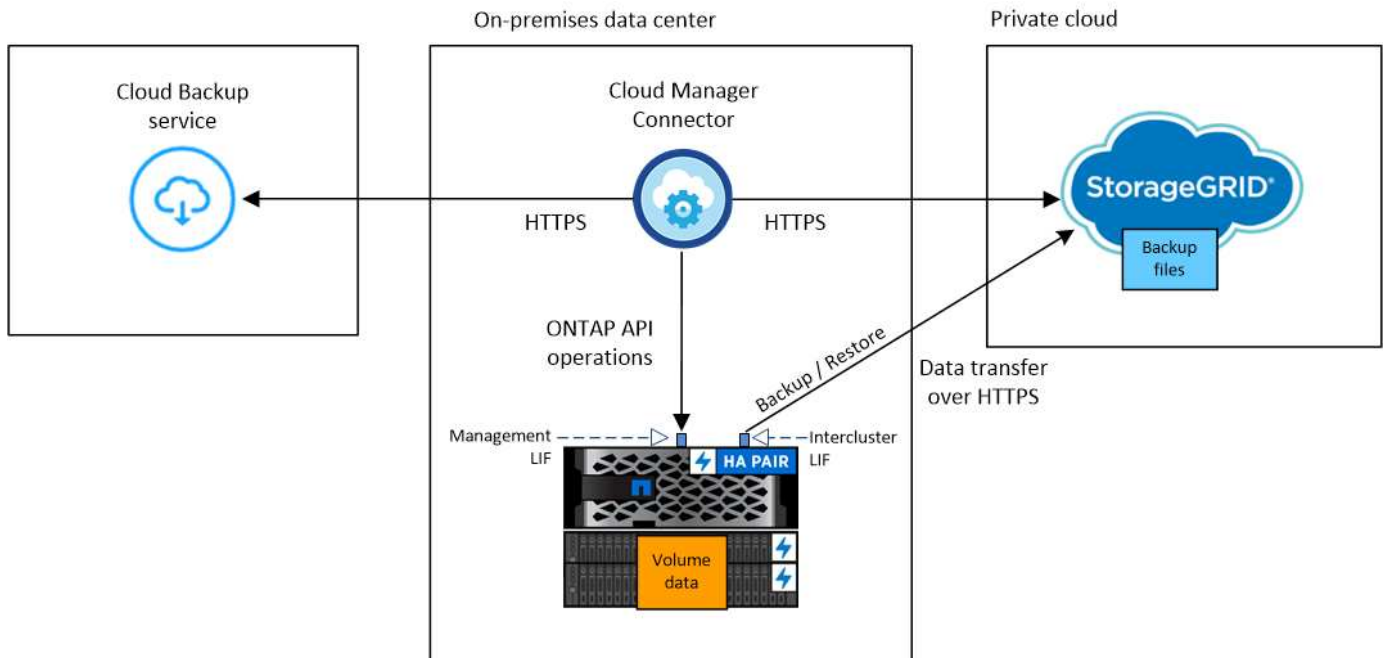
Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを特定します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、あとから追加のポリシーを作成してボリュームに適用できます。

S3 バケットは、入力した S3 アクセスキーとシークレットキーで指定されたサービスアカウントに自動的に作成され、そこにバックアップファイルが格納されます。

## 要件

オンプレミスボリュームを StorageGRID にバックアップする前に、次の要件を確認し、サポートされている構成であることを確認してください。

次の図は、オンプレミスの ONTAP システムを StorageGRID にバックアップする場合と、それらの間で準備する必要がある接続を含む各コンポーネントを示しています。



コネクタとオンプレミスの ONTAP システムがインターネットにアクセスできないオンプレミスの場所にインストールされている場合、StorageGRID システムは同じオンプレミスのデータセンターに配置されている必要があります。

## ONTAP クラスタの準備

ボリュームデータのバックアップを開始する前に、Cloud Manager でオンプレミスの ONTAP クラスタを検出する必要があります。

["クラスタの検出方法について説明します"](#)。

## ONTAP の要件

- ONTAP 9.7P5以降が必要です。ONTAP 9.8P11以降が推奨されます。
- SnapMirror ライセンス（Premium Bundle または Data Protection Bundle に含まれます）。
- 注：\* Cloud Backup を使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を参照してください ["クラスタライセンスを管理します"](#)。

- 時間とタイムゾーンが正しく設定されている。

方法を参照してください ["クラスタ時間を設定します"](#)。

## クラスタネットワークの要件

- ONTAP クラスタは、バックアップおよびリストア処理のために、ユーザ指定のポートをクラスタ間 LIF から StorageGRID へと接続します。ポートはバックアップのセットアップ時に設定できます。

ONTAP は、オブジェクトストレージとの間でデータの読み取りと書き込みを行います。オブジェクトストレージが開始されることはなく、応答するだけです。

- ONTAP では、コネクタからクラスタ管理 LIF へのインバウンド接続が必要です。コネクタは必ずオンプレミスに配置してください。

- クラスタ間 LIF は、バックアップ対象のボリュームをホストする各 ONTAP ノードに必要です。LIF は、ONTAP がオブジェクトストレージへの接続に使用する IPspace に関連付けられている必要があります。"[IPspace の詳細については、こちらをご覧ください](#)"。

Cloud Backup をセットアップすると、IPspace で使用するよう求められます。各 LIF を関連付ける IPspace を選択する必要があります。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

- ノードのクラスタ間 LIF はオブジェクトストアにアクセスできます（コネクタが「ダーク」サイトに設置されている場合は不要）。
- ボリュームが配置されている Storage VM に DNS サーバが設定されている。方法を参照してください "[SVM 用に DNS サービスを設定](#)"。
- をデフォルトとは異なる IPspace を使用している場合は、オブジェクトストレージへのアクセスを取得するために静的ルートの作成が必要になることがあります。
- 必要に応じてファイアウォールルールを更新し、指定したポート（通常はポート 443）を介した ONTAP からオブジェクトストレージへの Cloud Backup Service 接続、およびポート 53（TCP / UDP）を介した Storage VM から DNS サーバへの名前解決トラフィックを許可します。

## StorageGRID を準備しています

StorageGRID は、次の要件を満たす必要があります。を参照してください "[StorageGRID のドキュメント](#)" を参照してください。

サポートされている **StorageGRID** のバージョン

StorageGRID 10.3 以降がサポートされます。

## S3 クレデンシャル

StorageGRID へのバックアップを設定する際、サービスアカウントの S3 アクセスキーとシークレットキーを入力するようにバックアップウィザードで求められます。サービスアカウントを使用すると、Cloud Backup でバックアップの認証を行い、バックアップの格納に使用する StorageGRID バケットにアクセスできます。StorageGRID が誰が要求を行うかを認識できるようにするには、キーが必要です。

これらのアクセスキーは、次の権限を持つユーザに関連付ける必要があります。

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

## オブジェクトのバージョン管理

オブジェクトストアバケットで StorageGRID オブジェクトのバージョン管理を有効にすることはできません。

## コネクタの作成または切り替え

StorageGRID にデータをバックアップするときは、オンプレミスのコネクタが必要です。新しいコネクタ

をインストールするか、現在選択されているコネクタがオンプレミスにあることを確認する必要があります。コネクタは、インターネットに接続するかどうかに関係なく、サイトにインストールできます。

- ["コネクタについて説明します"](#)
- ["インターネットにアクセスできる Linux ホストにコネクタをインストールしています"](#)
- ["インターネットにアクセスできない Linux ホストにコネクタをインストールしています"](#)
- ["コネクタ間の切り替え"](#)



Cloud Backup の機能は、Cloud Manager Connector に組み込まれています。インターネットに接続されていないサイトにインストールする場合は、コネクタソフトウェアを定期的に更新して、新しい機能にアクセスする必要があります。を確認します ["Cloud Backup の新機能"](#) Cloud Backup の各リリースの新機能を確認し、手順 ~ を実行します ["Connector ソフトウェアをアップグレードします"](#) 新しい機能を使用する場合。

コネクタのネットワークを準備しています

コネクタに必要なネットワーク接続があることを確認します。

手順

1. コネクタが取り付けられているネットワークで次の接続が有効になっていることを確認します。
  - ポート 443 から StorageGRID への HTTPS 接続
  - ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
  - ポート 443 から Cloud Backup へのアウトバウンドインターネット接続（コネクタが「ダーク」サイトにインストールされている場合は不要）

ライセンス要件

クラスタのCloud Backupをアクティブ化する前に、NetAppからCloud Backup BYOLライセンスを購入してアクティブ化する必要があります。このライセンスはアカウント用であり、複数のシステムで使用できます。

ネットアップから提供されるシリアル番号を使用して、ライセンスの期間と容量にサービスを利用できるようにする必要があります。 ["BYOL ライセンスの管理方法について説明します"](#)。



PAYGO ライセンスは、ファイルを StorageGRID にバックアップする場合にはサポートされません。

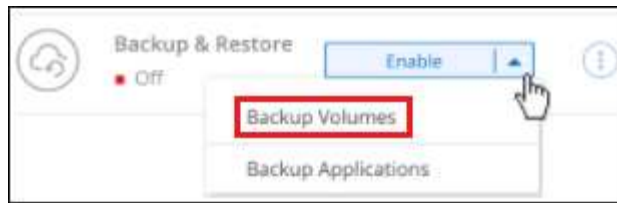
## StorageGRID へのクラウドバックアップを有効化

Cloud Backup は、オンプレミスの作業環境からいつでも直接有効にできます。

手順

1. キャンバスからオンプレミスの作業環境を選択し、右パネルのバックアップと復元サービスの横にある [\\*Enable> バックアップボリューム \\*](#) をクリックします。





ボタンを示すスクリーンショット"]

2. プロバイダとして \* StorageGRID \* を選択し、 \* Next \* をクリックして、プロバイダの詳細を入力します。
  - a. StorageGRID サーバの FQDN と ONTAP が StorageGRID との HTTPS 通信に使用するポート。例 : 「 3.eng.company.com:8082` 」
  - b. バックアップを格納するバケットへのアクセスに使用するアクセスキーとシークレットキー。
  - c. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace 。この IPspace のクラスタ間 LIF には、アウトバウンドのインターネットアクセスが必要です（コネクタが「ダーク」サイトにインストールされている場合は不要です）。

適切な IPspace を選択すると、ONTAP から StorageGRID オブジェクトストレージへの接続を Cloud Backup で確実にセットアップできます。

この情報は、サービスの開始後は変更できないことに注意してください。

3. [Define Policy] ページで、デフォルトのバックアップスケジュールと保持の値を選択し、 [\* Next] をクリックします。



を参照してください ["既存のポリシーのリスト"](#)。

4. Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを選択します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、追加のポリシーを作成し、それらのボリュームにあとから適用できます。

- すべてのボリュームをバックアップするには、タイトル行（☒ Volume Name）。
- 個々のボリュームをバックアップするには、各ボリュームのボックス（☒ Volume\_1）。

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy ⓘ						

このクラスタに追加するすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップ ...」のチェックボックスをオンのままにします。この設定を無効にした場合は、以降のボリュームのバックアップを手動で有効にする必要があります。

5. Activate Backup \* をクリックすると、選択した各ボリュームの初期バックアップの実行が開始されます。

S3 バケットは、入力した S3 アクセスキーとシークレットキーで指定されたサービスアカウントに自動的に作成され、そこにバックアップファイルが格納されます。ボリュームバックアップダッシュボードが表示され、バックアップの状態を監視できます。

可能です ["ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます スケジュール"](#)。また可能です ["ボリューム全体または個々のファイルをバックアップファイルからリストアする"](#) オンプレミスのONTAP システムへの移行をサポート

## ONTAP システムのバックアップの管理

Cloud Volumes ONTAP システムとオンプレミス ONTAP システムのバックアップの管理では、バックアップスケジュールの変更、ボリュームのバックアップの有効化 / 無効化、バックアップの削除などを行うことができます。



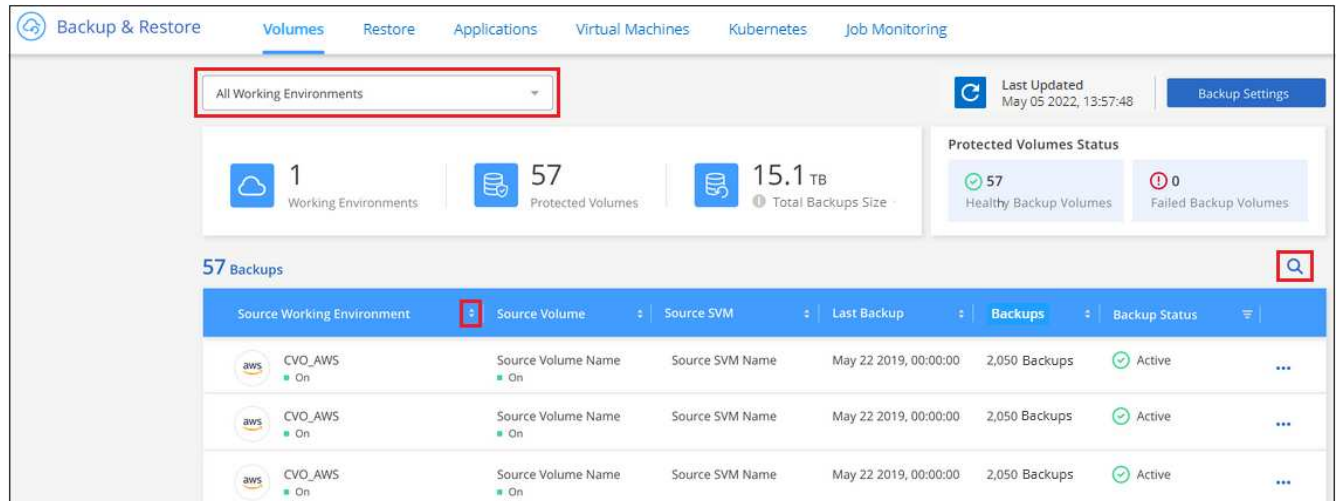
バックアップファイルをクラウドプロバイダ環境から直接管理したり変更したりしないでください。ファイルが破損し、サポートされていない構成になる可能性があります。

## バックアップしているボリュームを表示します

バックアップダッシュボードには、現在バックアップ中のすべてのボリュームのリストが表示されます。

### 手順

1. [バックアップと復元 \*] タブをクリックします。
2. [\* Volumes] タブをクリックして、Cloud Volumes ONTAP およびオンプレミス ONTAP システムのボリュームのリストを表示します。



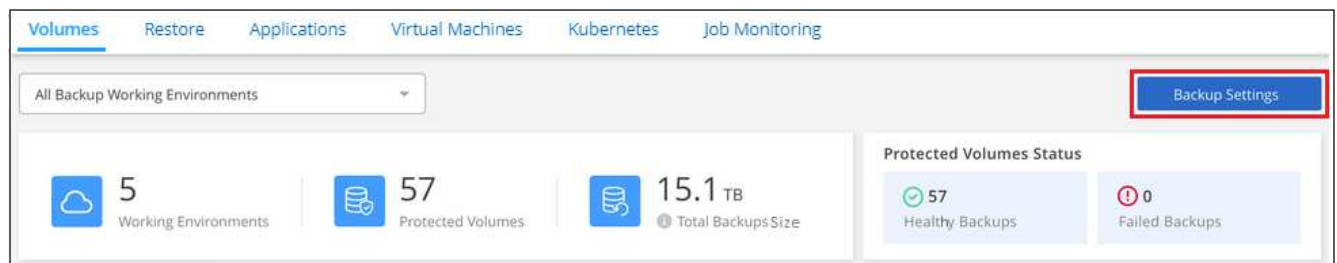
特定の作業環境で特定のボリュームを検索する場合は、作業環境とボリュームに基づいてリストを絞り込むか、検索フィルタを使用できます。

## ボリュームのバックアップの有効化と無効化

ボリュームのバックアップコピーが不要で、バックアップの格納コストを抑える必要がない場合は、ボリュームのバックアップを停止できます。新しいボリュームがバックアップ中でない場合は、バックアップリストに追加することもできます。

### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



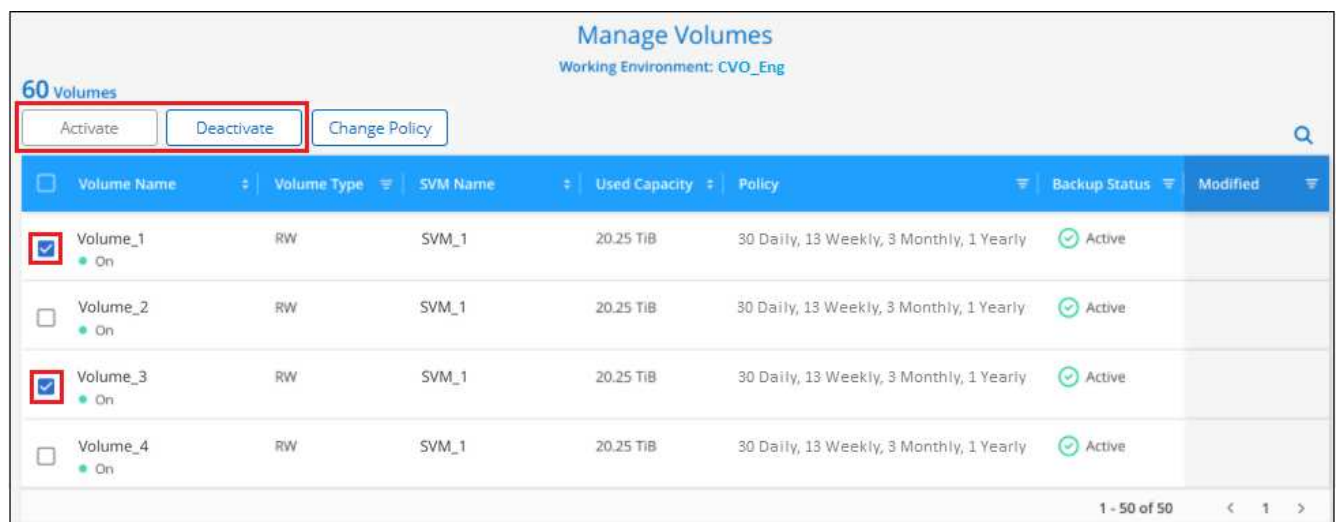
ボタンを示すスクリーンショット。"]

2. \_バックアップ設定ページ\_ で、をクリックします ... アイコン"] 作業環境では、\* ボリュームの管理 \* を選択します。



ページの [ ボリュームの管理 ] ボタンを示すスクリーンショット。"]

3. 変更するボリュームのチェックボックスを選択し、ボリュームのバックアップを開始するか停止するかに応じて、[Activate \* (アクティブ化 \*) ] または [\* Deactivate \* (非アクティブ化 \*) ] をクリックします。



4. [ 保存 ( Save ) ] をクリックして、変更をコミットします。

。注意： \* ボリュームのバックアップを停止すると、バックアップが停止します オブジェクトの料金はクラウドプロバイダが継続的に負担します を除いて、バックアップが使用する容量のストレージコスト あなた [バックアップを削除します](#)。

## 既存のバックアップポリシーを編集する

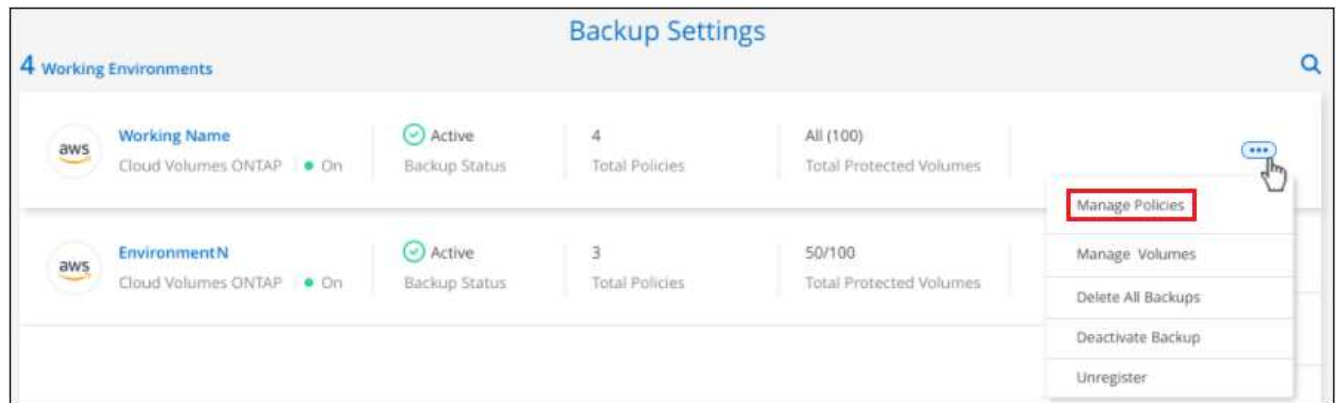
作業環境でボリュームに現在適用されているバックアップポリシーの属性を変更することができます。バックアップポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームが対象になります。

### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



2. [Backup Settings] ページで、をクリックします ... アイコン"] 設定を変更する作業環境で、[\* ポリシーの管理 \*] を選択します。



ページの [ポリシーの管理] オプションを示すスクリーンショット。"]

3. [ポリシーの管理] ページで、作業環境で変更するバックアップポリシーの [ポリシーの編集] をクリックします。



4. [ポリシーの編集] ページで、スケジュールとバックアップの保持を変更し、[保存] をクリックします。



クラスタでONTAP 9.10.1以降が実行されている場合は、特定の日数が経過したバックアップをアーカイブストレージに階層化するかどうかを有効または無効にすることもできます。

"Azure アーカイブストレージの使用方法については、こちらをご覧ください"。

[+]

The image shows two sections of a backup policy configuration interface. The top section is for 'Azure' and the bottom for 'AWS'. Both sections have a title 'Archival Policy' and a description: 'Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.' for Azure, and 'Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.' for AWS. Both sections have a checkbox 'Tier Backups to Archival' which is checked. For Azure, there is a text input 'Archive after (Days)' with the value '30' and a dropdown 'Access Tier' with 'Azure Archive' selected. For AWS, there is a text input 'Archive after (Days)' with the value '30' and a dropdown 'Storage Class' with 'S3 Glacier' selected, showing a list of options: 'S3 Glacier', 'S3 Glacier Deep Archive', and 'S3 Glacier'.

+アーカイブストレージに階層化されたバックアップファイルは、アーカイブへのバックアップの階層化を停止した場合、その階層に残ります。これらのファイルは自動的に標準階層に戻されません。

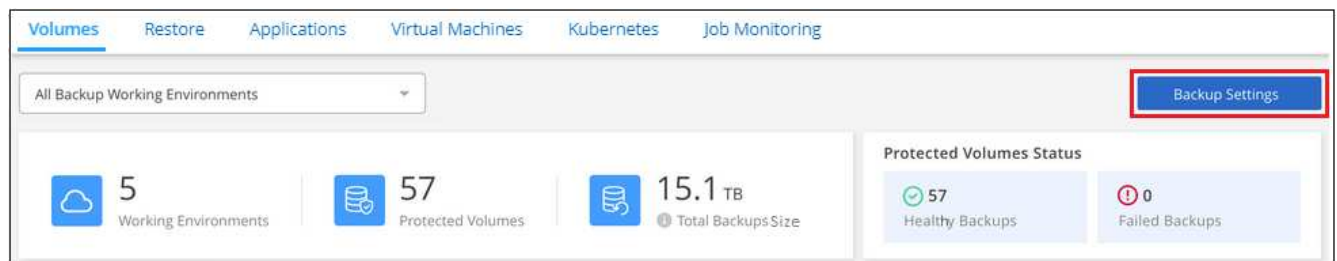
## 新しいバックアップポリシーを追加しています

作業環境で Cloud Backup を有効にすると、最初を選択したすべてのボリュームが、定義したデフォルトのバックアップポリシーを使用してバックアップされます。Recovery Point Objective（RPO；目標復旧時点）が異なるボリュームに対して異なるバックアップポリシーを割り当てる場合は、そのクラスタに追加のポリシーを作成し、そのポリシーを他のボリュームに割り当てることができます。

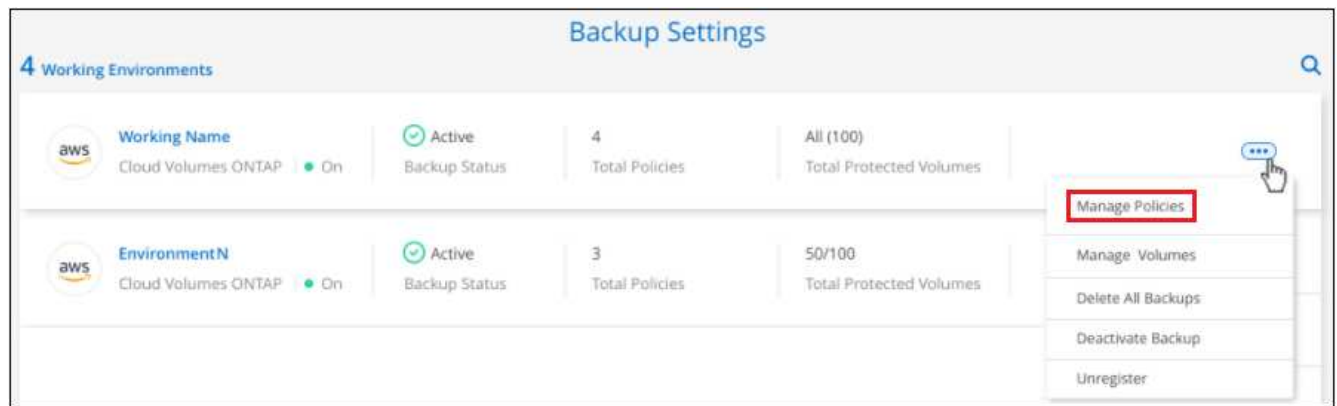
作業環境内の特定のボリュームに新しいバックアップポリシーを適用する場合は、最初にそのバックアップポリシーを作業環境に追加する必要があります。すると [その作業環境内のボリュームにポリシーを適用します](#)。

### 手順

1. [\* Volumes（ボリューム）] タブで、[\* Backup Settings（バックアップ設定）] を選択します。



2. [Backup Settings] ページで、をクリックします ... アイコン"] 新しいポリシーを追加する作業環境で、[ポリシーの管理] を選択します。



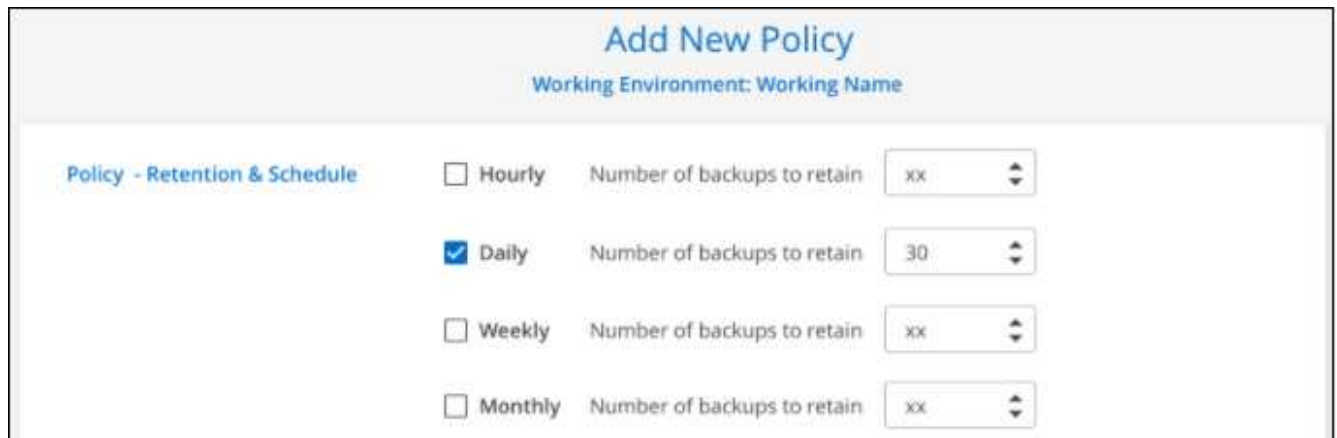
ページの [ ポリシーの管理 ] オプションを示すスクリーンショット。"]

3. [ ポリシーの管理 ] ページで、 [ 新しいポリシーの追加 ] をクリックします。



ページの [ 新しいポリシーの追加 ] ボタンを示すスクリーンショット。"]

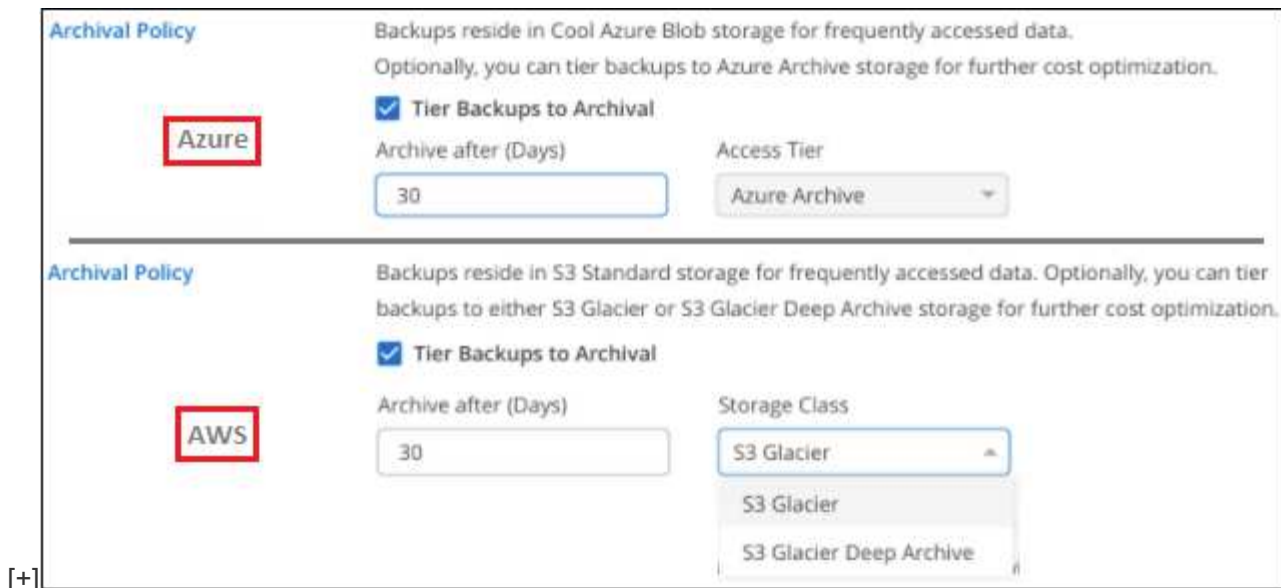
4. [ 新しいポリシーの追加 ] ページで、スケジュールとバックアップの保持を定義し、 [ 保存 ] をクリックします。



クラスターでONTAP 9.10.1以降が実行されている場合は、特定の日数が経過したバックアップをアーカイブストレージに階層化するかどうかを有効または無効にすることもできます。

"Azure アーカイブストレージの使用方法については、こちらをご覧ください"。





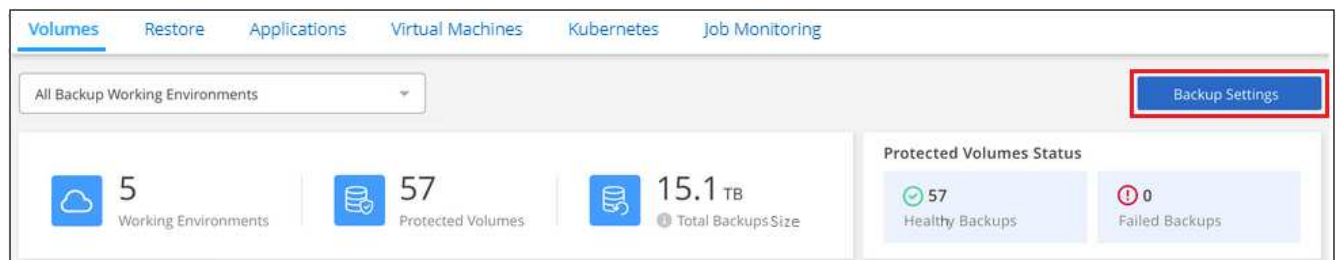
## 既存のボリュームに割り当てられているポリシーを変更する

既存のボリュームに割り当てられているバックアップポリシーは、バックアップを作成する頻度を変更する場合や、保持期間を変更する場合に変更できます。

ボリュームに適用するポリシーがすでに存在する必要があります。 [作業環境に新しいバックアップポリシーを追加する方法を参照してください。](#)

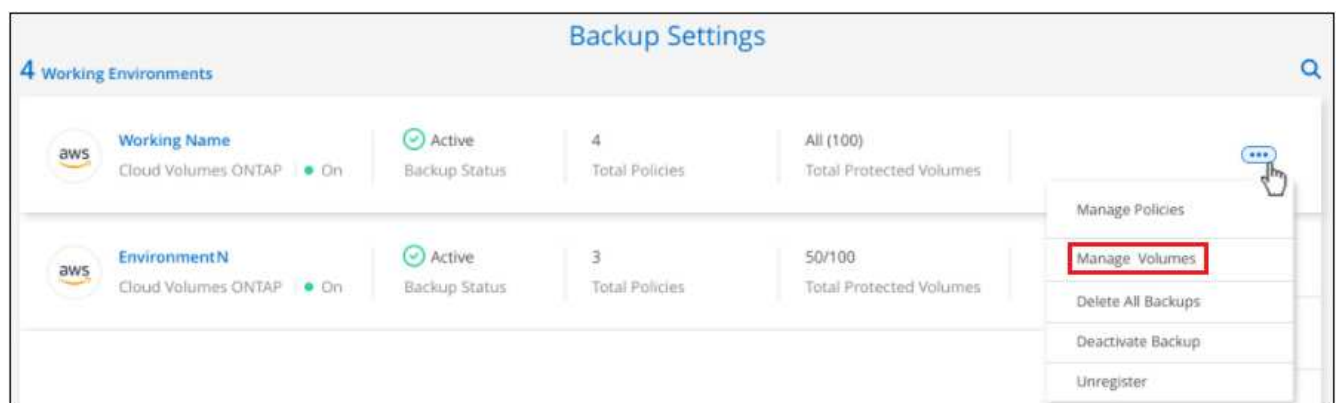
### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



ボタンを示すスクリーンショット。"]

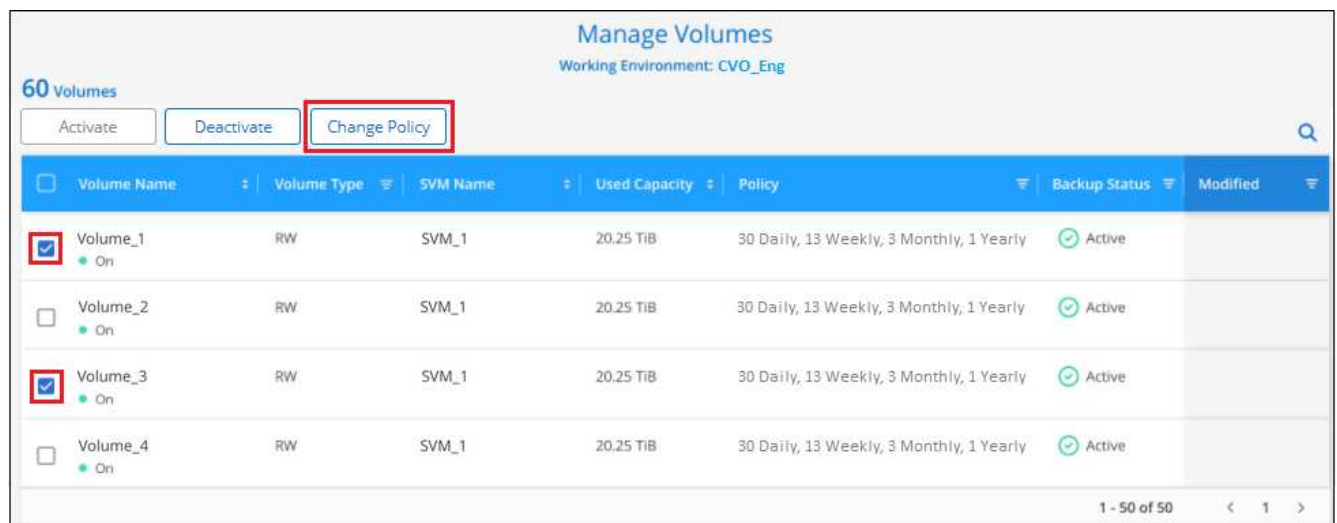
2. 「バックアップ設定ページ」で、をクリックします ... アイコン"] ボリュームが存在する作業環境で、\* ボリュームの管理 \* を選択します。



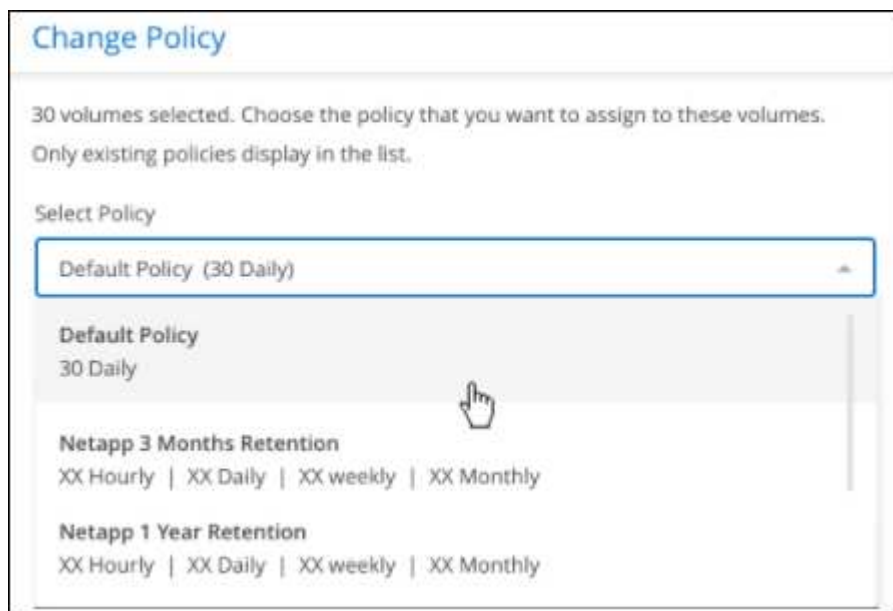


ページの [ ボリュームの管理 ] ボタンを示すスクリーンショット。"]

3. ポリシーを変更するボリュームのチェックボックスを選択し、 \* ポリシーの変更 \* をクリックします。



4. [Change Policy] ページで、ボリュームに適用するポリシーを選択し、 [\* ポリシーの変更 \*] をクリックします。



5. [ 保存 ( Save ) ] をクリックして、変更をコミットします。

## 新しいボリュームに割り当てるバックアップポリシーの設定

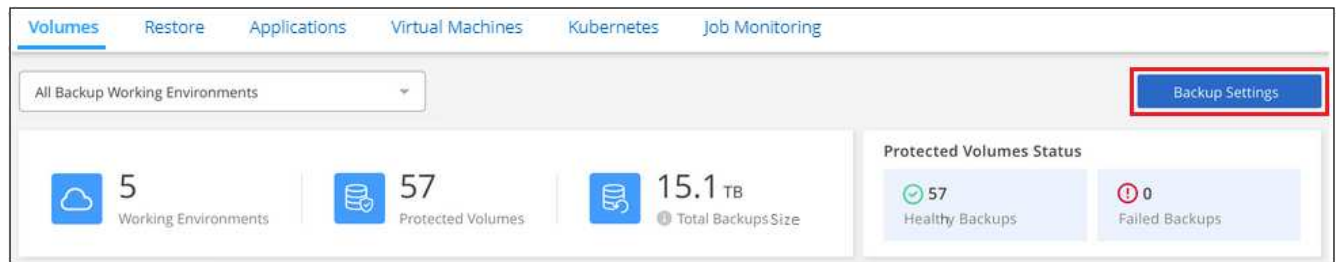
ONTAP クラスタでクラウドバックアップを初めてアクティブ化したときに、新しく作成したボリュームにバックアップポリシーを自動的に割り当てるオプションを選択していない場合は、あとで Backup Settings\_page でこのオプションを選択できます。新しく作成したボリュームにバックアップポリシーを割り当てると、すべてのデータを確実に保護できます。

ボリュームに適用するポリシーがすでに存在する必要があります。 [作業環境に新しいバックアップポリシーを追加する方法を参照してください。](#)

また、新しく作成したボリュームが自動的にバックアップされないようにするには、この設定を無効にします。その場合は、後でバックアップする特定のボリュームのバックアップを手動で有効にする必要があります。

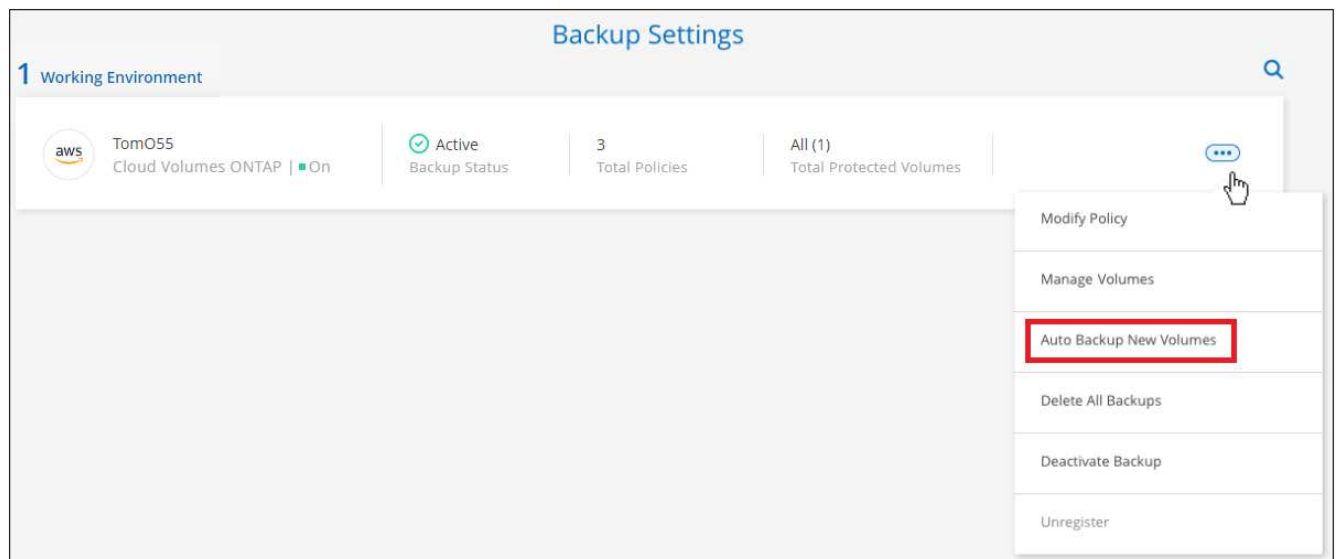
手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



ボタンを示すスクリーンショット。"]

2. 「バックアップ設定ページ」で、をクリックします ... アイコン"] ボリュームが存在する作業環境で、\*自動バックアップ新規ボリューム\*を選択します。



ページで[新しいボリュームの自動バックアップ]オプションを選択したスクリーンショット。"]

3. 「新しいボリュームを自動的にバックアップ...」チェックボックスをオンにし、新しいボリュームに適用するバックアップポリシーを選択して、「保存」をクリックします。

### Auto Backup New Volumes

☒ Automatically back up new volumes on all SVMs for Working Environment TomO55

Choose the policy that will be assigned to new volumes. Only existing policies are shown in the list.

Select Backup Policy

CloudBackupService-1611307085985\_V2 (30 Daily) ▼

Save

Cancel

このバックアップポリシーは、Cloud Manager、System Manager、またはONTAP CLIを使用して、この作業環境で作成した新しいボリュームに適用されます。

## ボリュームの手動バックアップをいつでも作成できます

オンデマンドバックアップはいつでも作成することができ、ボリュームの現在の状態をキャプチャすることができます。これは、ボリュームに非常に重要な変更が行われたために、次のスケジュールされたバックアップでそのデータが保護されるのを待たずに、現在バックアップ中ではなく現在の状態をキャプチャする場合に便利です。

バックアップ名にはタイムスタンプが含まれるため、他のスケジュールされたバックアップからオンデマンドバックアップを特定できます。

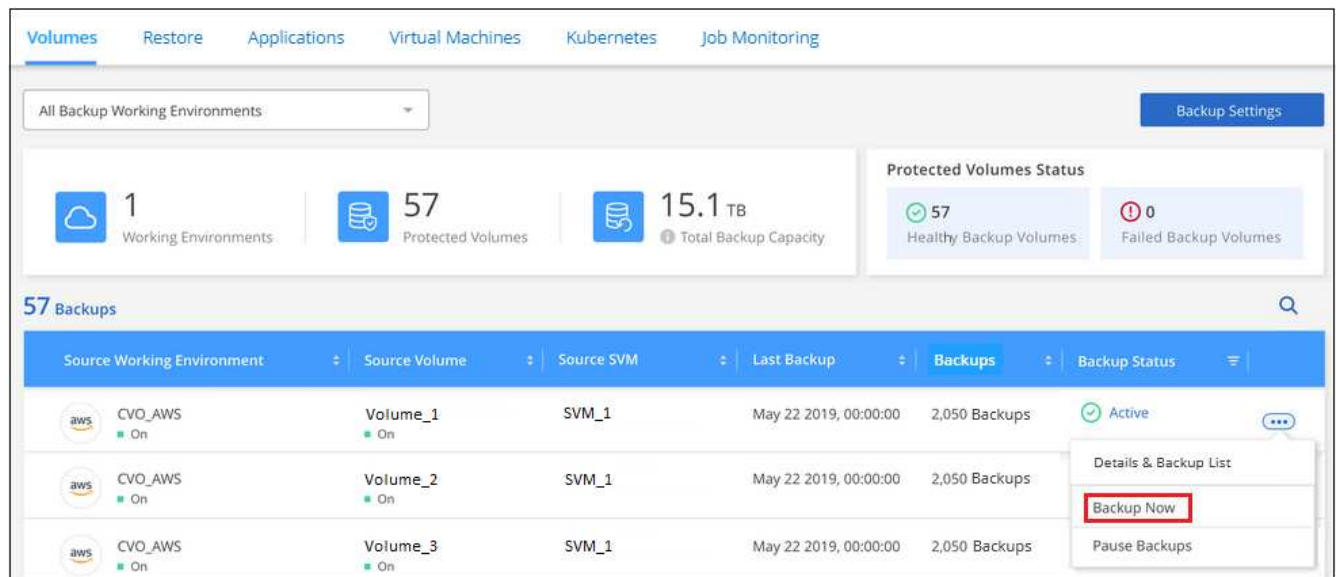
アドホックバックアップを作成する場合、ソースボリューム上にSnapshotが作成されることに注意してください。このSnapshotは通常のSnapshotスケジュールの一部ではないため、offのままになりません。バックアップの完了後に、このSnapshotをソースボリュームから手動で削除できます。これにより、このSnapshotに関連するブロックが解放されます。スナップショットの名前は'CBS-snapshot-adhoc -'で始まります ["ONTAP CLIを使用してSnapshotを削除する方法を参照してください"](#)。



オンデマンドボリュームバックアップは、データ保護ボリュームではサポートされません。

### 手順

1. [\* Volumes (ボリューム) ] タブで、をクリックします [...](#) アイコン"] ボリュームの場合は、\* 今すぐバックアップ\* を選択します。



ボタンのスクリーンショット。"]

バックアップが作成されるまで、このボリュームの Backup Status 列には「In Progress」と表示されます。

## 各ボリュームのバックアップリストを表示します

各ボリュームに存在するすべてのバックアップファイルのリストを表示できます。このページには、ソースボリューム、デスティネーションの場所、および前回作成されたバックアップの詳細、現在のバックアップポリシー、バックアップファイルのサイズなどのバックアップの詳細が表示されます。

このページでは、次のタスクも実行できます。

- ボリュームのすべてのバックアップファイルを削除します
- ボリュームの個々のバックアップファイルを削除する
- ボリュームのバックアップレポートをダウンロードします

### 手順

1. [\* Volumes (ボリューム) ] タブで、をクリックします ... アイコン"] をソースボリュームとして選択し、 \* Details & Backup List \* を選択します。

Buttons shown in screenshot: Backup Settings, Details & Backup List, Backup Now, Pause Backups.

ボタンを示すスクリーンショット"]

すべてのバックアップファイルのリストが、ソースボリューム、デスティネーションの場所、およびバックアップの詳細とともに表示されます。

Source			Destination		Backup Information	
Working Environment	Working Environment N...		Cloud Provider	AWS	Relationship Status	Active
Type	Cloud Volumes ONTAP (HA)		Region	us-east-1	Last Backup	Oct 05 2021, 2:41:33 pm
Provider	AWS		Bucket	netapp-backup	Lag Duration	14 days 3 hours, 38 mi...
Volume	Volume Name		Account ID	012345678901234567890	Backups	2,050
SVM	SVM Name				Backup Policy	Netapp7YearsRetention

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

## バックアップを削除する

Cloud Backup では、1 つのバックアップファイルを削除したり、ボリュームのすべてのバックアップを削除したり、作業環境内のすべてのボリュームのすべてのバックアップを削除したりできます。すべてのバックアップを削除するのは、不要になった場合やソースボリュームを削除したあとにすべてのバックアップを削除する場合などです。



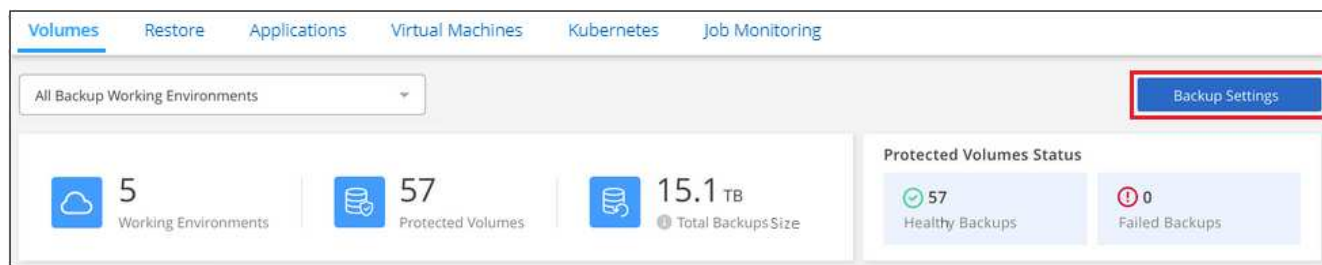
バックアップがある作業環境またはクラスタを削除する場合は、システムを削除する前に \* バックアップを削除する必要があります。システムを削除しても、Cloud Backup はバックアップを自動的に削除しません。また、システムを削除した後でバックアップを削除するための UI で現在サポートされていません。残りのバックアップについては、引き続きオブジェクトストレージのコストが発生します。

## 作業環境のすべてのバックアップファイルを削除する

作業環境のすべてのバックアップを削除しても、この作業環境のボリュームの以降のバックアップは無効になりません。作業環境ですべてのボリュームのバックアップの作成を停止するには、バックアップを非アクティブ化します [ここで説明するようにします](#)。

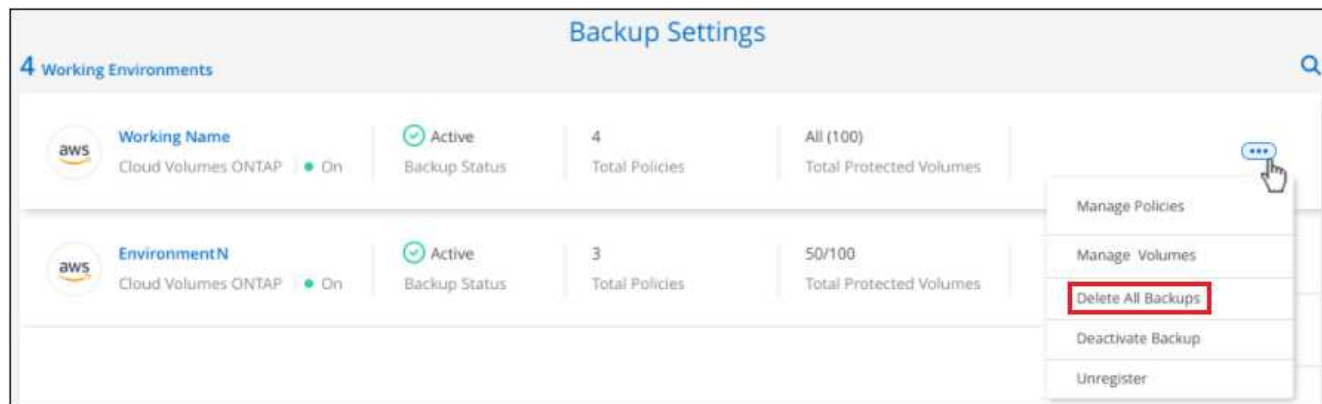
### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



ボタンを示すスクリーンショット。"]

2. をクリックします ... アイコン"] すべてのバックアップを削除する作業環境で、\* すべてのバックアップを削除 \* を選択します。



ボタンを選択したスクリーンショット。"]

3. 確認ダイアログボックスで、作業環境の名前を入力し、\* 削除 \* をクリックする。

## ボリュームのすべてのバックアップファイルを削除する

ボリュームのすべてのバックアップを削除すると、そのボリュームの以降のバックアップも無効になります。

可能です [ボリュームのバックアップの作成を再開します](#) [ Manage Backups (バックアップの管理) ] ページからいつでもアクセスできます。

### 手順



1. [\* Volumes (ボリューム) ] タブで、をクリックします ... アイコン"] をソースボリュームとして選択し、\* Details & Backup List \* を選択します。

The screenshot shows the 'Volumes' tab in a backup management console. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below the navigation bar, there's a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The main area displays summary statistics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. To the right, a 'Protected Volumes Status' box shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a table lists 57 Backups. The table has columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. The first three rows are visible, all showing 'CVO\_AWS' as the source environment and 'SVM\_1' as the source SVM. A dropdown menu is open for the first backup, showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

ボタンを示すスクリーンショット"]

すべてのバックアップファイルのリストが表示されます。

The screenshot shows the details of a backup. It is divided into three main sections: Source, Destination, and Backup Information. The Source section shows 'Working Environment' as 'Working Environment N...', 'Type' as 'Cloud Volumes ONTAP (HA)', 'Provider' as 'AWS', 'Volume' as 'Volume Name', and 'SVM' as 'SVM Name'. The Destination section shows 'Cloud Provider' as 'AWS', 'Region' as 'us-east-1', 'Bucket' as 'netapp-backup', and 'Account ID' as '012345678901234567890'. The Backup Information section shows 'Relationship Status' as 'Active', 'Last Backup' as 'Oct 05 2021, 2:41:33 pm', 'Lag Duration' as '14 days 3 hours, 38 mi...', 'Backups' as '2,050', and 'Backup Policy' as 'Netapp7YearsRetention'. Below these sections, a table lists 2,050 Backups. The table has columns: Backup Name, Date, and Size. The first three rows are visible, all showing 'Backup\_2020\_Jan', 'Backup\_2020\_Mar', and 'Backup\_2020\_Apr' as backup names, with dates from May 22, 2019, and sizes around 19,000.

2. [\* アクション \* > \* すべてのバックアップを削除 \* ] をクリックします。



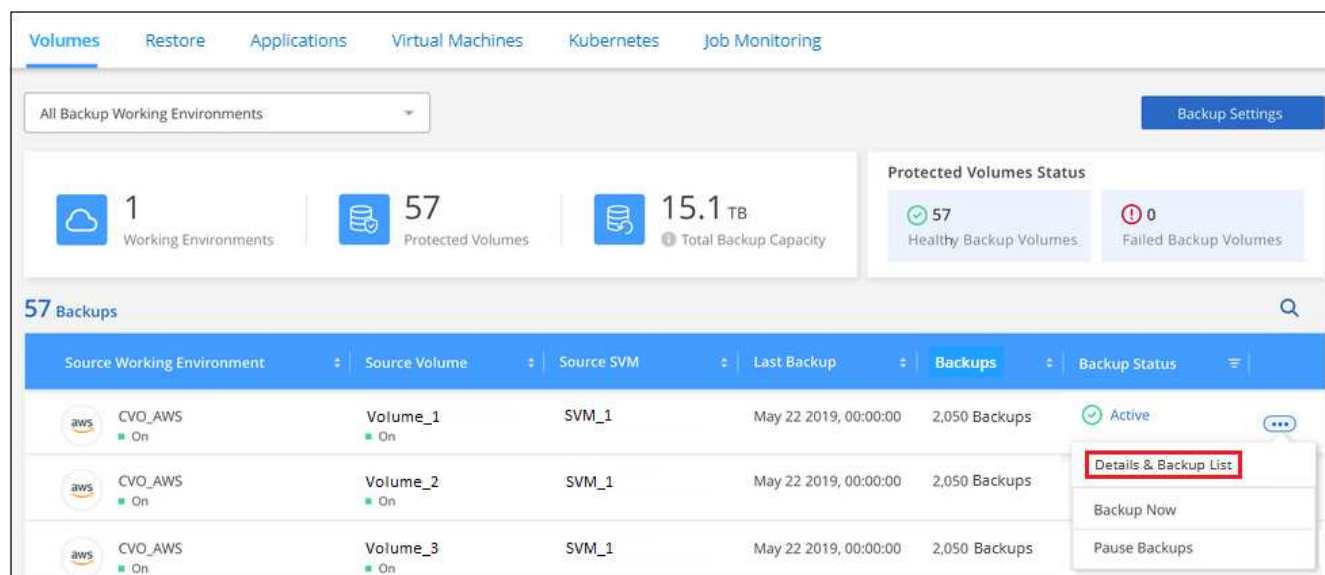
3. 確認ダイアログボックスで、ボリューム名を入力し、\* 削除 \* をクリックします。

ボリュームの単一のバックアップファイルを削除する

バックアップファイルは 1 つだけ削除できます。この機能は、ONTAP 9.8 以降のシステムでボリューム・バックアップを作成した場合にのみ使用できます。

手順

1. [\* Volumes (ボリューム) ] タブで、をクリックします ... アイコン"] をソースボリュームとして選択し、\* Details & Backup List \* を選択します。



ボタンを示すスクリーンショット"]

すべてのバックアップファイルのリストが表示されます。

2. をクリックします **...** アイコン] 削除するボリュームバックアップファイルに対して、**\* 削除 \*** をクリックします。

3. 確認ダイアログボックスで、**\* 削除 \*** をクリックします。

## 作業環境での Cloud Backup の無効化

作業環境で Cloud Backup を無効にすると、システム上の各ボリュームのバックアップが無効になり、ボリュームをリストアすることもできなくなります。既存のバックアップは削除されません。この作業環境からバックアップ・サービスの登録を解除することはありません。基本的には、すべてのバックアップおよびリストア処理を一定期間停止できます。

クラウドから引き続き課金されます が提供する容量のオブジェクトストレージコストのプロバイダ バックアップは自分以外で使います **バックアップを削除します**。

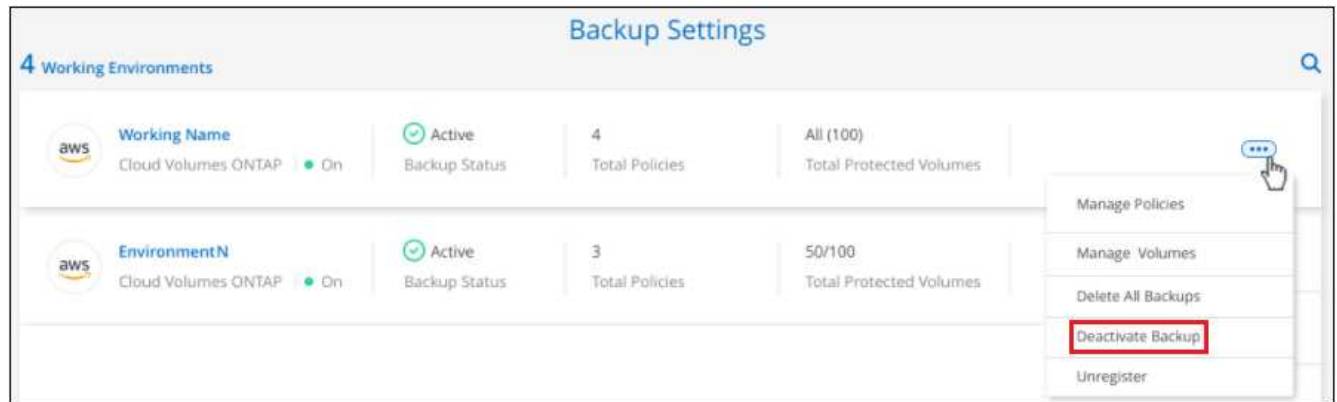
### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



ボタンを示すスクリーンショット。"]

2. 「バックアップ設定ページ」で、をクリックします ... アイコン"] バックアップを無効にする作業環境で、 \* バックアップを非アクティブ化 \* を選択します。



3. 確認ダイアログボックスで、 \* Deactivate \* をクリックします。



バックアップが無効になっている間は、その作業環境に対して \* バックアップのアクティブ化 \* ボタンが表示されます。このボタンは、作業環境でバックアップ機能を再度有効にする場合にクリックします。

## 作業環境のための Cloud Backup の登録を解除しています

バックアップ機能が不要になり、作業環境でバックアップの課金を停止する場合は、作業環境で Cloud Backup の登録を解除できます。通常、この機能は、作業環境を削除する予定で、バックアップサービスをキャンセルする場合に使用します。

この機能は、クラスタバックアップの格納先のオブジェクトストアを変更する場合にも使用できます。作業環境で Cloud Backup の登録を解除したら、新しいクラウドプロバイダ情報を使用してそのクラスタで Cloud Backup を有効にできます。

Cloud Backup の登録を解除する前に、次の手順をこの順序で実行する必要があります。

- 作業環境の Cloud Backup を非アクティブ化します
- その作業環境のバックアップをすべて削除します

登録解除オプションは、これら 2 つの操作が完了するまで使用できません。

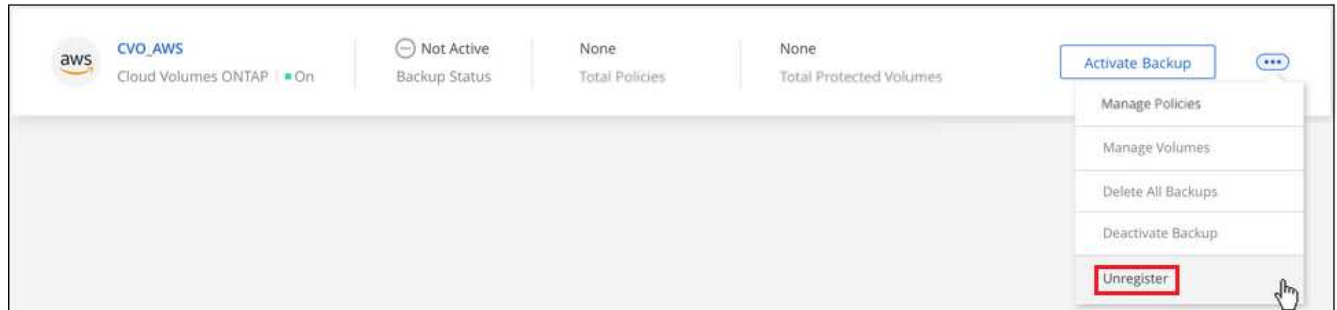
### 手順

1. [\* Volumes (ボリューム) ] タブで、[\* Backup Settings (バックアップ設定) ] を選択します。



ボタンを示すスクリーンショット。"]

2. バックアップ設定ページ で、をクリックします **...** アイコン"] バックアップ・サービスの登録を解除する作業環境では、**\* 登録解除 \*** を選択します。



3. 確認ダイアログボックスで、**\* 登録解除 \*** をクリックします。

## バックアップファイルからの **ONTAP** データのリストア

バックアップは、特定の時点のデータをリストアできるように、クラウドアカウントのオブジェクトストアに格納されます。ONTAP ボリューム全体をバックアップファイルからリストアすることも、一部のファイルのみをリストアする必要がある場合は、バックアップファイルから個々のファイルをリストアすることもできます。

元の作業環境、同じクラウドアカウントを使用している別の作業環境、またはオンプレミスの ONTAP システムに **\* ボリューム \*** を（新しいボリュームとして）リストアできます。

- **\* files \*** は、元の作業環境内のボリューム、同じクラウドアカウントを使用している別の作業環境内のボリューム、またはオンプレミスの ONTAP システム上のボリュームにリストアできます。

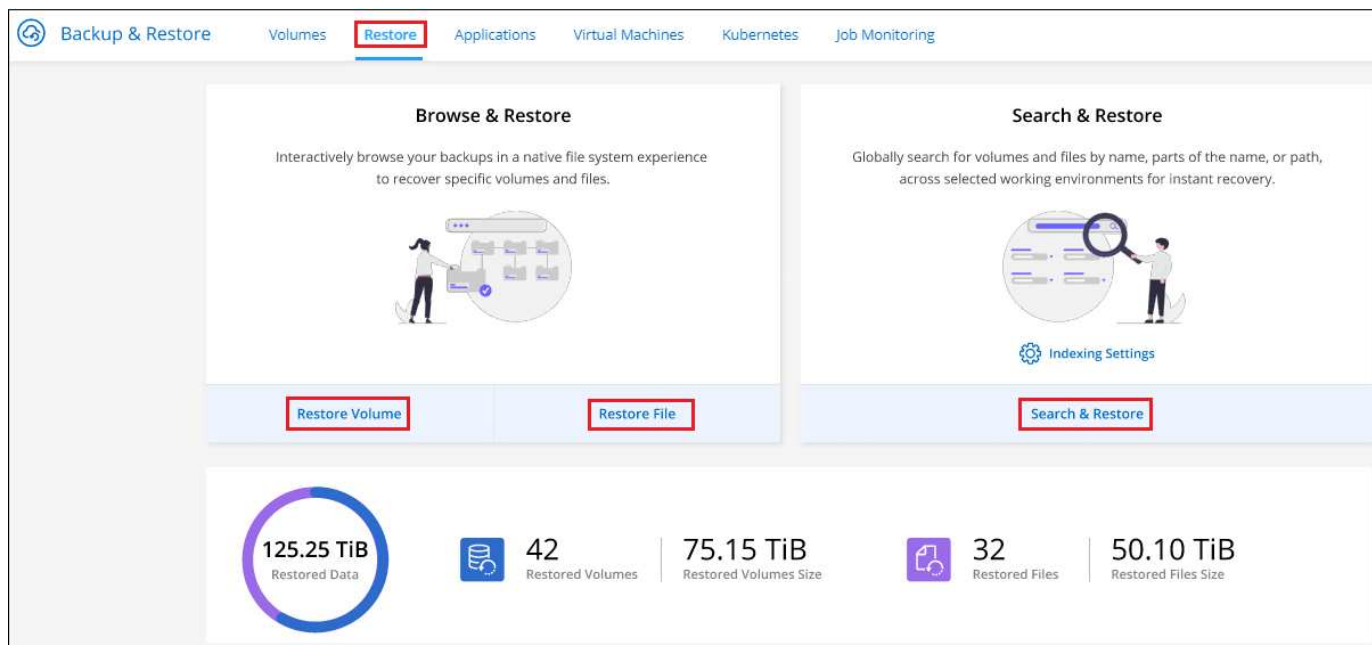
バックアップファイルから本番用システムにデータをリストアするには、有効な Cloud Backup ライセンスが必要です。

### リストアダッシュボード

リストアダッシュボードを使用して、ボリュームとファイルのリストア処理を実行できます。リストアダッシュボードにアクセスするには、Cloud Manager の上部にある **\* バックアップとリストア \*** をクリックし、**\* リストア \*** タブをクリックします。をクリックすることもできます **...** ボタン"] > **\* サービス・パネルからバックアップ / リストア・サービスのリストア・ダッシュボード \*** を表示します。



少なくとも 1 つの作業環境に対して Cloud Backup をアクティブ化しておく必要があります。また、初期バックアップファイルが存在する必要があります。



には「参照とリストア」または「検索とリストア」機能を使用するためのオプションが表示されます」

ご覧のように、リストアダッシュボードでは、\* 参照と復元 \* と \* 検索と復元 \* の 2 つの異なる方法でバックアップファイルからデータを復元できます。

## 参照と復元と検索と復元を比較します

一般的に、*Browse & Restore* は、特定のボリュームまたはファイルを過去 1 週間または 1 か月からリストアする必要がある場合に適しています。また、ファイルの名前と場所、およびファイルが最後に正常に作成された日付を把握している必要があります。*検索と復元* は、通常、ボリュームまたはファイルを復元する必要があるときに適していますが、正確な名前、保存されているボリューム、または最後に良好な状態になった日付は覚えていません。

この表は、2 つの方法の比較を示しています。

参照と復元	検索とリストア
フォルダ形式の構造を参照して、1 つのバックアップファイル内のボリュームまたはファイルを検索します	ボリューム名またはフルボリューム名、部分的またはフルファイル名、サイズ範囲、および追加の検索フィルタを指定して、すべてのバックアップファイル * 全体でボリュームまたはファイルを検索します
ボリュームとファイルのリストアは、Amazon S3、Azure Blob、Google Cloud、NetApp StorageGRID に格納されたバックアップファイルと連携します。	ボリュームとファイルのリストアは、Amazon S3 と Google Cloud に格納されたバックアップファイルと連携します
インターネットにアクセスできないサイトの StorageGRID からボリュームとファイルをリストアします	ダークサイトではサポートされない
では、名前が変更されたファイルや削除されたファイルは処理されません	新しく作成 / 削除 / 名前変更されたディレクトリと新しく作成 / 削除 / 名前変更されたファイル进行处理します
パブリッククラウドとプライベートクラウドの結果を参照できます	パブリッククラウドとローカル Snapshot コピーの結果を参照できます



参照と復元	検索とリストア
クラウドプロバイダのリソースを追加する必要はありません	アカウントごとにバケットとAWSまたはGoogleのリソースを追加する必要があります
クラウドプロバイダのコストを追加する必要はありません	バックアップとボリュームをスキャンして検索結果を表示するときに、AWSまたはGoogleのリソースにかかるコスト

いずれかのリストア方式を使用する前に、固有のリソース要件に対応するように環境を設定しておく必要があります。これらの要件については、以降のセクションで説明します。

使用するリストア処理のタイプに応じた要件とリストア手順を確認します。

- [ブラウズおよびリストアを使用してボリュームをリストアします](#)
- [ブラウズおよび復元を使用してファイルを復元します](#)
- [Search & Restore を使用してボリュームとファイルをリストアします](#)

## 参照と復元を使用した ONTAP データの復元

ボリュームまたはファイルのリストアを開始する前に、リストアするボリュームまたはファイルの名前、ボリュームが存在する作業環境の名前、およびリストア元のバックアップファイルのおおよその日付を確認しておく必要があります。

\*注：リストアするボリュームのバックアップファイルがアーカイブストレージ（ONTAP 9.10.1以降）にある場合、リストア処理にはより長い時間がかかり、コストが発生します。また、デスティネーションクラスタで ONTAP 9.10.1 以降が実行されている必要があります。

"[Azure アーカイブストレージからのリストアの詳細については、こちらをご覧ください](#)"。

サポートされている作業環境とオブジェクトストレージプロバイダの参照とリストア

ONTAP バックアップファイルから次の作業環境にボリュームまたは個々のファイルをリストアできます。

バックアップファイルの場所	デスティネーションの作業環境	
	* ボリュームの復元 *	ファイルのリストア ifdef : aws []
Amazon S3	オンプレミスの AWS ONTAP システムに Cloud Volumes ONTAP が導入されている	AWSオンプレミスONTAP システムのCloud Volumes ONTAP 。endif : aws [] ifdef : azure[]
Azure Blob の略	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入	AzureオンプレミスONTAP システムのCloud Volumes ONTAP 。endif : azure[] ifdef : gCP[]
Google クラウドストレージ	Google オンプレミス ONTAP システムの Cloud Volumes ONTAP	GoogleオンプレミスONTAP システムのCloud Volumes ONTAP : GCP[]
NetApp StorageGRID	オンプレミスの ONTAP システム	オンプレミスの ONTAP システム

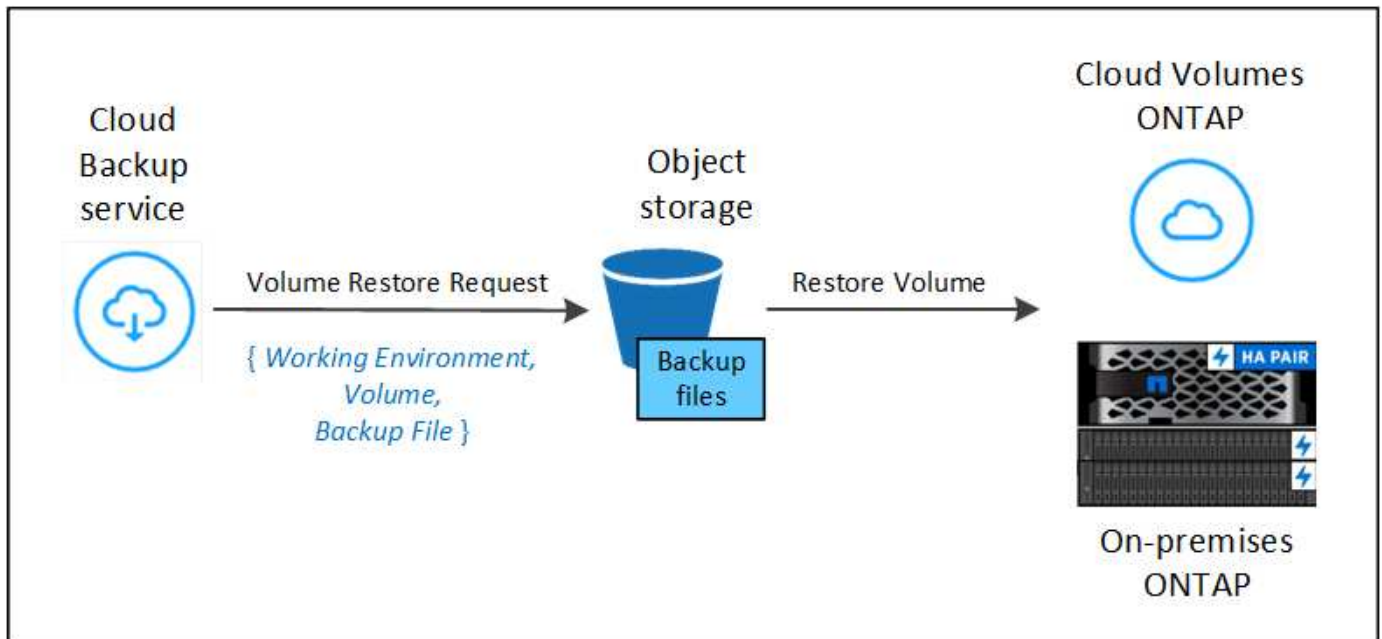
「オンプレミス ONTAP システム」とは、FAS、AFF、ONTAP Select の各システムを指します。



バックアップファイルがアーカイブストレージにある場合は、ボリュームリストアのみがサポートされます。Browse & Restore の使用時に、アーカイブストレージからのファイルのリストアは現在サポートされていません。

### Browse & Restore を使用してボリュームをリストアする

バックアップファイルからボリュームをリストアすると、Cloud Backup はバックアップのデータを使用して `_new_volume` を作成します。データは、元の作業環境のボリューム、またはソースの作業環境と同じクラウドアカウントにある別の作業環境にリストアできます。オンプレミスの ONTAP システムにボリュームをリストアすることもできます。



この出力からわかるように、ボリュームリストアを実行するには、作業環境名、ボリューム名、バックアップファイルの日付を確認しておく必要があります。

次のビデオでは、ボリュームのリストア手順を簡単に紹介しています。

# Cloud Backup Service: Restore Demo

Powered by Cloud Manager

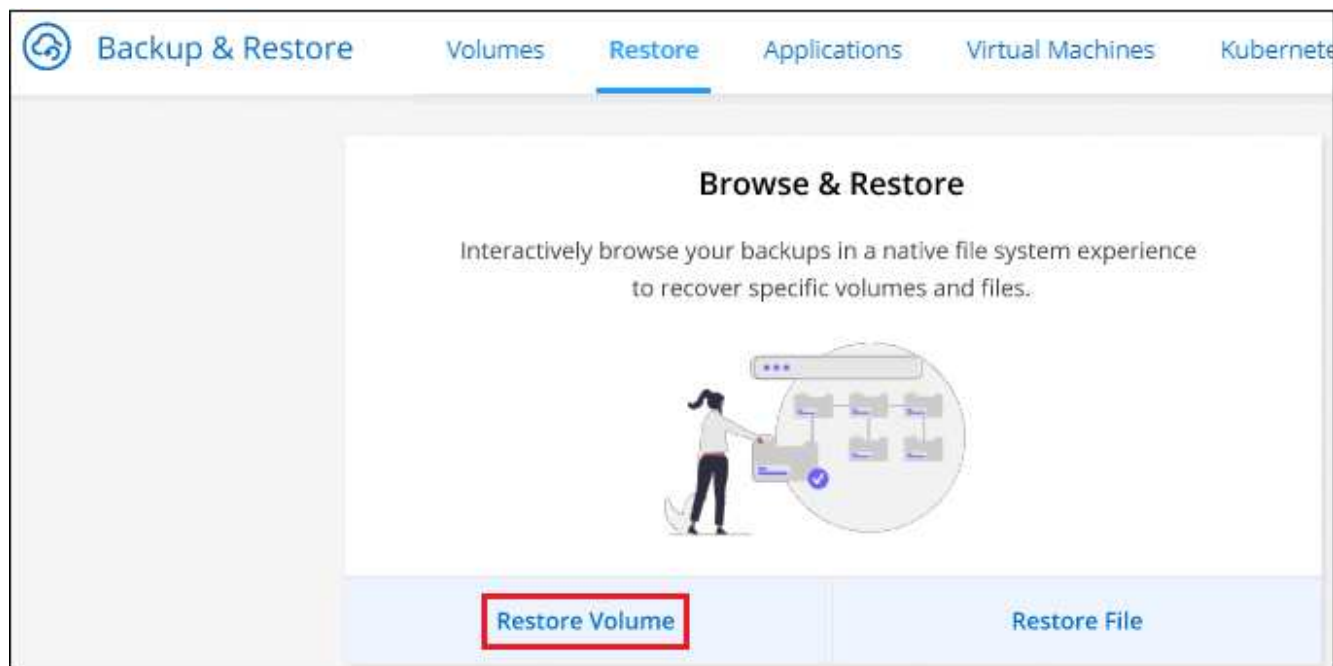
January 2022

 NetApp

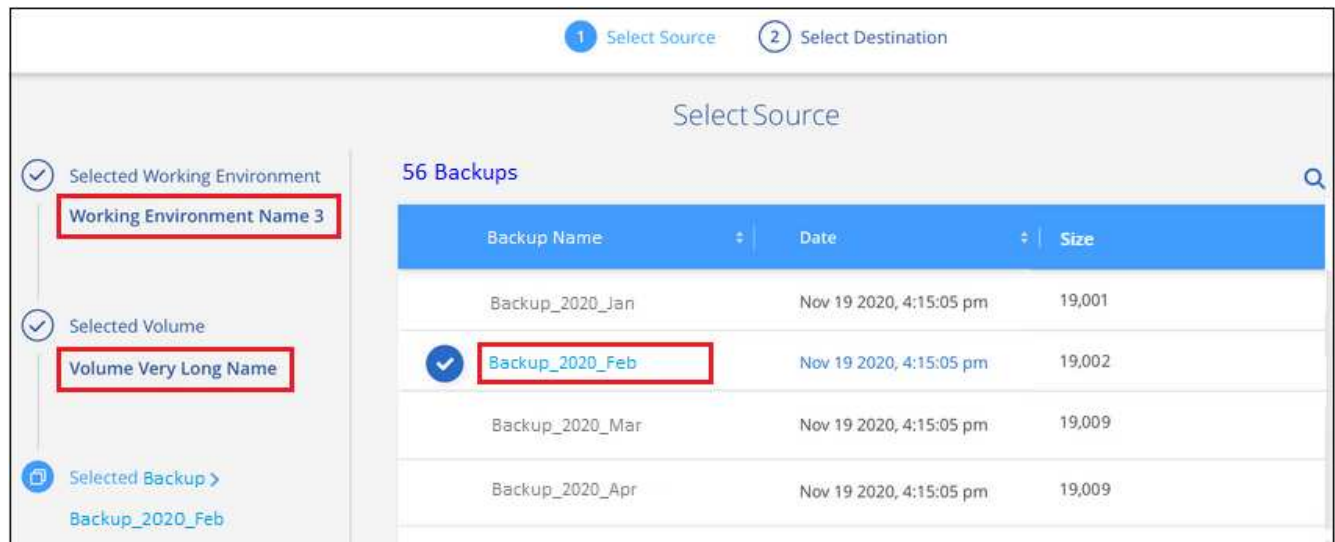


## 手順

1. Backup & Restore \* サービスを選択します。
2. [\* Restore \* (復元) ] タブをクリックすると、[Restore Dashboard (復元ダッシュボード) ] が表示されます。
3. [Browse & Restore] セクションで、[\* Restore Volume] をクリックします。

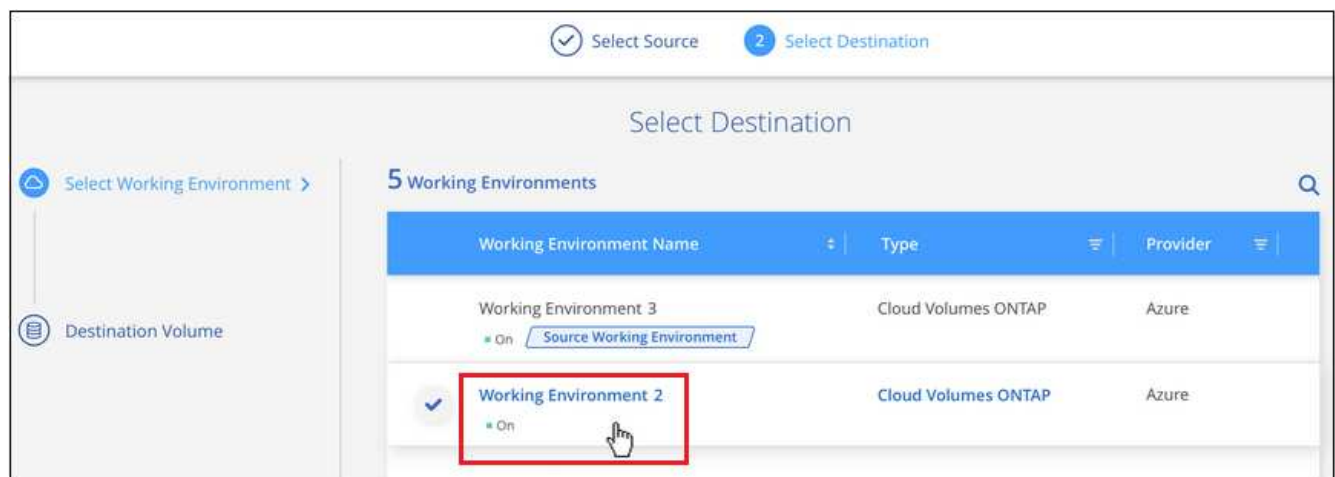


4. [ソースの選択] ページで、リストアするボリュームのバックアップ・ファイルに移動します。リストア元の日付 / 時刻スタンプを含む \* Working Environment \*、\* Volume \*、および \* Backup \* ファイルを選択します。



5. [\* Continue (続行) ] をクリックします

6. [ リストア先の選択 ] ページで、ボリュームをリストアする \* 作業環境 \* を選択します。



7. オンプレミスの ONTAP システムを選択し、オブジェクトストレージへのクラスタ接続をまだ設定していない場合は、追加情報を入力するように求められます。

- Azure Blob からリストアする場合は、デスティネーションボリュームを配置する ONTAP クラスタ内の IPspace を選択し、オブジェクトストレージにアクセスする Azure サブスクリプションを選択します。また、VNet とサブネットを選択して、データ転送を安全に行うプライベートエンドポイントを選択することもできます。
- StorageGRID StorageGRID からリストアする場合は、StorageGRID サーバの FQDN と ONTAP との HTTPS 通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキー、およびデスティネーションボリュームを配置する ONTAP クラスタの IPspace を選択します。
  - a. リストアしたボリュームに使用する名前を入力し、ボリュームを配置する Storage VM を選択します。デフォルトでは、\* <source\_volume\_name> \_ Restore \* がボリューム名として使用されます。

ボリュームの容量に使用するアグリゲートは、オンプレミスの ONTAP システムにボリュームをリストアする場合にのみ選択できます。

また、（ONTAP 9.10.1 以降で使用可能な）アーカイブストレージ階層にあるバックアップファイルからボリュームをリストアする場合は、リストア優先度を選択できます。

"Azure アーカイブストレージからのリストアの詳細については、[こちらをご覧ください](#)。"

1. リストアの進行状況を確認できるように、\* リストア \* をクリックするとリストアダッシュボードに戻ります。

Cloud Backup は、選択したバックアップに基づいて新しいボリュームを作成します。可能です "[この新しいボリュームのバックアップ設定を管理します](#)" 必要に応じて。

アーカイブストレージにあるバックアップファイルからボリュームをリストアする場合は、アーカイブ階層とリストアの優先順位によって数分から数時間かかることがあります。[\* ジョブ・モニタ \*] タブをクリックすると、リストアの進行状況を確認できます。

#### 参照と復元を使用した ONTAP ファイルの復元

ONTAP のバックアップから数ファイルしかリストアしない場合は、ボリューム全体をリストアするのではなく、ファイルを個別にリストアすることもできます。ファイルは元の作業環境の既存のボリューム、または同じクラウドアカウントを使用している別の作業環境にリストアできます。オンプレミスの ONTAP システム上のボリュームにファイルをリストアすることもできます。

複数のファイルを選択した場合は、選択したデスティネーションボリュームにすべてのファイルがリストアされます。したがって、ファイルを別のボリュームにリストアする場合は、リストアプロセスを複数回実行する必要があります。



バックアップファイルがアーカイブストレージにある場合、個々のファイルをリストアすることはできません。この場合、アーカイブされていない新しいバックアップファイルからファイルをリストアしたり、アーカイブされたバックアップからボリューム全体をリストアして必要なファイルにアクセスしたり、検索とリストアを使用してファイルをリストアしたりできます。

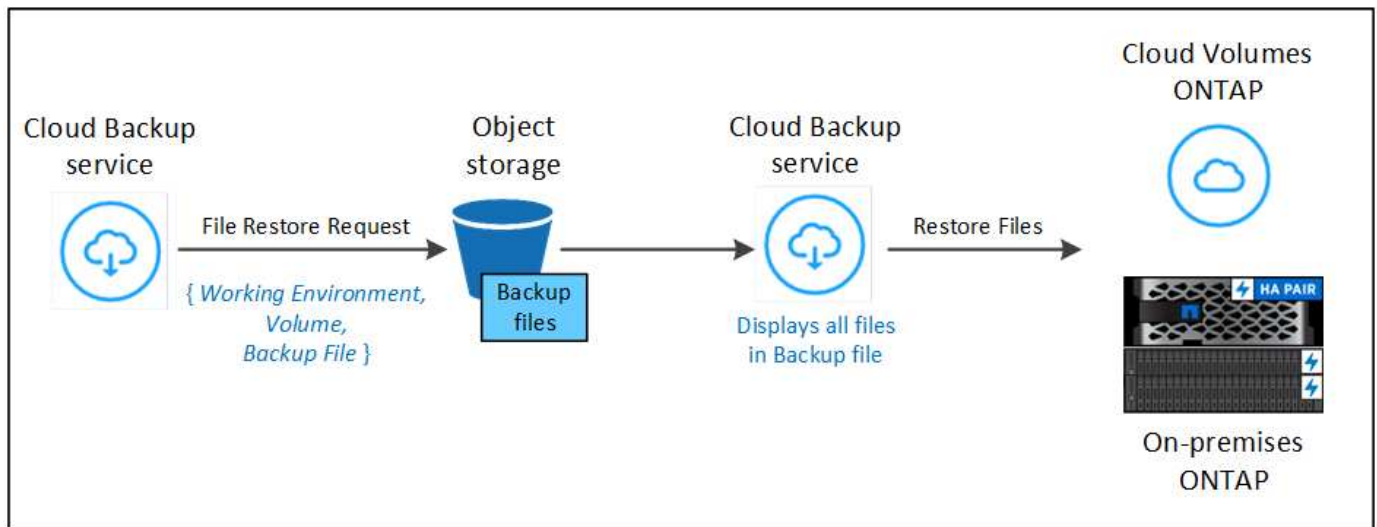
#### 前提条件

- ファイルリストア処理を実行するには、Cloud Volumes ONTAP またはオンプレミスの ONTAP システムで ONTAP のバージョンが 9.6 以降である必要があります。

## ファイルのリストアプロセス

プロセスは次のようになります。

1. ボリュームバックアップから 1 つ以上のファイルを復元する場合は、\* リストア \* タブをクリックし、参照 & 復元 の下の \* ファイルの復元 \* をクリックして、ファイル（またはファイル）が存在するバックアップファイルを選択します。
2. Cloud Backupに、選択したバックアップファイル内に存在するフォルダとファイルが表示されます。
3. バックアップからリストアするファイル（複数可）を選択します。
4. ファイル（作業環境、ボリューム、およびフォルダ）をリストアする場所を選択し、\* リストア \* をクリックします。
5. ファイルがリストアされます。



このように、ファイルのリストアを実行するには、作業環境名、ボリューム名、バックアップファイルの日付、およびファイル名を把握しておく必要があります。

**Browse & Restore** を使用してファイルを復元します

ONTAP ボリュームのバックアップからボリュームにファイルをリストアするには、次の手順を実行します。ボリュームの名前と、ファイルのリストアに使用するバックアップファイルの日付を確認しておく必要があります。この機能では、ライブブラウズを使用して、各バックアップファイル内のディレクトリとファイルのリストを表示できます。

次のビデオでは、1 つのファイルをリストアする手順を簡単に紹介します。



# Cloud Backup Service: Restore Demo

Powered by Cloud Manager

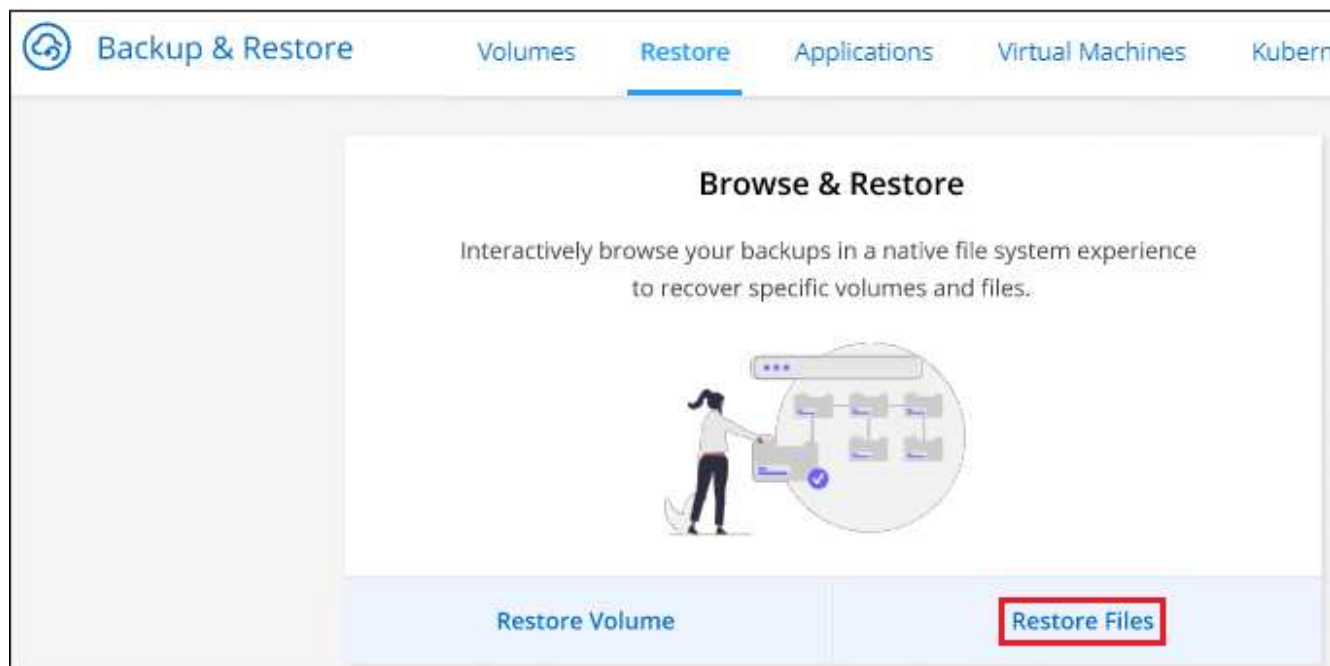
January 2022

 NetApp



## 手順

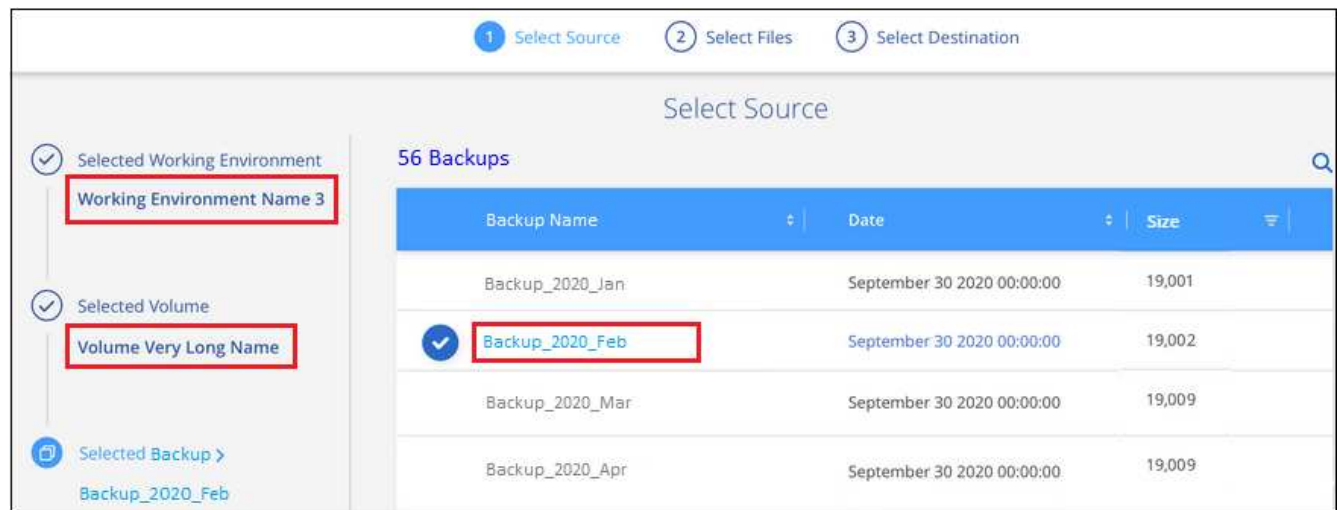
1. Backup & Restore \* サービスを選択します。
2. [\* Restore \* (復元) ] タブをクリックすると、[Restore Dashboard (復元ダッシュボード) ] が表示されます。
3. [ 参照と復元 ] セクションで、[ ファイルの復元 \* ] をクリックします。



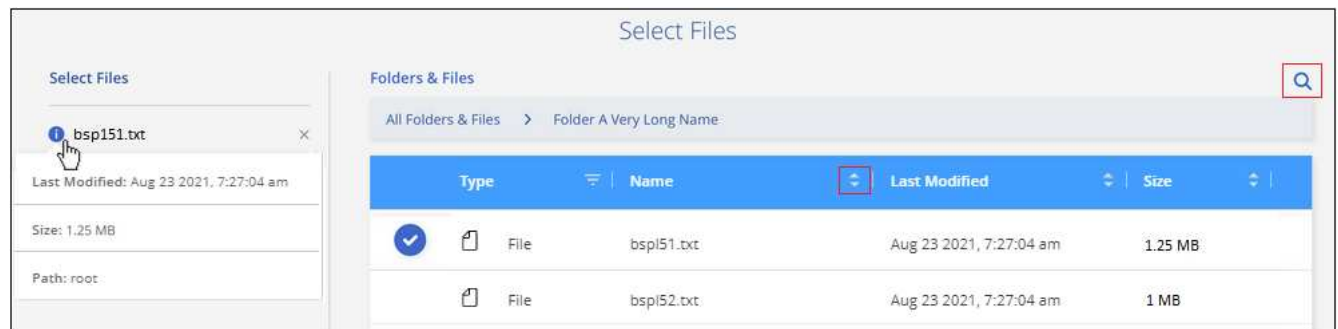
ボタンを選択するスクリーンショット。"]

4. [ ソースの選択 ] ページで ' リストアするファイルを含むボリュームのバックアップ・ファイルに移動します  
ファイルのリストア元の日付 / タイムスタンプを持つ \* 作業環境 \*、\* ボリューム \*、および \* バック

アップ \* を選択します。



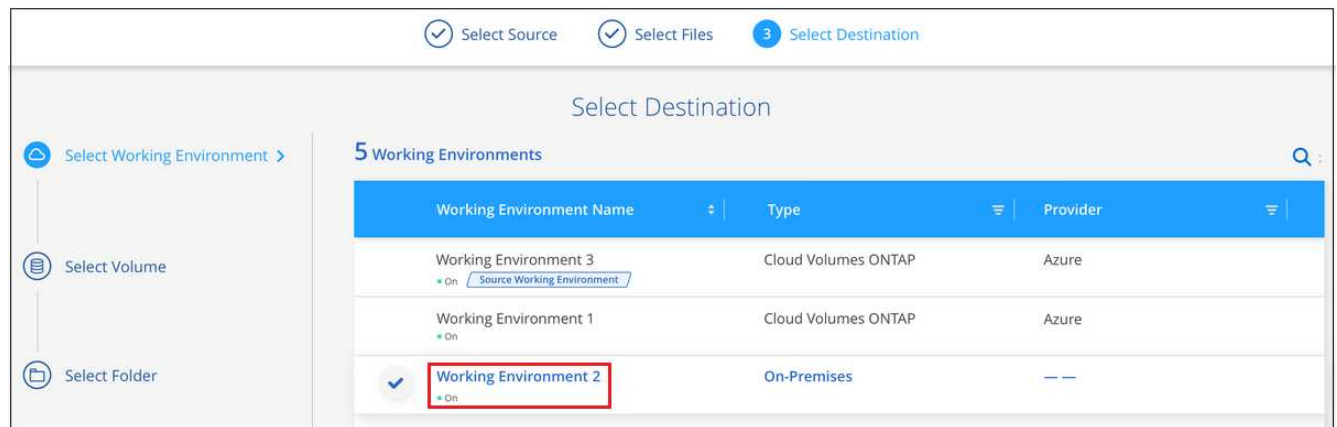
5. [\* Continue (続行) ]をクリックすると、ボリュームバックアップのフォルダとファイルのリストが表示されます。



6. \_ファイルの選択\_ ページで、復元するファイルを選択し、\* 続行 \* をクリックします。ファイルの検索を支援するために、次の手順を実行します。
- ファイル名が表示されている場合は、そのファイル名をクリックします。
  - 検索アイコンをクリックしてファイル名を入力すると、そのファイルに直接移動できます。
  - を使用して、フォルダ内の下位レベルに移動できます ▶ ボタンをクリックして、ファイルを検索します。

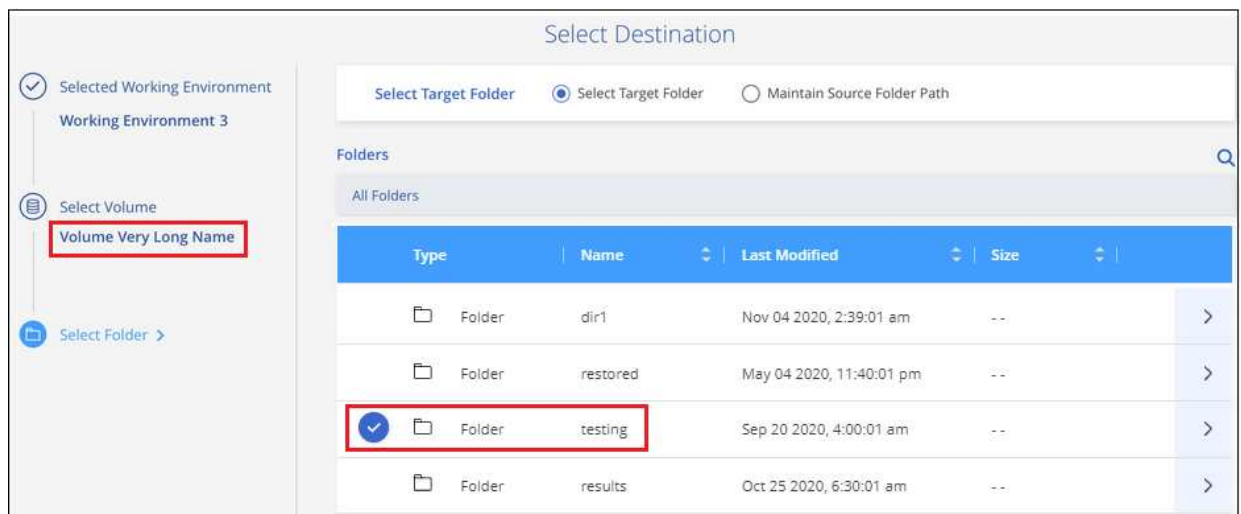
ファイルを選択すると、ページの左側に追加され、選択済みのファイルが表示されます。必要に応じて、ファイル名の横にある \* x \* をクリックすると、このリストからファイルを削除できます。

7. 保存先の選択ページで、ファイルを復元する \* 作業環境 \* を選択します。



オンプレミスクラスタを選択し、オブジェクトストレージへのクラスタ接続をまだ設定していない場合は、追加情報を入力するように求められます。

- Azure Blob からリストアする場合は、デスティネーションボリュームが配置されている ONTAP クラスタ内の IPspace を入力します。
- StorageGRID からリストアする場合は、StorageGRID サーバのFQDNとONTAP とのHTTPS通信に使用するポートを入力し、オブジェクトストレージへのアクセスに必要なアクセスキーとシークレットキー、およびデスティネーションボリュームが配置されているONTAP クラスタのIPspaceを入力します。
- a. 次に、ファイルを復元する \* Volume \* と \* Folder \* を選択します。



ファイルを復元する場合は、いくつかのオプションがあります。

- 上の図のように、[ ターゲットフォルダの選択 ] を選択した場合は、次のようになります。
  - 任意のフォルダを選択できます。
  - フォルダにカーソルを合わせて、をクリックできます ▶ 行の末尾にあるサブフォルダをドリルダウンし、フォルダを選択します。
- ソースファイルがある場所と同じ宛先作業環境とボリュームを選択した場合は、「ソースフォルダーパスを保持」を選択して、ソース構造内に存在していた同じフォルダーにファイルまたはすべてのファイルを復元できます。同じフォルダとサブフォルダがすべて存在する必要があります。フォルダは作成されません。

- a. リストアの進行状況を確認できるように、\* リストア \* をクリックするとリストアダッシュボードに戻ります。また、\* Job Monitor \* タブをクリックしてリストアの進捗状況を確認することもできます。

## 検索とリストアを使用した **ONTAP** データのリストア

検索とリストアを使用して、ONTAP バックアップファイルからボリュームまたは個々のファイルをリストアできます。検索とリストアでは、クラウドストレージに保存されているすべてのバックアップから特定のプロバイダの特定のボリュームまたはファイルを検索して、リストアを実行できます。正確な作業環境名やボリューム名がわからなくても、検索ではすべてのボリュームのバックアップファイルが検索されます。

検索処理では、ONTAP ボリュームに対応するすべてのローカル Snapshot コピーも検索されます。ローカル Snapshot コピーからデータをリストアする方が、バックアップファイルからリストアするよりも高速で低コストなので、Snapshot からデータをリストアできます。スナップショットは、キャンバスのボリュームの詳細ページから新しいボリュームとして復元できます。

バックアップファイルからボリュームをリストアすると、Cloud Backup はバックアップのデータを使用して new volume を作成します。データは、元の作業環境のボリュームとしてリストアすることも、ソースの作業環境と同じクラウドアカウントにある別の作業環境にリストアすることもできます。オンプレミスの ONTAP システムにボリュームをリストアすることもできます。

ファイルは、元のボリュームの場所、同じ作業環境内の別のボリューム、または同じクラウドアカウントを使用している別の作業環境にリストアできます。オンプレミスの ONTAP システム上のボリュームにファイルをリストアすることもできます。

リストアするボリュームのバックアップファイルがアーカイブストレージ（ONTAP 9.10.1以降で使用可能）にある場合、リストア処理にはより長い時間がかかり、追加コストが発生します。デスティネーションクラスターで ONTAP 9.10.1 以降が実行されている必要があり、そのファイルをアーカイブストレージからリストアすることは現在サポートされていません。

開始する前に、リストアするボリュームやファイルの名前や場所を把握しておく必要があります。

次のビデオでは、1つのファイルをリストアする手順を簡単に紹介します。

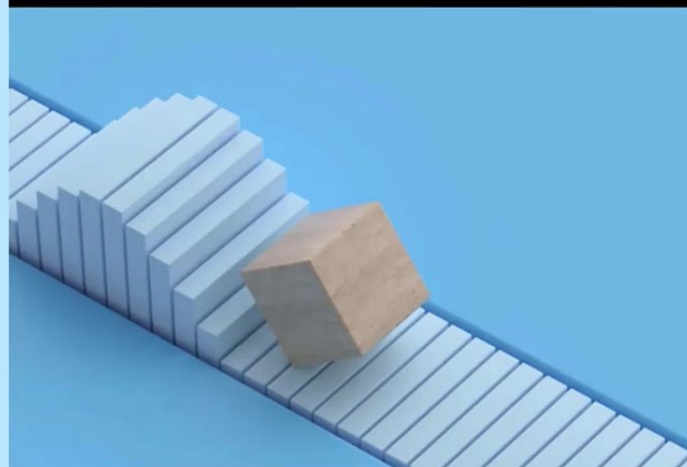
# Cloud Backup : Search and Restore

Indexed Catalog Preview Feature

February 2022

© 2022 NetApp, Inc. All rights reserved.

 NetApp



サポートされている作業環境とオブジェクトストレージプロバイダの検索とリストア

ONTAP バックアップファイルから次の作業環境にボリュームまたは個々のファイルをリストアできます。

バックアップファイルの場所	デスティネーションの作業環境	
	* ボリュームの復元 *	ファイルのリストア <code>ifdef : aws []</code>
Amazon S3	オンプレミスの AWS ONTAP システムに Cloud Volumes ONTAP が導入されている	AWS オンプレミス ONTAP システムの Cloud Volumes ONTAP 。 <code>endif : aws [] ifdef : azure []</code>
Azure Blob の略	現在サポートされていません	<code>endif : azure [] ifdef : GCP []</code>
Google クラウドストレージ	Google オンプレミス ONTAP システムの Cloud Volumes ONTAP	Google オンプレミス ONTAP システムの Cloud Volumes ONTAP : <code>GCP []</code>
NetApp StorageGRID	現在サポートされていません	

「オンプレミス ONTAP システム」とは、FAS、AFF、ONTAP Select の各システムを指します。

## 前提条件

- クラスタの要件：
  - ONTAP のバージョンは 9.8 以降である必要があります。
  - ボリュームが配置されている Storage VM（SVM）に設定済みのデータ LIF が必要です。
  - ボリュームで NFS が有効になっている必要があります。
  - SVM で SnapDiff RPC サーバをアクティブ化する必要があります。作業環境でインデックスの作成を有効にすると、Cloud Manager によって自動的にインデックス作成が実行されます。

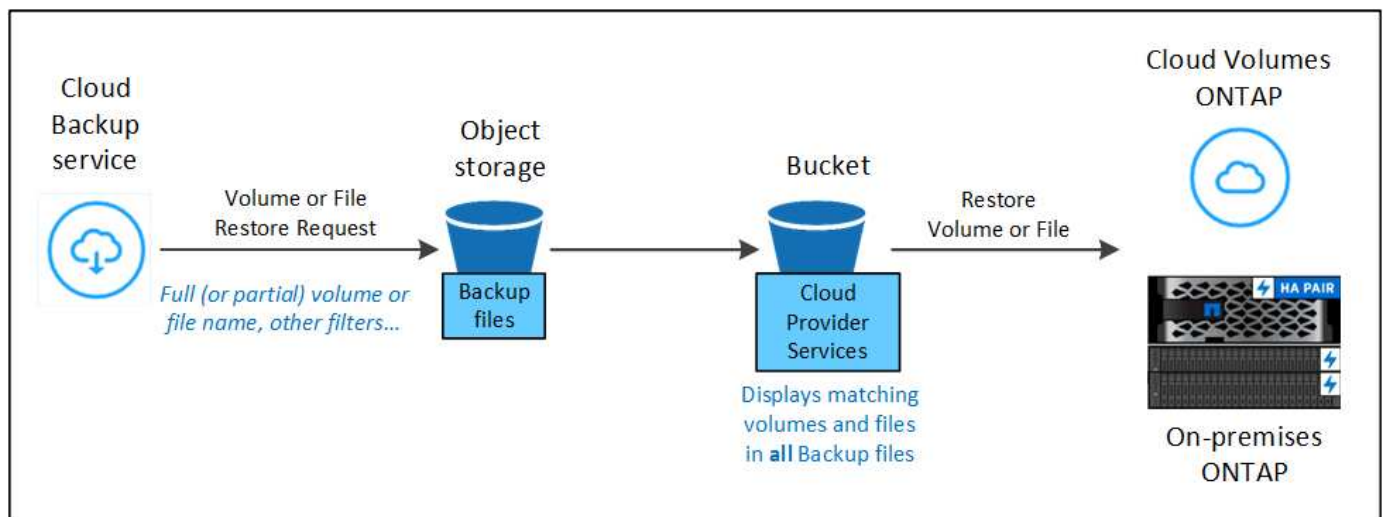
## 検索とリストアのプロセス

プロセスは次のようになります。

1. 検索とリストアを使用する前に、ボリュームまたはファイルをリストアする各ソース作業環境でインデックス作成を有効にする必要があります。これにより、Indexed Catalog は、すべてのボリュームのバックアップファイルを追跡できます。
2. ボリュームバックアップからボリュームまたはファイルを復元する場合は、\_ 検索と復元 \_ で \* 検索と復元 \* をクリックします。
3. ボリューム名またはファイルの一部または全体の名前、ファイル名の一部または全部、サイズの範囲、作成日の範囲、その他の検索フィルタを入力し、\* 検索 \* をクリックします。

検索結果ページには、検索条件に一致するファイルまたはボリュームを含むすべての場所が表示されます。

4. ボリュームまたはファイルの復元に使用する場所の \* すべてのバックアップの表示 \* をクリックし、実際に使用するバックアップファイルの \* 復元 \* をクリックします。
5. ボリュームまたはファイルをリストアする場所を選択し、\* リストア \* をクリックします。
6. ボリュームまたはファイルがリストアされます。



ご覧のように、必要なのはボリュームやファイルの一部だけです。Cloud Backup では、検索条件に一致するすべてのバックアップファイルが検索されます。

### 各作業環境のインデックスカタログを有効にする

検索とリストアを使用する前に、ボリュームまたはファイルのリストア元となる各ソース作業環境でインデックス作成を有効にする必要があります。これにより、インデックスカタログですべてのボリュームとすべてのバックアップファイルを追跡できるため、検索をすばやく効率的に実行できます。

この機能を有効にすると、ボリュームに対してCloud BackupがSVMでSnapDiff v3を有効にし、次の処理を実行します。

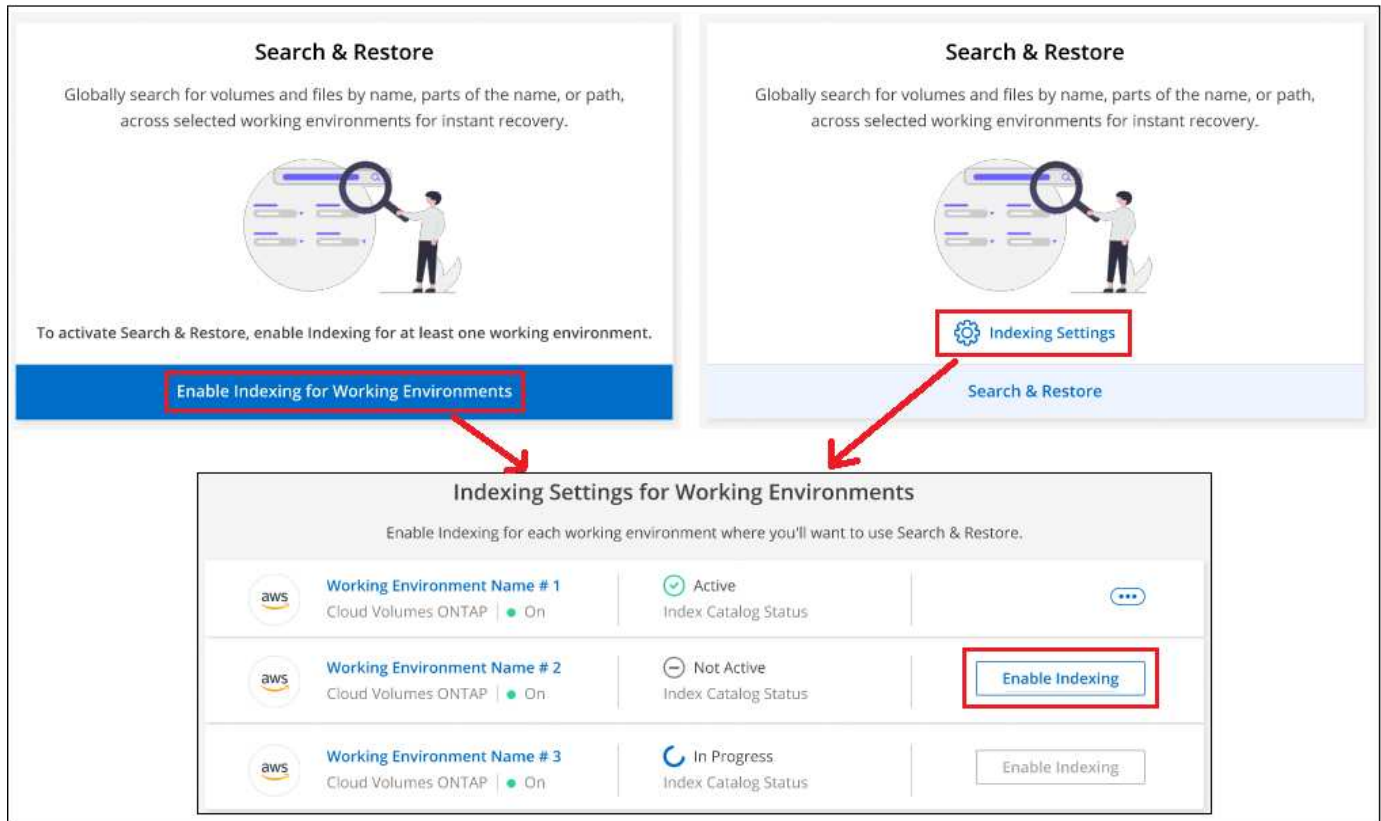
作業環境でインデックス作成がすでに有効になっている場合は、次のセクションに進んでデータをリストアしてください。



作業環境でインデックス作成を有効にするには：

- 作業環境にインデックスが作成されていない場合は、リストアダッシュボードの *Search&Restore* で \* 作業環境でインデックス作成を有効にする \* をクリックし、作業環境で \* インデックス作成を有効にする \* をクリックします。
- 少なくとも 1 つの作業環境にインデックスが作成されている場合は、リストアダッシュボードの *Search & Restore* で、\* インデックス設定 \* をクリックし、作業環境で \* インデックス作成を有効にする \* をクリックします。

すべてのサービスがプロビジョニングされ、インデックスカタログがアクティブ化されると、作業環境は「アクティブ」と表示されます。



作業環境内のボリュームのサイズとクラウド内のバックアップファイルの数によっては、最初のインデックス作成プロセスに最大 1 時間かかることがあります。その後は、1 時間ごとに差分変更を反映して透過的に更新され、最新の状態が維持されます。

検索とリストアを使用したボリュームとファイルのリストア

お先にどうぞ [作業環境のインデックス作成を有効にしました](#) では、検索とリストアを使用してボリュームまたはファイルをリストアできます。これにより、幅広いフィルタを使用して、すべてのバックアップファイルからリストアするファイルまたはボリュームを検索できます。

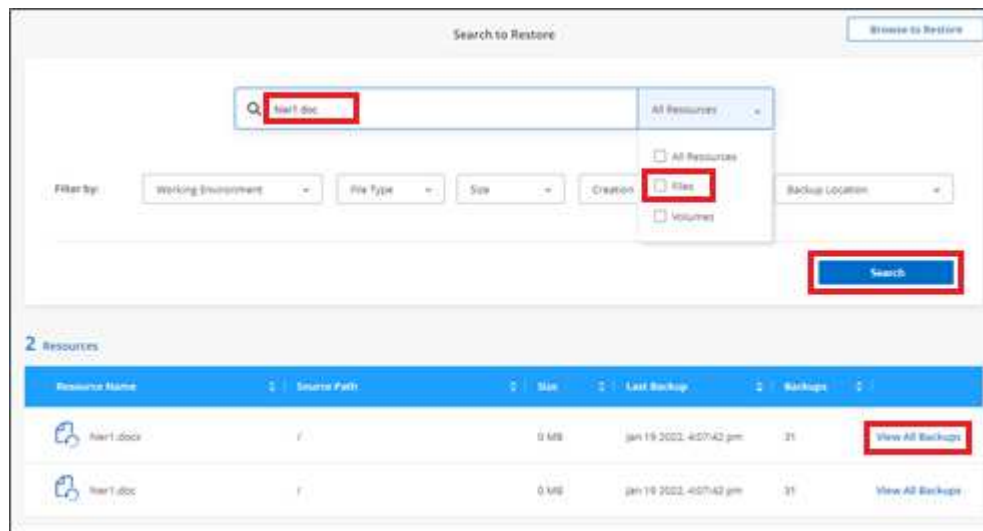
手順

1. Backup & Restore \* サービスを選択します。
2. [\* Restore \* (復元) ] タブをクリックすると、[Restore Dashboard (復元ダッシュボード) ] が表示されます。
3. [ 検索と復元 ] セクションで、[ \* 検索と復元 \* ] をクリックします。



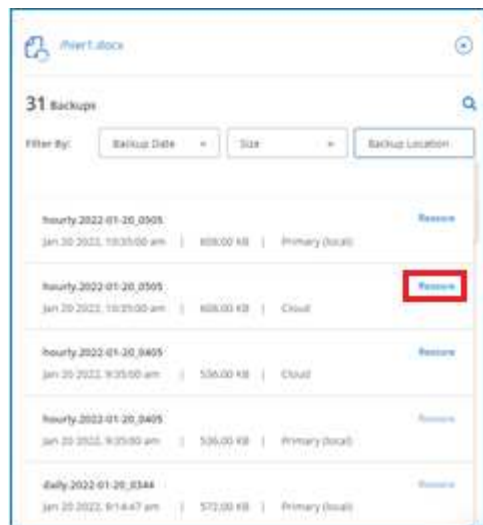
ボタンを選択するスクリーンショット。"]

4. [ 検索と復元 ] ページで、次の操作を行います。
  - a. 検索バーに、ボリューム名またはファイル名の全体または一部を入力します。
  - b. [ フィルタ ( Filter ) ] 領域で、フィルタ条件を選択する。たとえば、データが存在する作業環境を選択し、.doc ファイルなどのファイルタイプを選択できます。
5. [ \* 検索 ( \* Search ) ] をクリックすると、[ 検索結果 ( Search Results ) ] 領域に、検索に一致するファイルまたはボリュームを持つすべての場所が表示されます。



ページに表示されます"]

6. 復元するデータが格納されている場所の \* すべてのバックアップの表示 \* をクリックして、そのボリュームまたはファイルが含まれているすべてのバックアップファイルを表示します。



- クラウドからボリュームまたはファイルを復元するために使用するバックアップファイルに対して、\* 復元 \* をクリックします。

検索結果からは、検索結果にファイルが含まれているローカルボリュームの Snapshot コピーも特定されます。この時点では、スナップショットに対して \* リストア \* ボタンは機能しませんが、バックアップファイルではなく Snapshot コピーからデータをリストアする場合は、ボリュームの名前と場所を書き留め、キャンバスのボリュームの詳細ページを開きます。および \* Restore from Snapshot copy \* オプションを使用します。

- ボリュームまたはファイルをリストアする場所を選択し、\* リストア \* をクリックします。

- ファイルの場合は、元の場所にリストアするか、別の場所を選択できます
- ボリュームの場所は選択できます。

ボリュームまたはファイルがリストアされ、リストアダッシュボードに戻ります。これにより、リストア処理の進捗状況を確認できます。また、\* Job Monitor \* タブをクリックしてリストアの進捗状況を確認することもできます。

リストアしたボリュームに対しては、を実行できます ["この新しいボリュームのバックアップ設定を管理します"](#) 必要に応じて。

# Kubernetes データのバックアップとリストア

## Cloud Backup を使用して Kubernetes クラスタのデータを保護

Cloud Backup は、Kubernetes クラスタデータを保護し、長期アーカイブするためのバックアップおよびリストア機能を提供します。バックアップは自動的に生成され、パブリックまたはプライベートクラウドアカウントのオブジェクトストアに格納されます。

必要に応じて、バックアップから同じ作業環境または別の作業環境に全面的に `_ ボリューム _` をリストアできます。

### の機能

バックアップ機能：

- ・ 永続ボリュームの独立したコピーを低コストのオブジェクトストレージにバックアップできます。
- ・ クラスタ内のすべてのボリュームに単一のバックアップポリシーを適用するか、または一意のリカバリポイント目標が設定されたボリュームに異なるバックアップポリシーを割り当てます。
- ・ バックアップデータは、転送中の AES-256 ビット暗号化と TLS 1.2 HTTPS 接続によって保護されます。
- ・ 単一ボリュームで最大 4、000 個のバックアップがサポートされます。

リストア機能：

- ・ 特定の時点からデータをリストアします。
- ・ ボリュームをソースシステムまたは別のシステムにリストアします。
- ・ 元の ACL を維持したまま、指定した場所にデータを直接配置して、ブロックレベルでデータをリストアします。

### サポートされている Kubernetes 作業環境とオブジェクトストレージプロバイダ

Cloud Backup を使用すると、以下の作業環境から以下のパブリックおよびプライベートクラウドプロバイダのオブジェクトストレージに Kubernetes ボリュームをバックアップできます。

ソースの作業環境	バックアップファイルデスティネーション <code>ifdef : aws []</code>
AWS の Kubernetes クラスタ	Amazon S3 <code>endif : aws []ifdef : azure[]</code>
Azure の Kubernetes クラスタ	Azure Blob <code>endif : Azure[] ifdef : GCP []</code>
Google の Kubernetes クラスタ	Google Cloud Storage <code>endif : GCP []</code>

Kubernetes バックアップファイルから次の作業環境にボリュームをリストアできます。

バックアップファイルの場所	デスティネーション作業環境 <code>ifdef : aws []</code>
Amazon S3	AWS <code>endif</code> のKubernetesクラスタ： <code>aws [] ifdef : azure[]</code>

バックアップファイルの場所	デスティネーション作業環境ifdef : aws []
Azure Blob の略	Azure endifのKubernetesクラスタ : azure[] ifdef : gCP[]
Google クラウドストレージ	Google endifのKubernetesクラスタ : GCP []

## コスト

Cloud Backup の使用に関連するコストには、リソース料金とサービス料金の 2 種類があります。

### ・リソース料金 \*

クラウド内のオブジェクトストレージの容量については、リソースの料金がクラウドプロバイダに支払われます。クラウドバックアップではソースボリュームの Storage Efficiency が保持されるため、クラウドプロバイダ側で、data\_after\_ONTAP 効率化のコストを支払います（重複排除と圧縮が適用されたあとのデータ量が少ないほど）。

### ・サービス料金 \*

サービス料金はネットアップにお支払いいただき、バックアップの作成時とリストア時のコストの両方を負担させていただきます。保護するデータの料金は、オブジェクトストレージにバックアップされるボリュームのソースの使用済み論理容量（ONTAP 効率化）で計算されます。この容量はフロントエンドテラバイト（FETB）とも呼ばれます。

バックアップサービスの料金を支払う方法は 2 つあります。1 つ目は、クラウドプロバイダを利用して月額料金を支払う方法です。2 つ目の選択肢は、ネットアップから直接ライセンスを購入することです。を参照してください [ライセンス](#) 詳細については、を参照してください

## ライセンス

Cloud Backup には、従量課金制（PAYGO）とお客様所有のライセンス（BYOL）の 2 つのライセンスオプションがあります。ライセンスをお持ちでない場合は、30 日間の無償トライアルをご利用いただけます。

無償トライアルをご利用ください

30 日間の無償トライアルを使用すると、残りの無料試用日数が通知されます。無償トライアルが終了すると、バックアップは作成されなくなります。サービスを引き続き使用するには、サービスに登録するかライセンスを購入する必要があります。

サービスが無効になってもバックアップファイルは削除されません。バックアップを削除しないかぎり、バックアップで使用する容量のオブジェクトストレージのコストは引き続きクラウドプロバイダから請求されます。

### 従量課金制のサブスクリプション

Cloud Backup は従量課金制モデルで、使用量に応じたライセンスを提供します。クラウドプロバイダの市場に登録した後は、バックアップされたデータに対して GB 単位の支払いを行います。つまり、前払いによる支払いはありません。クラウドプロバイダから月額料金で請求されます。

無償トライアルを利用されている場合や、お客様が独自のライセンスを使用（BYOL）されている場合も、サブスクリプションを設定する必要があります。

### ・登録すると、無料トライアルの終了後にサービスが中断されることがなくなります。

試用期間が終了すると、バックアップしたデータの量に応じて 1 時間ごとに課金されます。

- BYOL ライセンスで許可されている数を超えるデータをバックアップした場合、データバックアップは従量課金制サブスクリプションを使用して続行されます。

たとえば、10 TB の BYOL ライセンスがある場合、10 TB を超える容量はすべて、PAYGO サブスクリプションによって課金されます。

お客様は、無料トライアル期間中、または BYOL ライセンスを超えていない場合は、従量課金制サブスクリプションから料金を請求されることはありません。

["従量課金制サブスクリプションの設定方法について説明します"](#)。

お客様所有のライセンスを使用

BYOL は、期間ベース（12 カ月、24 カ月、36 カ月）の \_ と \_ の容量ベースで、1 TB 単位での増分に基づいています。ネットアップに料金を支払って、1 年分のサービスを使用し、最大容量である 10TB を支払うことになります。

サービスを有効にするために、Cloud Manager のデジタルウォレットのページに入力したシリアル番号が表示されます。いずれかの制限に達すると、ライセンスを更新する必要があります。Backup BYOL ライセンス環境では、に関連付けられているすべてのソースシステムがライセンスされます ["Cloud Manager アカウント"](#)。

["BYOL ライセンスの管理方法について説明します"](#)。

## Cloud Backup の仕組み

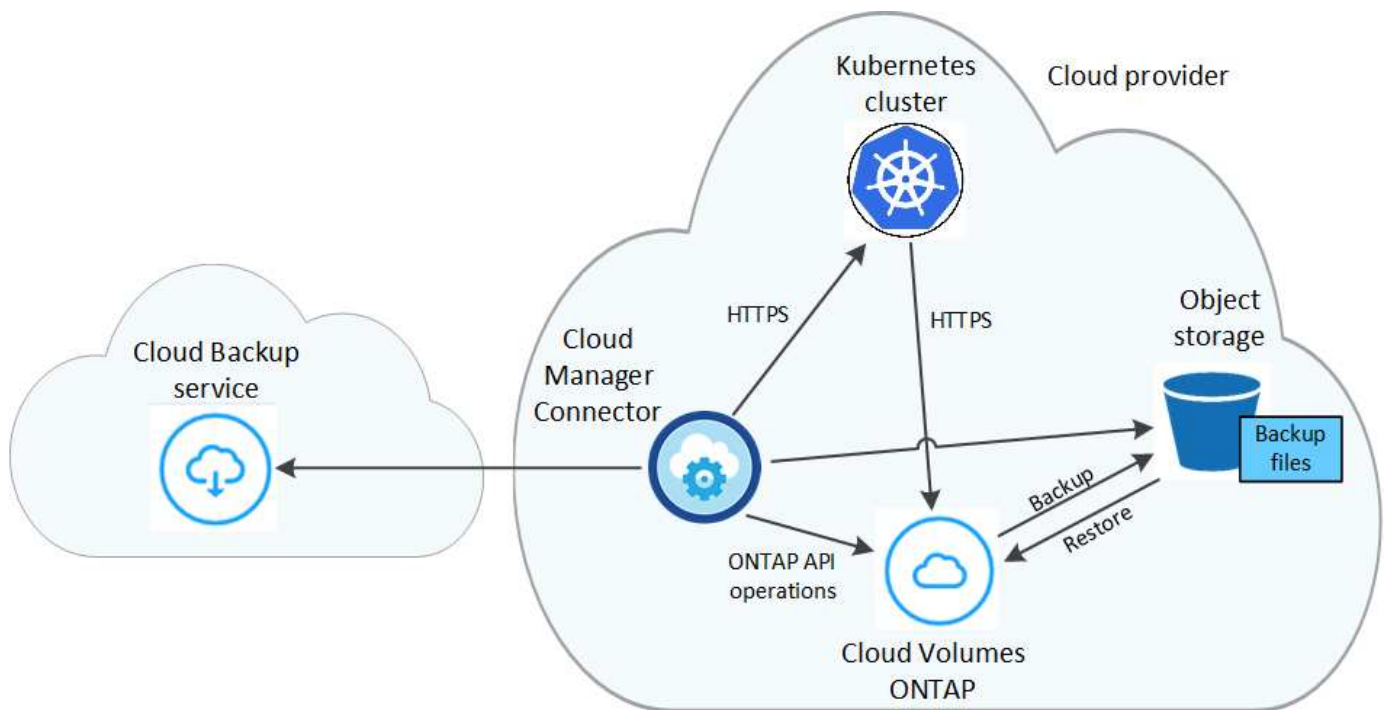
Kubernetes システムで Cloud Backup を有効にすると、サービスはデータのフルバックアップを実行します。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。



クラウドプロバイダ環境からバックアップファイルの管理や変更を直接行くと、ファイルが破損してサポートされない構成になる可能性があります。

次の図は、各コンポーネント間の関係を示しています。





サポートされるストレージクラスまたはアクセス階層

- Azure では、バックアップは \_COOL アクセス層に関連付けられます。

クラスタごとにカスタマイズ可能なバックアップスケジュールと保持設定

作業環境で Cloud Backup を有効にすると、最初を選択したすべてのボリュームが、定義したデフォルトのバックアップポリシーを使用してバックアップされます。Recovery Point Objective (RPO ; 目標復旧時点) が異なるボリュームに対して異なるバックアップポリシーを割り当てる場合は、そのクラスタに追加のポリシーを作成し、そのポリシーを他のボリュームに割り当てることができます。

すべてのボリュームについて、毎時、毎日、毎週、および毎月のバックアップを組み合わせることで選択できます。

カテゴリまたは間隔のバックアップの最大数に達すると、古いバックアップは削除されるため、常に最新のバックアップが保持されます。

サポートされるボリューム

Cloud Backup は永続ボリューム (PVS) をサポートしています。

制限

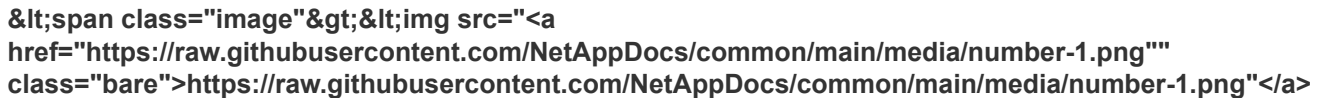
- ポリシーにボリュームが割り当てられていない場合にバックアップポリシーを作成または編集するときは、バックアップの保持数を 1018 以下にする必要があります。回避策 では、ポリシーを作成するバックアップの数を減らすことができます。その後、ポリシーを編集して、ポリシーにボリュームを割り当てたあとで最大 4、000 個のバックアップを作成できます。
- Kubernetes ボリュームでは、\* 今すぐバックアップ \* ボタンを使用したアドホックボリュームのバックアップはサポートされていません。

# Kubernetes の永続ボリュームのデータを Azure BLOB ストレージにバックアップする

AKS Kubernetes クラスタ上の永続ボリュームから Azure BLOB ストレージへのデータのバックアップを開始するには、いくつかの手順を実行します。

## クイックスタート

これらの手順を実行してすぐに作業を開始するか、残りのセクションまでスクロールして詳細を確認してください。

前提条件を確認します

- Kubernetes クラスタを Cloud Manager の作業環境として検出しておきます。
  - Trident がクラスタにインストールされている必要があります。Trident のバージョンは 21.1 以降である必要があります。
  - バックアップする永続ボリュームの作成に使用されるすべての PVC で、「snapshotPolicy」が「default」に設定されている必要があります。
  - クラスタのバックエンドストレージに Azure 上の Cloud Volumes ONTAP が使用されている必要があります。
  - Cloud Volumes ONTAP システムで ONTAP 9.7P5 以降が実行されている必要があります。
- バックアップを格納するストレージスペースに対する有効なクラウドプロバイダのサブスクリプションが必要です。
- に登録しておきます ["Cloud Manager Marketplace のバックアップソリューション"](#)またはを購入したことが必要です ["アクティブ化されます"](#) NetApp の Cloud Backup BYOL ライセンス。

作業環境を選択し、右パネルの [バックアップと復元] サービスの横にある [\*Enable] をクリックして、セットアップ・ウィザードに従います。



デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

Define Policy

**Policy - Retention & Schedule**

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

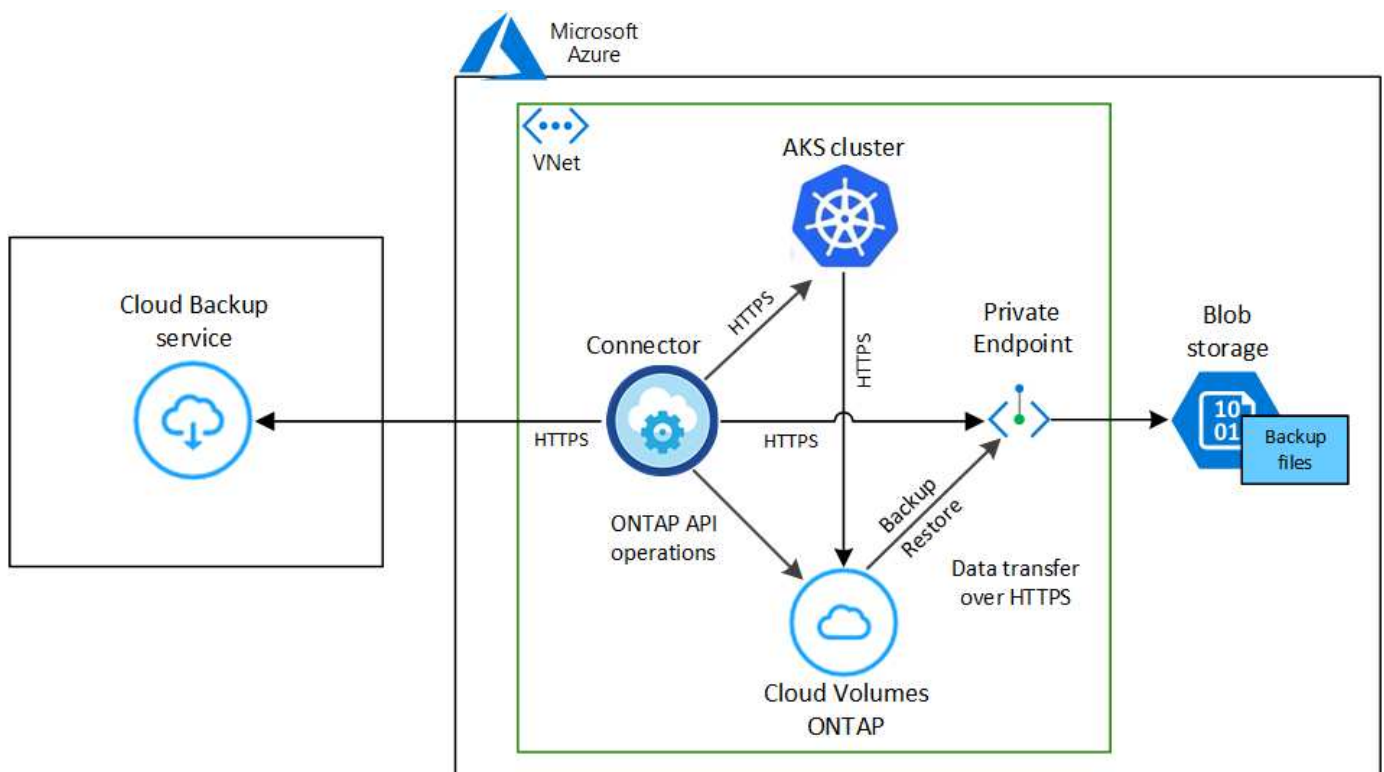
**Storage Account** Cloud Manager will create the storage account after you complete the wizard

Select Volumes（ボリュームの選択）ページで、バックアップするボリュームを特定します。バックアップファイルは、Cloud Volumes ONTAP システムと同じ Azure サブスクリプションとリージョンを使用して BLOB コンテナに格納されます。

## 要件

Kubernetes 永続ボリュームを BLOB ストレージにバックアップする前に、次の要件を読み、サポートされている構成であることを確認してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



プライベートエンドポイントはオプションです。

## Kubernetes クラスタの要件

- Kubernetes クラスタを Cloud Manager の作業環境として検出しておきます。 ["Kubernetes クラスタの検出方法を参照してください"](#)。

- Trident はクラスタにインストールされている必要があります。Trident のバージョンは 21.1 以上である必要があります。を参照してください ["Trident のインストール方法"](#) または ["Trident バージョンをアップグレードする方法"](#)。
- クラスタのバックエンドストレージに Azure 上の Cloud Volumes ONTAP が使用されている必要があります。
- Cloud Volumes ONTAP システムはKubernetesクラスタと同じAzureリージョンに配置する必要があります、ONTAP 9.7P5以降を実行している必要があります（ONTAP 9.8P11以降を推奨）。

オンプレミス環境の Kubernetes クラスタはサポートされていません。Cloud Volumes ONTAP システムを使用するクラウド環境では、Kubernetes クラスタのみがサポートされます。

- バックアップする永続ボリュームの作成に使用されるすべての Persistent Volume Claim オブジェクトで、「snapshotPolicy」が「default」に設定されている必要があります。

これは、注釈の下に「SnapshotPolicy」を追加することで、個々の PVC に対して行うことができます。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

バックエンド・ストレージに関連付けられているすべての PVC に対してこの操作を行うには、backend.json ファイルの defaults に 'snapshotPolicy' フィールドを追加します

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

## ライセンス要件

Cloud Backup 従量課金制のライセンスの場合は、Cloud Backup を有効にする前に Azure Marketplace でサブスクリプションを購入する必要があります。Cloud Backup の請求は、このサブスクリプションを通じて行われます。 ["作業環境ウィザードの詳細 & 資格情報ページから購読できます"](#)。

Cloud Backup BYOL ライセンスを使用するには、ライセンスの期間と容量にサービスを使用できるように、ネットアップから提供されたシリアル番号が必要です。 ["BYOL ライセンスの管理方法について説明します"](#)。

また、バックアップを格納するストレージスペースには、Microsoft Azure サブスクリプションが必要です。

## サポートされている Azure リージョン

Cloud Backup はすべての Azure リージョンでサポートされます ["Cloud Volumes ONTAP がサポートされている場合"](#)。

## Cloud Backup を有効にしています

Kubernetesの作業環境からCloud Backupをいつでも直接有効にできます。

### 手順

1. 作業環境を選択し、右パネルの [バックアップと復元] サービスの横にある [\*Enable] をクリックします。



2. バックアップポリシーの詳細を入力し、\* Next \* をクリックします。

バックアップスケジュールを定義して、保持するバックアップの数を選択できます。

3. バックアップする永続ボリュームを選択します。

- すべてのボリュームをバックアップするには、タイトル行 (☒ Volume Name)。
- 個々のボリュームをバックアップするには、各ボリュームのボックス (☒ Volume\_1)。

<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	PV1 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	PV2 On	Namespace 2	10 TB	Not Active

☒ Automatically back up all existing and future persistent volumes with the selected backup policy

4. 現在および将来のすべてのボリュームでバックアップを有効にする場合は、「今後のボリュームを自動的にバックアップします...一時保持」チェックボックスをオンのままにします。この設定を無効にした場合は、将来のボリュームのバックアップを手動で有効にする必要があります。

5. Activate Backup \* をクリックすると、選択した各ボリュームの初期バックアップの実行が開始されます。

バックアップファイルは、Cloud Volumes ONTAP システムと同じ Azure サブスクリプションとリージョンを



使用して BLOB コンテナに格納されます。

Kubernetes ダッシュボードが表示され、バックアップの状態を監視できます。

可能です "ボリュームのバックアップを開始および停止したり、バックアップを変更したりできます [スケジュール](#)"。また可能です "バックアップファイルからボリューム全体をリストアする" Azure 内の同じまたは別の Kubernetes クラスター（同じリージョン内）に新しいボリュームとして配置する必要があります。

## Kubernetes システムのバックアップの管理

Kubernetes システムのバックアップは、バックアップスケジュールの変更、ボリュームのバックアップの有効化 / 無効化、バックアップの削除などによって管理できます。



バックアップファイルをクラウドプロバイダ環境から直接管理したり変更したりしないでください。ファイルが破損し、サポートされていない構成になる可能性があります。

### バックアップしているボリュームを表示します

Cloud Backup で現在バックアップされているすべてのボリュームのリストを表示できます。

手順

1. [バックアップと復元] サービスをクリックします。
2. Kubernetes システムの永続ボリュームのリストを表示するには、\* Kubernetes \* タブをクリックします。

Source K8s Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backup Copies	Backup Status
aws eks1 Unknown	pvc-1704aa1f-af1d-49e9-87fd-6edd86125855 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-1615f0a8-2d5d-44d0-b4e4-f365cc3fb4a6 Unknown	default	Jun 09 2022, 10:00:24 am	20	Unknown
aws eks1 Unknown	pvc-d1f839c1-d932-4f49-b620-33321dbe939e Unknown	trident	Jun 09 2022, 10:00:24 am	20	Unknown

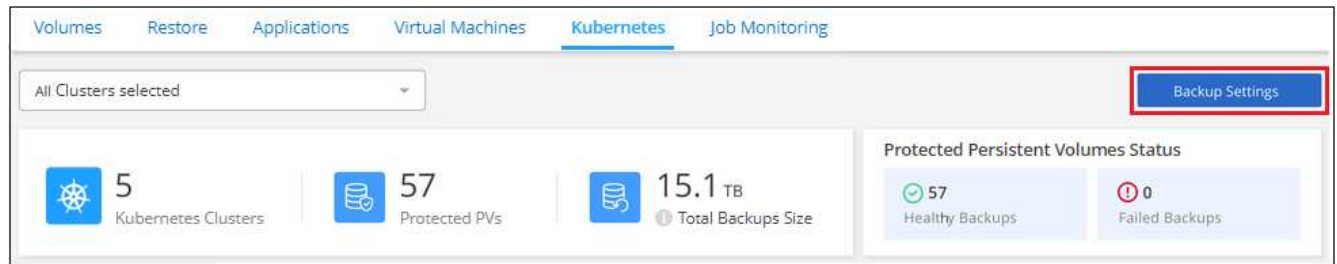
特定のクラスターの特定のボリュームを検索する場合は、クラスターおよびボリュームに基づいてリストを絞り込むか、検索フィルタを使用できます。

### ボリュームのバックアップの有効化と無効化

ボリュームのバックアップコピーが不要で、バックアップの格納コストを抑える必要がない場合は、ボリュームのバックアップを停止できます。新しいボリュームがバックアップ中でない場合は、バックアップリストに追加することもできます。

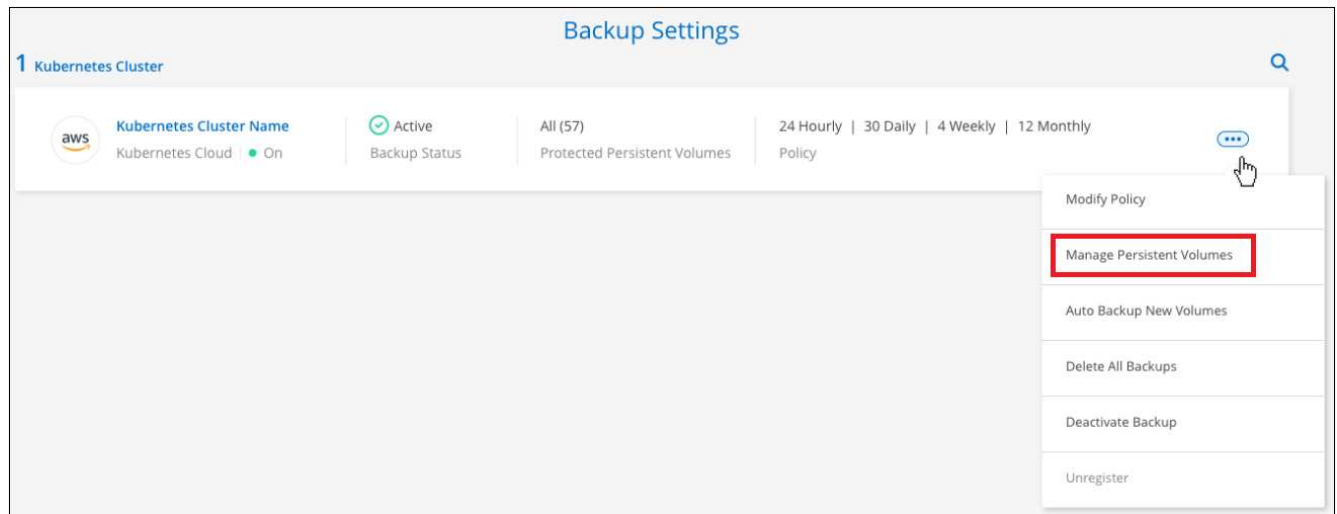
## 手順

1. **[Kubernetes \*]** タブで、**[ バックアップ設定 \* ]** を選択します。



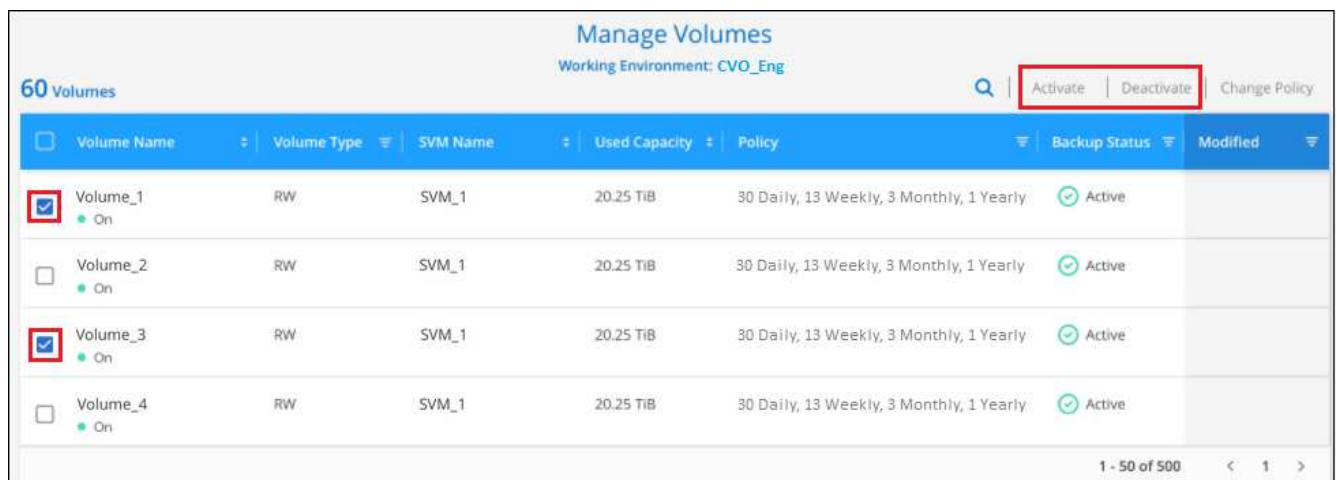
ボタンを示すスクリーンショット。"]

2. **\_ バックアップ設定ページ \_** で、をクリックします **... アイコン**] Kubernetes クラスタで、**\* Manage Persistent Volumes \*** を選択します。



ページの[永続ボリュームの管理]ボタンを示すスクリーンショット。"]

3. 変更するボリュームのチェックボックスを選択し、ボリュームのバックアップを開始するか停止するかに応じて、**[Activate \* (アクティブ化 \*) ]** または **[\* Deactivate \* (非アクティブ化 \*) ]** をクリックします。



4. **[ 保存 ( Save ) ]** をクリックして、変更をコミットします。

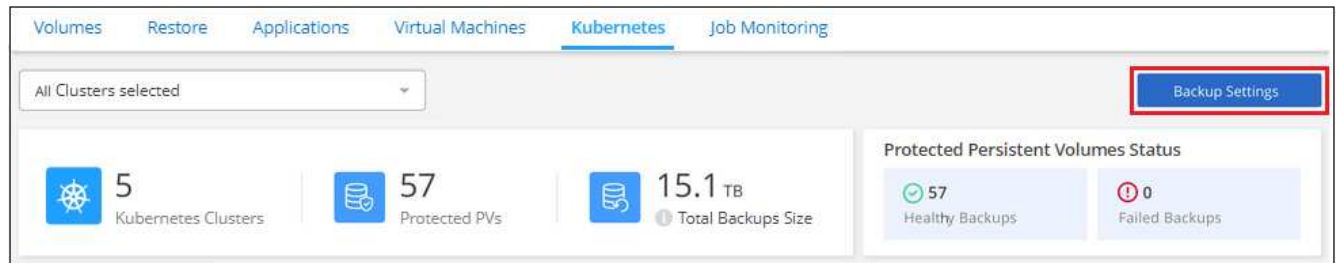
- 。注意：\* ボリュームのバックアップを停止すると、バックアップが停止します オブジェクトの料金はクラウドプロバイダが継続的に負担します を除いて、バックアップが使用する容量のストレージコスト あなた [バックアップを削除します](#)。

## 既存のバックアップポリシーを編集する

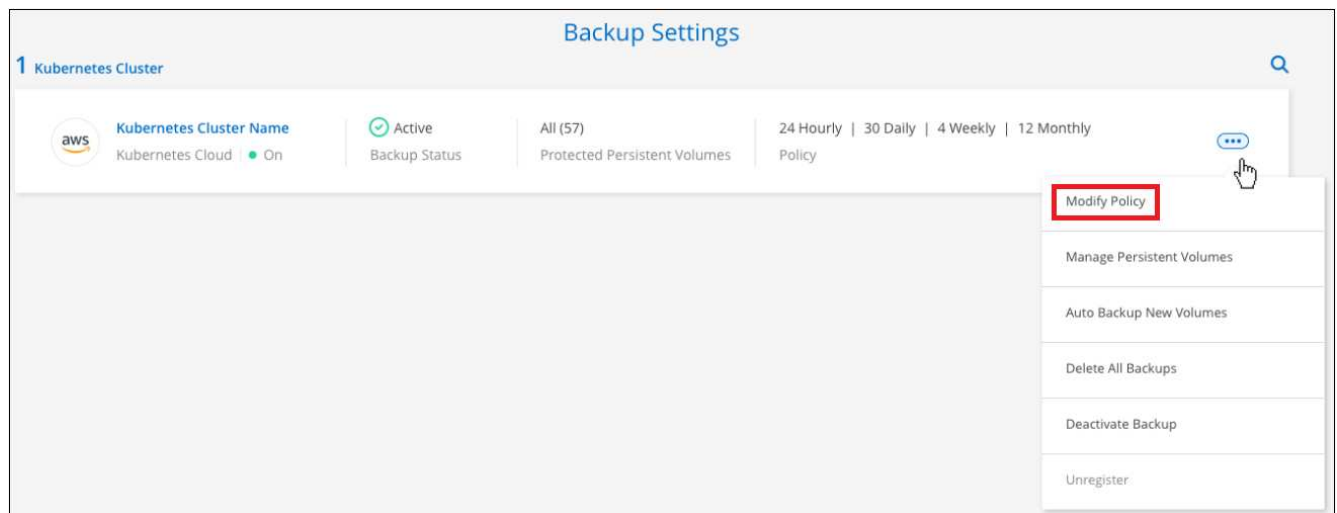
作業環境でボリュームに現在適用されているバックアップポリシーの属性を変更することができます。バックアップポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームが対象になります。

### 手順

1. **[Kubernetes \*]** タブで、**[ バックアップ設定 \* ]** を選択します。



2. **[Backup Settings]** ページで、をクリックします **... アイコン**] 設定を変更する作業環境で、**[ \* ポリシーの管理 \* ]** を選択します。



ページの **[ ポリシーの管理 ]** オプションを示すスクリーンショット。"]

3. **[ ポリシーの管理 ]** ページで、作業環境で変更するバックアップポリシーの **[ ポリシーの編集 ]** をクリックします。



4. [ポリシーの編集] ページで、スケジュールとバックアップの保持を変更し、[保存] をクリックします。



## 新しいボリュームに割り当てるバックアップポリシーの設定

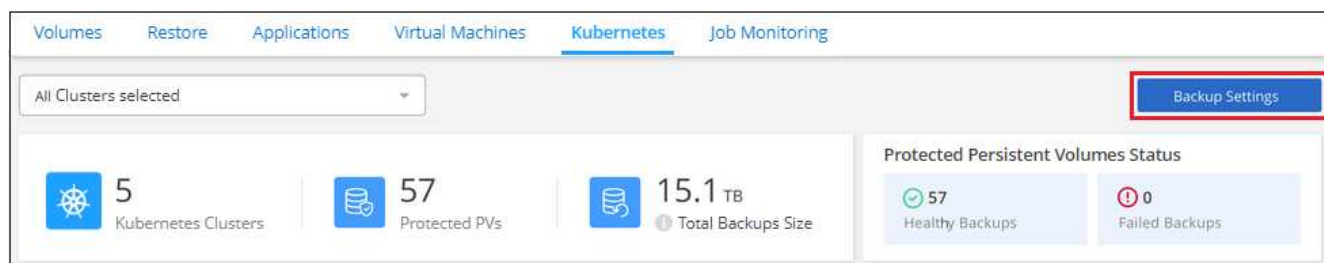
Kubernetes クラスターで Cloud Backup を初めてアクティブ化したときに、新しく作成したボリュームにバックアップポリシーを自動的に割り当てるオプションを選択しなかった場合は、後で [\\_Backup Settings\\_page](#) でこのオプションを選択できます。新しく作成したボリュームにバックアップポリシーを割り当てると、すべてのデータを確実に保護できます。

ボリュームに適用するポリシーがすでに存在する必要があります。 [作業環境に新しいバックアップポリシーを追加する方法を参照してください。](#)

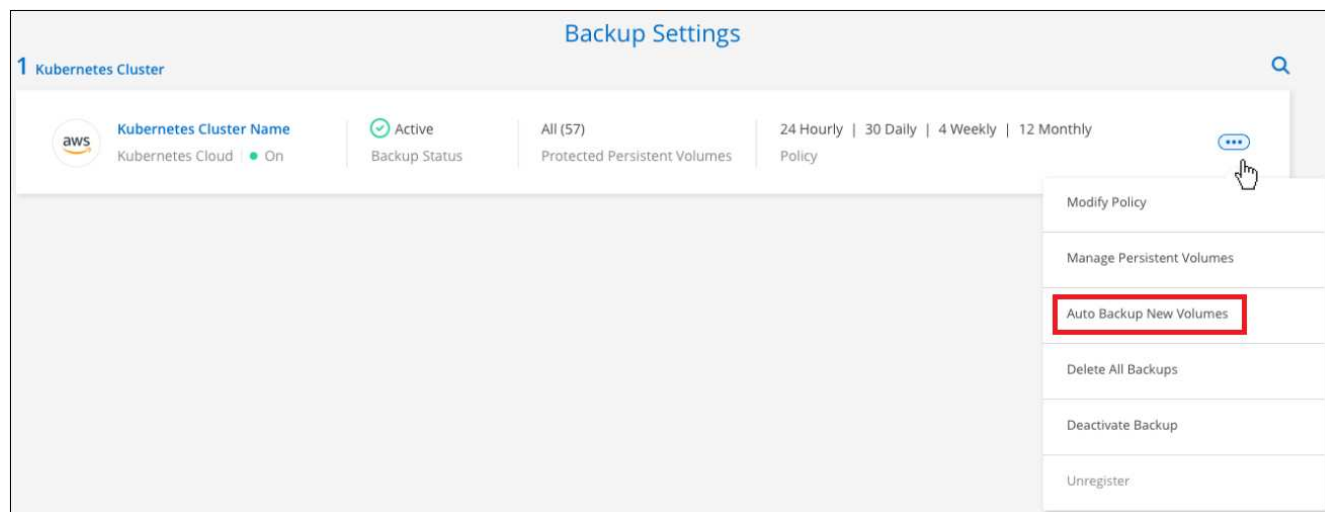
また、新しく作成したボリュームが自動的にバックアップされないようにするには、この設定を無効にします。その場合は、後でバックアップする特定のボリュームのバックアップを手動で有効にする必要があります。

### 手順

1. **[Kubernetes \*]** タブで、**[バックアップ設定 \*]** を選択します。

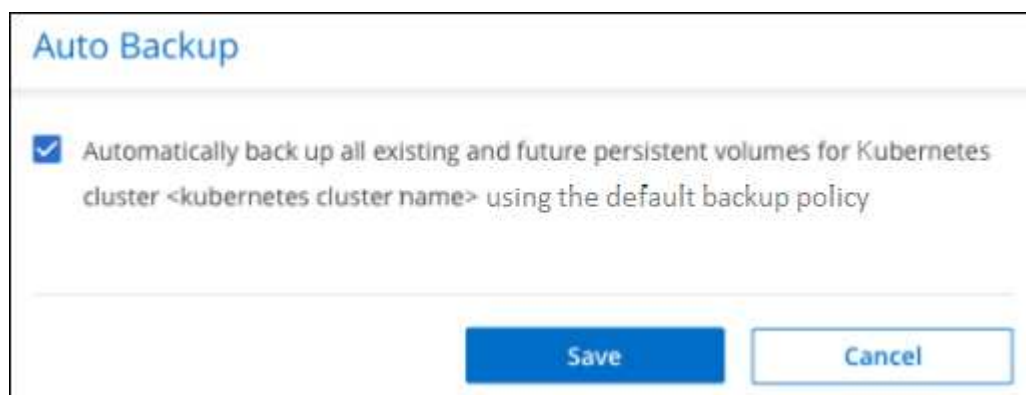


2. \_バックアップ設定ページ\_で、をクリックします **...** アイコン"] ボリュームが存在するKubernetesクラスタで、\* Auto Backup New Volumes \*を選択します。



ページで[新しいボリュームの自動バックアップ]オプションを選択したスクリーンショット。"]

3. [今後の永続ボリュームを自動的にバックアップする...]チェックボックスをオンにし、新しいボリュームに適用するバックアップポリシーを選択して、[保存]をクリックします。



このバックアップポリシーは、このKubernetesクラスタで作成されるすべての新しいボリュームに適用されます。

## 各ボリュームのバックアップリストを表示します

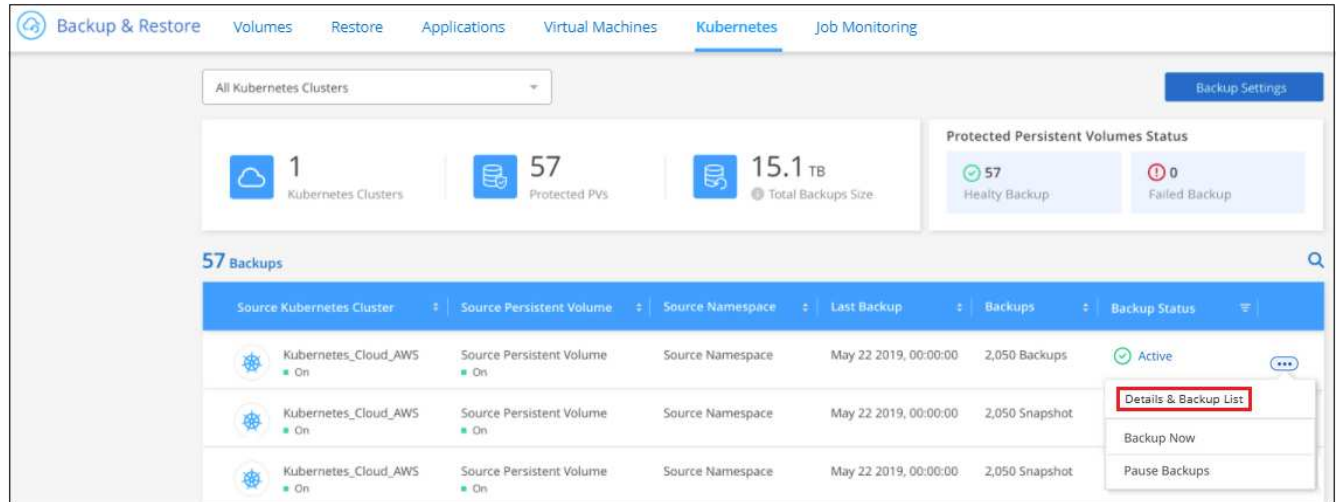
各ボリュームに存在するすべてのバックアップファイルのリストを表示できます。このページには、ソースボリューム、デスティネーションの場所、および前回作成されたバックアップの詳細、現在のバックアップポリシー、バックアップファイルのサイズなどのバックアップの詳細が表示されます。

このページでは、次のタスクも実行できます。

- ボリュームのすべてのバックアップファイルを削除します
- ボリュームの個々のバックアップファイルを削除する
- ボリュームのバックアップレポートをダウンロードします

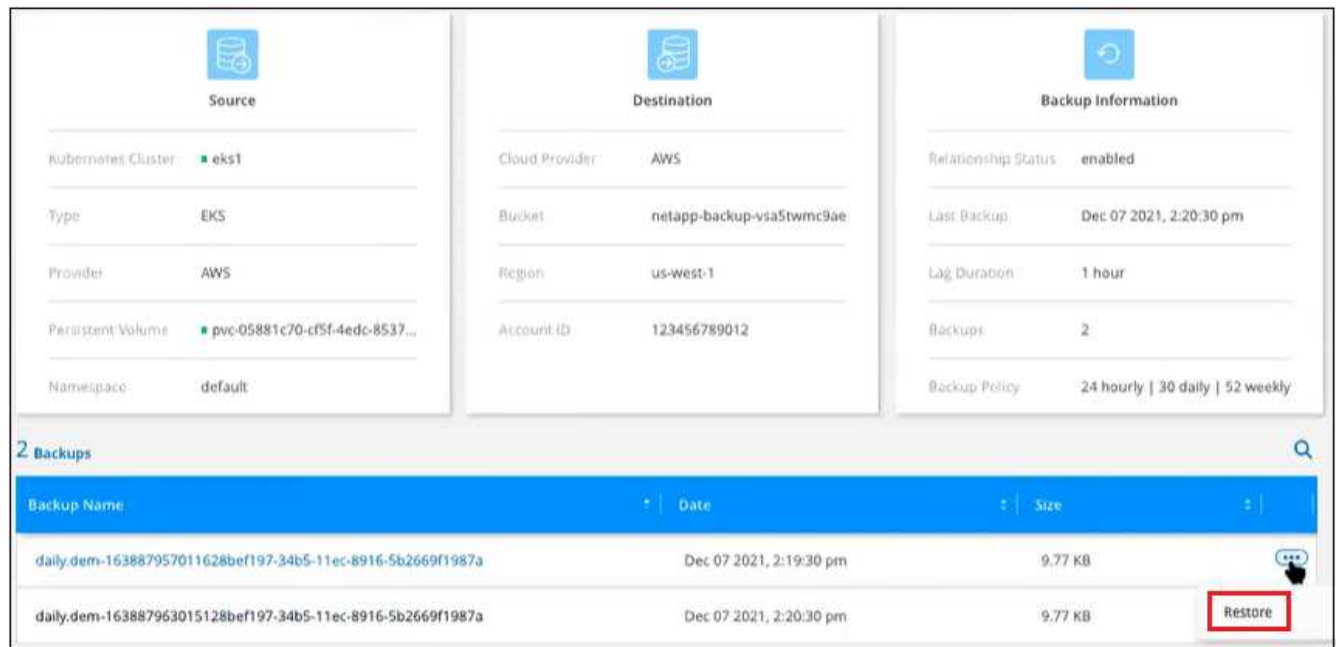
手順

1. [\*Kubernetes \*] タブで、をクリックします ... アイコン"] をソースボリュームとして選択し、\* Details & Backup List \* を選択します。



ボタンを示すスクリーンショット"]

すべてのバックアップファイルのリストが、ソースボリューム、デスティネーションの場所、およびバックアップの詳細とともに表示されます。



## バックアップを削除する

Cloud Backup では、単一のバックアップファイルの削除、ボリュームのすべてのバックアップの削除、Kubernetes クラスタ内のすべてのボリュームのすべてのバックアップの削除を実行できます。すべてのバックアップを削除するのは、不要になった場合やソースボリュームを削除したあとにすべてのバックアップを削除する場合などです。





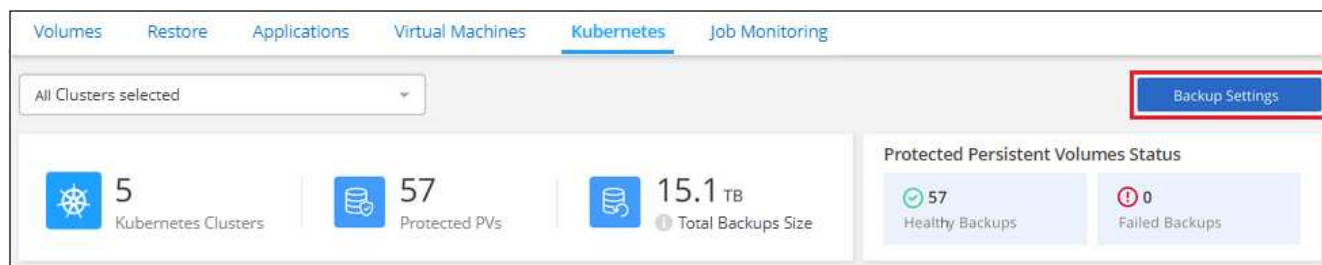
バックアップがある作業環境またはクラスタを削除する場合は、システムを削除する前に \* バックアップを削除する必要があります。システムを削除しても、Cloud Backup はバックアップを自動的に削除しません。また、システムを削除した後でバックアップを削除するための UI で現在サポートされていません。残りのバックアップについては、引き続きオブジェクトストレージのコストが発生します。

## 作業環境のすべてのバックアップファイルを削除する

作業環境のすべてのバックアップを削除しても、この作業環境のボリュームの以降のバックアップは無効になりません。作業環境ですべてのボリュームのバックアップの作成を停止するには、バックアップを非アクティブ化します [ここで説明するようにします](#)。

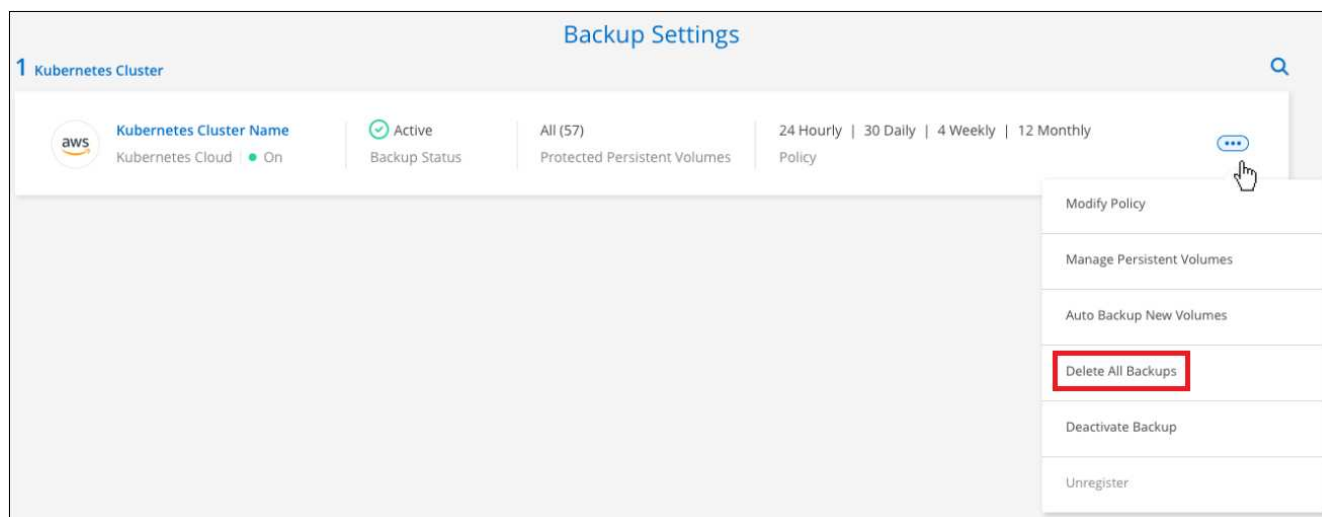
### 手順

1. **[Kubernetes \*]** タブで、**[ バックアップ設定 \* ]** を選択します。



ボタンを示すスクリーンショット。"]

2. をクリックします **... アイコン**] すべてのバックアップを削除する Kubernetes クラスタで、 \* すべてのバックアップを削除 \* を選択します。



ボタンを選択したスクリーンショット。"]

3. 確認ダイアログボックスで、作業環境の名前を入力し、 \* 削除 \* をクリックする。

## ボリュームのすべてのバックアップファイルを削除する

ボリュームのすべてのバックアップを削除すると、そのボリュームの以降のバックアップも無効になります。

可能です [ボリュームのバックアップの作成を再開します](#) [ Manage Backups (バックアップの管理) ] ページからいつでもアクセスできます。

## 手順

1. [\*Kubernetes \*] タブで、をクリックします ... アイコン] をソースボリュームとして選択し、 \* Details & Backup List \* を選択します。

Backup & Restore Volumes Restore Applications Virtual Machines **Kubernetes** Job Monitoring

All Kubernetes Clusters

Backup Settings

1 Kubernetes Clusters 57 Protected PVs 15.1 TB Total Backups Size

Protected Persistent Volumes Status

57 Healthy Backup 0 Failed Backup

57 Backups

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

Details & Backup List

Backup Now

Pause Backups

ボタンを示すスクリーンショット]

すべてのバックアップファイルのリストが表示されます。

Source Destination Backup Information

Working Environment Working Environment N... Cloud Provider AWS

Type Cloud Volumes ONTAP (HA) Region us-east-1

Provider AWS Bucket netapp-backup

Volume Volume Name Account ID 012345678901234567890

SVM SVM Name

Relationship Status Active

Last Backup Oct 05 2021, 2:41:33 pm

Lag Duration 14 days 3 hours, 38 mi...

Backups 2,050

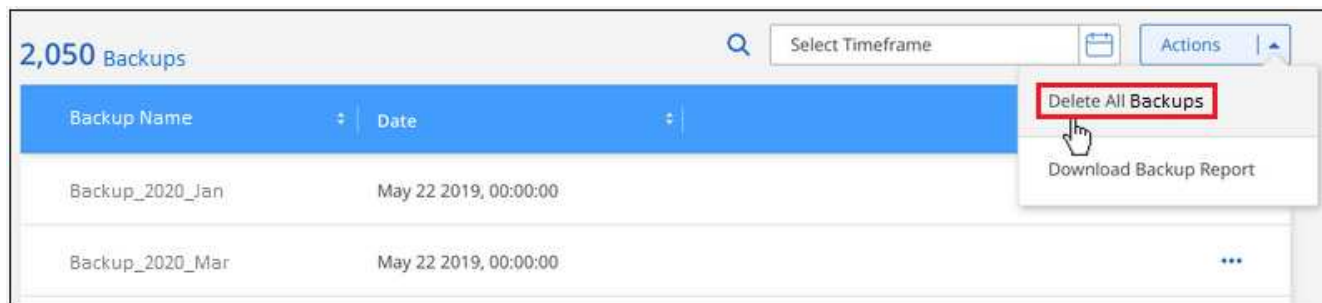
Backup Policy Netapp7YearsRetention

2,050 Backups

Select Timeframe Actions

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

2. [\* アクション \* > \* すべてのバックアップを削除 \*] をクリックします。



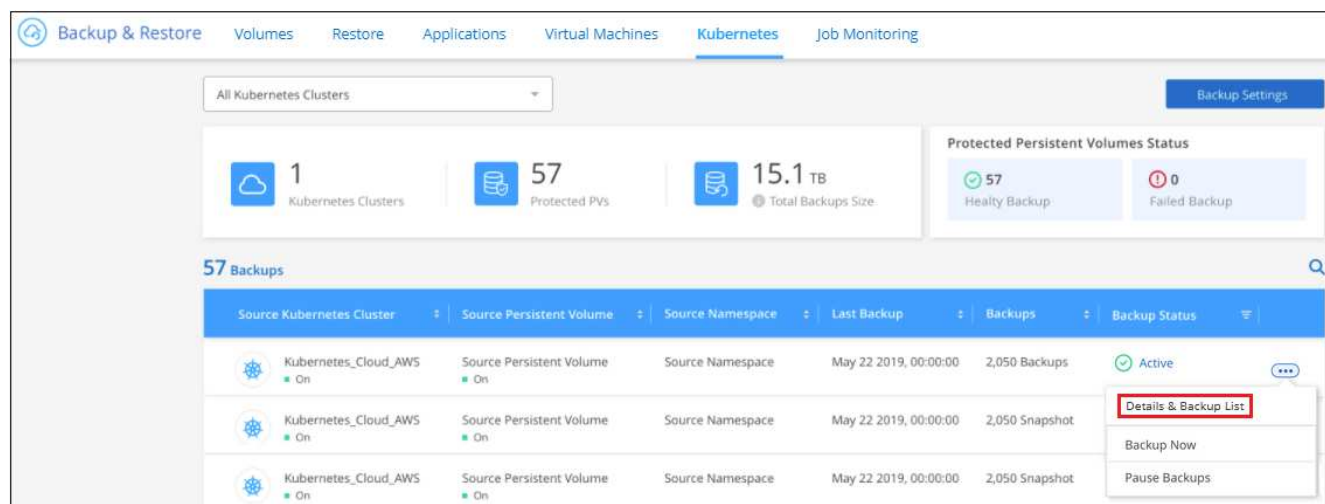
3. 確認ダイアログボックスで、ボリューム名を入力し、\* 削除 \* をクリックします。

ボリュームの単一のバックアップファイルを削除する

バックアップファイルは 1 つだけ削除できます。この機能は、ONTAP 9.8 以降のシステムでボリューム・バックアップを作成した場合にのみ使用できます。

手順

1. [\*Kubernetes \*] タブで、をクリックします ... アイコン"] をソースボリュームとして選択し、\* Details & Backup List \* を選択します。



ボタンを示すスクリーンショット"]

すべてのバックアップファイルのリストが表示されます。

2. をクリックします **...** アイコン] 削除するボリュームバックアップファイルに対して、**\* 削除 \*** をクリックします。

3. 確認ダイアログボックスで、**\* 削除 \*** をクリックします。

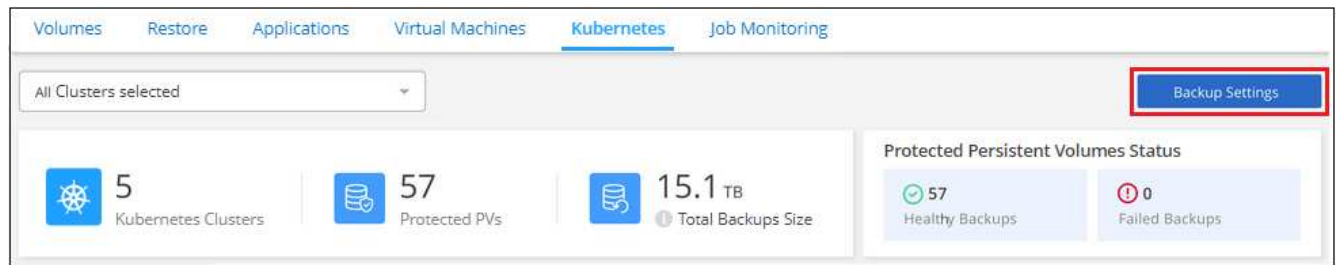
## 作業環境での Cloud Backup の無効化

作業環境で Cloud Backup を無効にすると、システム上の各ボリュームのバックアップが無効になり、ボリュームをリストアすることもできなくなります。既存のバックアップは削除されません。この作業環境からバックアップ・サービスの登録を解除することはありません。基本的には、すべてのバックアップおよびリストア処理を一定期間停止できます。

クラウドから引き続き課金されます が提供する容量のオブジェクトストレージコストのプロバイダ バックアップは自分以外で使います **バックアップを削除します**。

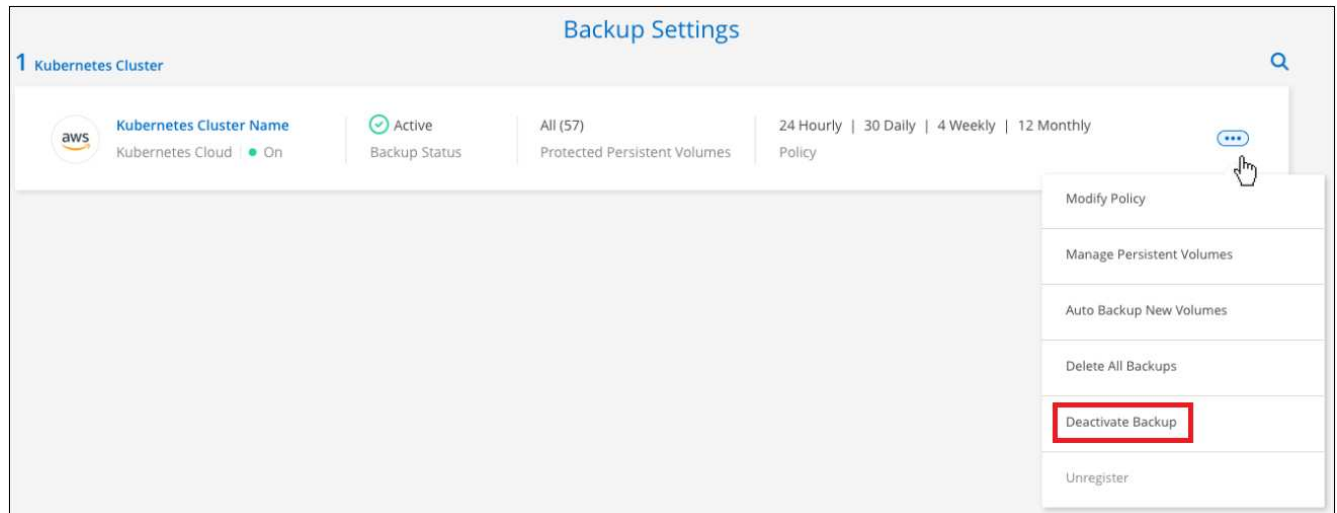
### 手順

1. **[Kubernetes \*]** タブで、**[ バックアップ設定 \* ]** を選択します。



ボタンを示すスクリーンショット。"]

2. バックアップ設定ページ で、をクリックします ... アイコン"] バックアップを無効にする作業環境または Kubernetes クラスターで、\* バックアップを非アクティブ化 \* を選択します。



3. 確認ダイアログボックスで、\* Deactivate \* をクリックします。



バックアップが無効になっている間は、その作業環境に対して \* バックアップのアクティブ化 \* ボタンが表示されます。このボタンは、作業環境でバックアップ機能を再度有効にする場合にクリックします。

## 作業環境のための **Cloud Backup** の登録を解除しています

バックアップ機能が不要になり、作業環境でバックアップの課金を停止する場合は、作業環境で Cloud Backup の登録を解除できます。通常、この機能は、Kubernetes クラスターを削除する予定でバックアップサービスをキャンセルする場合に使用します。

この機能は、クラスターバックアップの格納先のオブジェクトストアを変更する場合にも使用できます。作業環境で Cloud Backup の登録を解除したら、新しいクラウドプロバイダ情報を使用してそのクラスターで Cloud Backup を有効にできます。

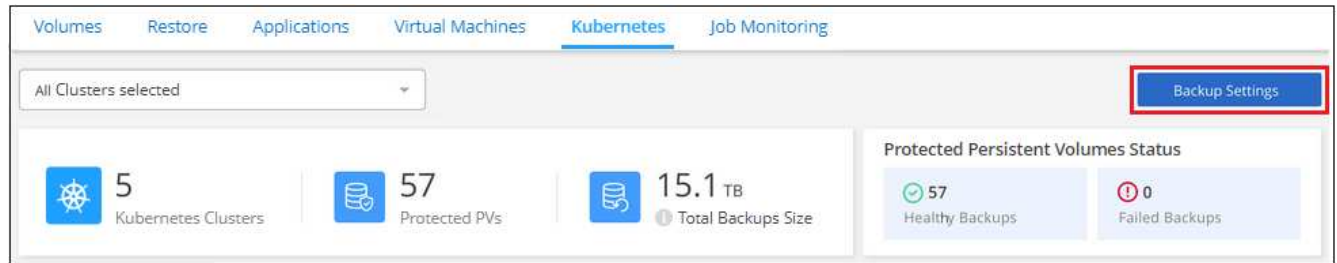
Cloud Backup の登録を解除する前に、次の手順をこの順序で実行する必要があります。

- 作業環境の Cloud Backup を非アクティブ化します
- その作業環境のバックアップをすべて削除します

登録解除オプションは、これら 2 つの操作が完了するまで使用できません。

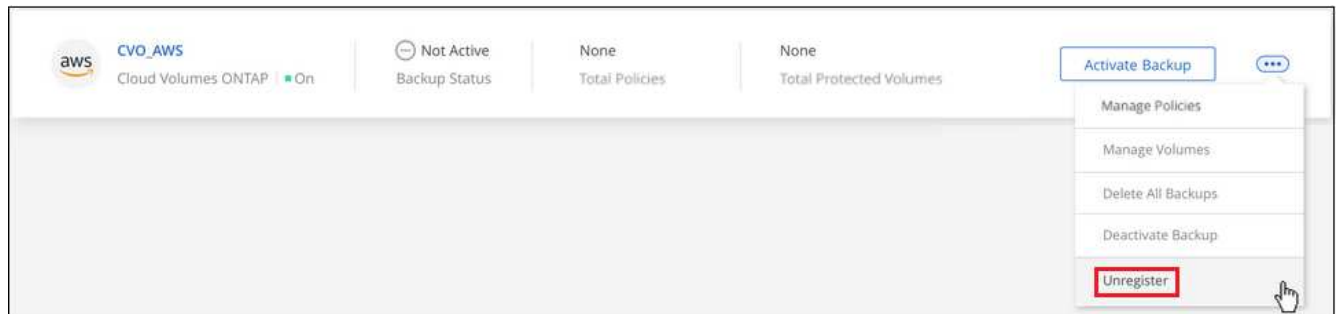
手順

1. **[Kubernetes \*]** タブで、**[ バックアップ設定 \* ]** を選択します。



ボタンを示すスクリーンショット。"]

2. **\_ バックアップ設定ページ \_** で、をクリックします **... アイコン**] バックアップサービスの登録を解除する Kubernetes クラスターで、**\* 登録解除 \*** を選択します。



3. 確認ダイアログボックスで、**\* 登録解除 \*** をクリックします。

## バックアップファイルからの **Kubernetes** データのリストア

バックアップは、特定の時点のデータをリストアできるように、クラウドアカウントのオブジェクトストアに格納されます。Kubernetes の永続ボリューム全体を、保存したバックアップファイルからリストアできます。

永続ボリュームは、（新しいボリュームとして）同じ作業環境または同じクラウドアカウントを使用している別の作業環境にリストアできます。

### サポートされている作業環境とオブジェクトストレージプロバイダ

Kubernetes バックアップファイルから次の作業環境にボリュームをリストアできます。

バックアップファイルの場所	デスティネーション作業環境
Amazon S3	aws []
Azure Blob の略	azure[] ifdef : gCP[]
Google クラウドストレージ	Google endifのKubernetesクラスター：GCP []



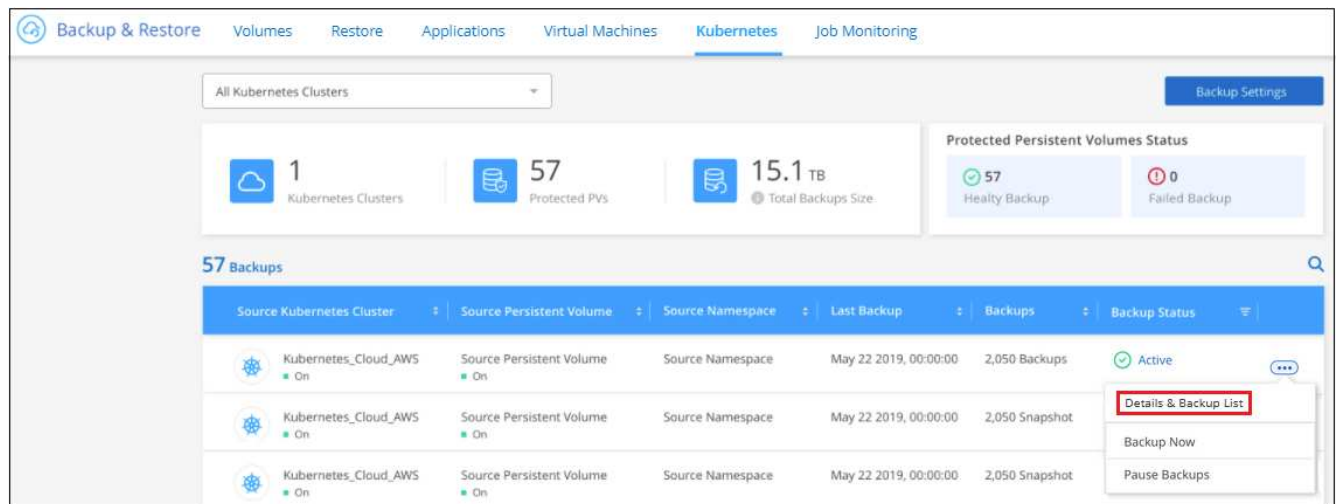
## Kubernetes バックアップファイルからのボリュームのリストア

バックアップファイルから永続ボリュームをリストアすると、Cloud Manager はバックアップのデータを使用して `_new_volume` を作成します。データは、同じ Kubernetes クラスタ内のボリューム、またはソースの Kubernetes クラスタと同じクラウドアカウントにある別の Kubernetes クラスタにリストアできます。

開始する前に、リストアするボリュームの名前と、新規にリストアされたボリュームの作成に使用するバックアップファイルの日付を確認しておく必要があります。

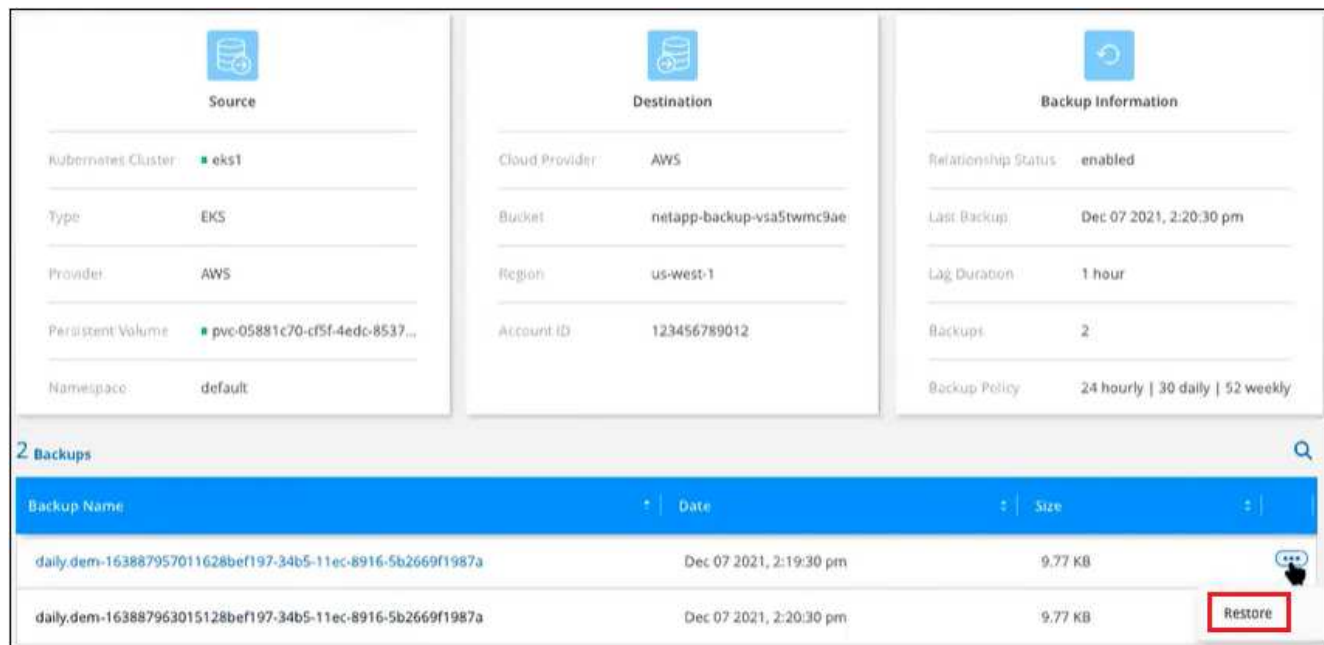
### 手順

1. Backup & Restore \* サービスを選択します。
2. [\*Kubernetes \*] タブをクリックすると、[Kubernetes Dashboard] が表示されます。



3. リストアするボリュームを選択し、をクリックします **... アイコン**]をクリックし、\*詳細とバックアップリスト\*をクリックします。

そのボリュームのすべてのバックアップファイルと、ソースボリューム、デスティネーションの場所、およびバックアップの詳細が表示されます。



4. 日付 / タイムスタンプに基づいてリストアする特定のバックアップファイルを選択し、をクリックします  
 ... アイコンをクリックし、次に \* Restore \* を実行します。
5. Select Destination\_page で、ボリュームをリストアする *Kubernetes cluster\_where* を選択します。 \_  
*Namespace* \_、 \_ *Storage Class*、および new\_Persistent ボリューム name \_。

### Select Destination

Select Kubernetes Cluster

eks1

Namespace

default

Storage Class

basic

PVC Name

pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restore

Cancel

Restore

6. リストア \* をクリックすると、Kubernetes ダッシュボードに戻り、リストア処理の進捗状況を確認できます。

選択したバックアップに基づいて、Cloud Manager が Kubernetes クラスタに新しいボリュームを作成します。可能です "この新しいボリュームのバックアップ設定を管理します" 必要に応じて。

# オンプレミスのアプリケーションデータのバックアップとリストア

## オンプレミスアプリケーションのデータを保護

Cloud Backup for Applications を Cloud Manager とオンプレミスの SnapCenter に統合することで、アプリケーションと整合性のある Snapshot をオンプレミスの ONTAP からクラウドにバックアップできます。必要に応じて、クラウドからオンプレミスの SnapCenter サーバにリストアできます。

OracleおよびMicrosoft SQLアプリケーションのデータをオンプレミスのONTAP システムから次のクラウドプロバイダにバックアップできます。

- Amazon Web Services の
- Microsoft Azure



SnapCenter ソフトウェア 4.6 を使用している必要があります。

Cloud Backup for Applications の詳細については、以下を参照してください。

- ["クラウドバックアップと SnapCenter を使用したアプリケーション対応バックアップ"](#)
- ["アプリケーション向けのクラウドバックアップ"](#)

## 要件

アプリケーションデータを クラウド サービス にバックアップする前に、次の要件を参照して、サポートされる構成になっていることを確認してください。

- ONTAP 9.8 以降
- Cloud Manager 3.9
- SnapCenter サーバ 4.6
- SnapCenter サーバでは、各アプリケーションに使用可能なバックアップを少なくとも 1 つ用意する必要があります
- SnapCenter の、Cloud Manager の Cloud Backup for Applications ポリシーと同じラベルまたはラベルのない日次、週次、または月単位のポリシーが少なくとも 1 つ必要です。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



## 保護ポリシー

アプリケーションデータをクラウドにバックアップするには、Cloud Backup for Applications で定義されているいずれかのポリシーを使用する必要があります。



カスタムポリシーはサポートされません。

ポリシー名	ラベル	保持値
1 年ごとの LTR	毎日	366
5 年ごとの LTR	毎日	1830 年に
7 年ごとの LTR	毎週	370
10 年間の月単位 LTR	毎月	120

これらのポリシーのラベルと保持の値は、ポリシーがアプリケーションに関連付けられるまで REST API を使用して変更できます。1 つのアプリケーションに関連付けることができるポリシーは 1 つだけで、関連付けが完了すると、関連付けを解除できません。

クラウドへのアプリケーションデータのバックアップには、Cloud Backup for Applications のポリシーに加えて、少なくとも 1 つの SnapCenter ポリシーが必要です。

# オンプレミスアプリケーションのデータをクラウドにバックアップ

Cloud Backup for Applications を Cloud Manager とオンプレミスの SnapCenter に統合することで、ONTAP からクラウドにアプリケーションデータをバックアップできます。

## SnapCenter サーバを登録します

SnapCenterAdmin ロールのユーザだけが、SnapCenter サーバ 4.6 が実行されているホストを登録できます。複数の SnapCenter サーバホストを登録できますが、登録後に SnapCenter サーバホストを削除することはできません。

### • 手順 \*

1. Cloud Manager UI で、\* Backup & Restore \* > \* Applications \* の順にクリックします。
2. [\* 設定] ドロップダウンから、[ SnapCenter サーバ \* ] をクリックします。
3. [\* SnapCenter サーバーの登録 \* ] をクリックします。
4. 次の情報を指定します。
  - a. SnapCenter Server フィールドで、SnapCenter サーバホストの FQDN または IP アドレスを指定します。
  - b. Port フィールドで、SnapCenter サーバが稼働しているポート番号を指定します。

SnapCenter サーバと Cloud Backup for Applications の間の通信用にポートが開いていることを確認してください。

- c. [ タグ ] フィールドで、SnapCenter サーバーにタグを付けるサイト名、都市名、またはカスタム名を指定します。

タグはカンマで区切って指定します。

- d. Username and Password フィールドで、SnapCenterAdmin ロールを持つユーザのクレデンシャルを指定します。

5. [\*Register] をクリックします。

### • 終了後 \*

[\* バックアップと復元 > アプリケーション \*] をクリックして、登録済み SnapCenter サーバ・ホストを使用して保護されているすべてのアプリケーションを表示します。



SQL Server データベースの場合、[ アプリケーション名 ] 列には、名前が \_application\_name (ホスト名) 形式で表示されます。名前を \_application\_name (ホスト名) \_format で指定して検索する場合、SQL Server データベースの詳細は表示されません。

サポートされるアプリケーションとその構成は次のとおりです。

- Oracle データベース：日単位、週単位、または月単位のスケジュールを少なくとも 1 つ使用して作成されたフルバックアップ（データ + ログ）。

- Microsoft SQL Server データベース：
  - スタンドアロン、フェイルオーバークラスティンスタンス、および可用性グループ
  - フルバックアップ：日単位、週単位、または月単位のスケジュールを少なくとも 1 つずつ設定して作成します

次の Oracle データベースおよび SQL Server データベースは表示されません。

- バックアップがないデータベース
- オンデマンドまたは毎時ポリシーのみのデータベース
- RDM または VMDK にあるデータベース

## アプリケーションデータをバックアップ

単一のポリシーを使用して、1 つ以上のアプリケーションをクラウドで同時に保護することができます。アプリケーションを保護するために割り当てることができるのは、デフォルトの組み込みポリシーだけです。



Cloud Manager の GUI を使用している場合、一度に保護できるアプリケーションは 1 つだけです。ただし、REST API を使用する場合は、複数のアプリケーションを同時に保護できます。

SQL Server インスタンスを保護する場合、そのインスタンスの対象となるデータベースのすべてのボリュームに対してクラウド保護が設定されます。SQL Server 可用性グループを保護する場合は、その可用性グループ内のデータベースのすべてのボリュームに対してクラウド保護が設定されます。ただし、バックアップの設定に基づいて、各ボリュームから Snapshot がコピーされます。

- 手順 \*
  1. Cloud Manager UI で、\* Backup & Restore \* > \* Applications \* の順にクリックします。
  2. をクリックします ... アプリケーションに対応して、\* バックアップのアクティブ化 \* をクリックします。
  3. 作業環境を追加します。

アプリケーションが実行されている SVM をホストする ONTAP クラスタを設定します。いずれかのアプリケーション用の作業環境を追加したら、同じ ONTAP クラスタにある他のすべてのアプリケーションでその作業環境を再利用できます。

- a. SVM を選択し、作業環境の追加をクリックします。
- b. 作業環境の追加ウィザードで、次の手順を実行します。
  - i. ONTAP クラスタの IP アドレスを指定します。
  - ii. 管理クレデンシャルを指定します。

Cloud Backup for Applications でサポートされているのはクラスタ管理者のみです。

- c. \* 作業環境の追加 \* をクリックします。





作業環境の詳細が更新されるまで先に進まないでください。作業環境の詳細が更新されるまでに最大 30 分かかることがあります。30 分後にウィザードを閉じ、手順 1 から再試行して作業環境の詳細を確認してください。作業環境の詳細が更新されていない場合は再試行して、正しい作業環境が追加されていることを確認してください。

#### 4. クラウドプロバイダを選択して設定します。

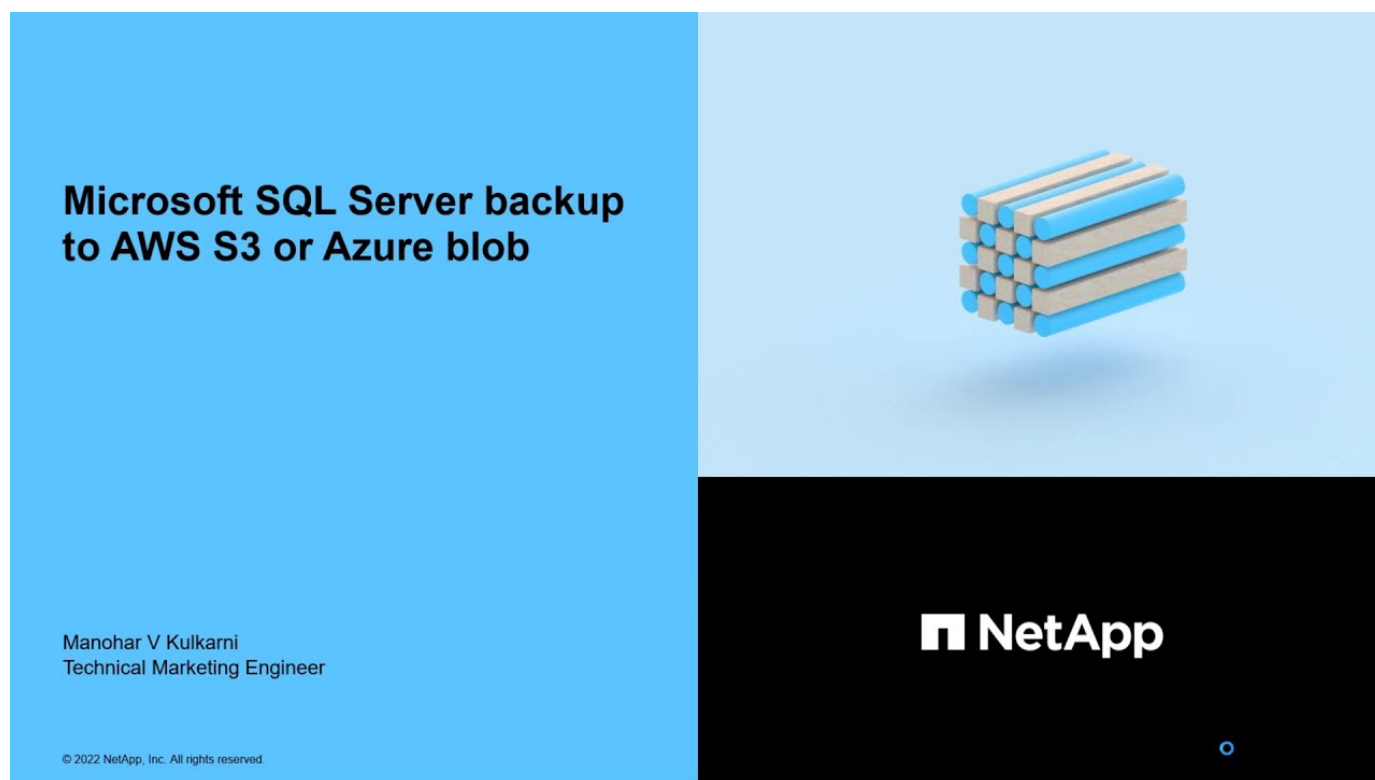
##### Microsoft Azure を設定

- Azure サブスクリプション ID を指定します。
- バックアップを作成するリージョンを選択します。
- 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てください。
- 作業環境として追加した ONTAP クラスタの IP アドレスを指定します。

#### 5. [ ポリシーの割り当て ] ページで、ポリシーを選択して [ 次へ \* ] をクリックします。

#### 6. 詳細を確認し、 \* バックアップのアクティブ化 \* をクリックします。

次のビデオでは、データベースを保護する簡単な手順を示します。



## アプリケーションの保護を管理します

ポリシーとバックアップを表示できます。データベース、ポリシー、またはリソースグループの変更に応じて、Cloud Manager UI から更新情報を更新できます。

## ポリシーを表示します

デフォルトの組み込みポリシーをすべて表示できます。これらの各ポリシーについて、関連付けられているすべての Cloud Backup for Applications ポリシーと関連するすべてのアプリケーションの詳細を表示すると、それらが表示されます。

1. [ \* バックアップと復元 > アプリケーション \* ] をクリックします。
2. [ \* 設定 ] ドロップダウンから、[ ポリシー \* ] をクリックします。
3. 詳細を表示するポリシーに対応する **View Details** をクリックします。

関連する Cloud Backup for Applications ポリシーとすべてのアプリケーションが表示されます。



Cloud Backup for Applications ポリシーは削除しないでください。

「Get-SmResources」 SnapCenter コマンドレットを実行して、クラウド拡張 SnapCenter ポリシーを表示することもできます。コマンドレットで利用できるパラメータとその説明については、Get-Help コマンドレットを実行して確認できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

## クラウド上のバックアップを表示します

クラウド上のバックアップは、Cloud Manager の UI で確認できます。

1. [ \* バックアップと復元 > アプリケーション \* ] をクリックします。
2. をクリックします アプリケーションに対応して、 \* 詳細を表示 \* をクリックします。



表示されるバックアップの所要時間は、ONTAP のデフォルトのレプリケーションスケジュール（最大 1 時間）と Cloud Manager（最大 6 時間）によって異なります。

- Oracle データベースの場合は、バックアップごとにデータバックアップとログバックアップの両方、SCN 番号、バックアップごとの終了日が表示されます。データバックアップのみを選択し、オンプレミスの SnapCenter サーバにデータベースをリストアできます。
- Microsoft SQL Server データベースの場合は、各バックアップのフルバックアップと終了日だけが表示されます。バックアップを選択し、オンプレミスの SnapCenter サーバにデータベースをリストアできます。
- Microsoft SQL Server インスタンスの場合は、バックアップが表示されるのではなく、そのインスタンスのデータベースだけが表示されます。



クラウド保護を有効にする前に作成したバックアップはリストア対象として表示されません。

これらのバックアップは 'Get-SmBackup' SnapCenter コマンドレットを実行して表示することもできます。コマンドレットで利用できるパラメータとその説明については、Get-Help コマンドレットを実行して確認できます。または、を参照することもできます ["SnapCenter ソフトウェアコマンドレットリファレンスガイド"](#)。

## データベースレイアウトの変更

ボリュームがデータベースに追加されると、SnapCenter サーバは、ポリシーとスケジュールに基づいて、新しいボリューム上の Snapshot に自動的にラベルを付けます。これらの新しいボリュームにはオブジェクトス

トアエンドポイントがないため、次の手順を実行して更新する必要があります。

1. [ \* バックアップと復元 > アプリケーション \* ] をクリックします。
2. [ \* 設定 ] ドロップダウンから、[ SnapCenter サーバ \* ] をクリックします。
3. をクリックします ... アプリケーションをホストしている SnapCenter サーバーに対応し、[ 更新 ] をクリックします。

新しいボリュームが検出されます。

4. をクリックします ... アプリケーションに対応し、 \* 保護の更新 \* をクリックして、新しいボリュームのクラウド保護を有効にします。

クラウドサービスの設定後にストレージボリュームをアプリケーションから削除すると、SnapCenter サーバは、アプリケーションが存在する Snapshot にのみラベルを付けます。削除したボリュームが他のアプリケーションで使用されていない場合は、オブジェクトストア関係を手動で削除する必要があります。アプリケーションインベントリを更新すると、アプリケーションの現在のストレージレイアウトが反映されます。

## ポリシーまたはリソースグループの変更

SnapCenter ポリシーまたはリソースグループに変更がある場合は、保護を更新する必要があります。

1. [ \* バックアップと復元 > アプリケーション \* ] をクリックします。
2. をクリックします ... アプリケーションに対応して、[ \* 保護の更新 \* ] をクリックします。

## ジョブを監視します

すべてのクラウドバックアップ処理に対してジョブが作成されます。すべてのジョブと、各タスクの一部として実行されるすべてのサブタスクを監視できます。

1. [ \* バックアップと復元 \* > \* ジョブ監視 \* ] をクリックします。

処理を開始すると、ジョブが開始されたことを示すウィンドウが表示されます。リンクをクリックするとジョブを監視できます。

2. プライマリタスクをクリックすると、これらの各サブタスクのサブタスクとステータスが表示されます。

## CA 証明書を設定します

CA 証明書がある場合は、ルート CA 証明書を Connector マシンに手動でコピーする必要があります。

CA 証明書がない場合は、CA 証明書を設定せずに続行できます。

### • 手順 \*

1. Docker エージェントからアクセス可能なボリュームに証明書をコピーします。
  - 「`cd /var/lib/docker/dochels/cloudmanager_snapcenter_volume/_data/mkdir sc_certs`」と入力します
  - `chmod 777 SC_certs`
2. RootCA 証明書ファイルを Connector マシンの上のフォルダにコピーします。

```
`cp <path on connector> /<filename>/var/lib/docx/volumes/cloudmanager_snapcenter  
volume/_data/sc_certs'
```

3. CRL ファイルを、 Docker エージェントからアクセス可能なボリュームにコピーします。
  - 「 cd /var/lib/docker/volumes/cloudmanager\_snapcenter \_ volume/\_data/mkdir sc\_crl 」 のように入力します
  - 'chmod 777 SC\_CRL

4. CRL ファイルを Connector マシンの上のフォルダにコピーします。

```
cp <path on connector>  
/<filename>/var/lib/docx/volumes/cloudmanager_snapcenter volume/_data/sc_crl
```

5. 証明書と CRL ファイルをコピーしたら、 Cloud Backup for Apps サービスを再起動します。
  - 「 sudo Docker exec cloudmanager\_snapcenter sed -i /skipSCCertValidation :  
true/skipSCCertValidation : false/g/opt/NetApp/cloudmanager-snapcenter agent/config/config.yml
  - 「 sudo Docker restart cloudmanager\_snapcenter 」 と入力します

## アプリケーションデータをリストアする

### Oracle データベースをリストアします

Oracle データベースは、同じ SnapCenter サーバホスト、同じ SVM 、または同じデータベースホストにのみリストアできます。 RAC データベースの場合は、バックアップが作成されたオンプレミスノードにデータがリストアされます。

制御ファイルのリストアを含むフルデータベースのみがサポートされます。アーカイブログが AFS 内にはない場合は、リカバリに必要なアーカイブログが格納されている場所を指定する必要があります。

#### • 手順 \*

1. Cloud Manager UI で、 \* Backup & Restore \* > \* Applications \* の順にクリックします。
2. [\* フィルター条件 \*] フィールドで、フィルター \* タイプ \* を選択し、ドロップダウンから [\* Oracle\*] を選択します。
3. リストアするデータベースに対応する **View Details** をクリックし、 **Restore** をクリックします。
4. [ リストアタイプ ] ページで、次の操作を実行します。
  - a. 制御ファイルとフルデータベースをリストアする場合は、「 \* 制御ファイル」を選択します。
  - b. リストアとリカバリに必要な場合は、「 \* データベースの状態を変更」を選択して、データベースの状態をリストアとリカバリ処理の実行に必要な状態に変更します。

データベースの状態は、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。リストア処理を実行するために、データベースの状態を高いレベルから低いレベルに変更する必要がある場合は、このチェックボックスをオンにします。リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェックボックスをオンにしなくても自動的に状態が変更されます。

データベースが OPEN 状態で、リストアのためにデータベースが MOUNTED 状態である必要がある場

合、データベースの状態はこのチェックボックスをオンにした場合にのみ変更されます。

1. Recovery Scope ページで、次のアクションを実行します。

a. リカバリの範囲を指定します。

状況	手順
最後のトランザクションまでリカバリする場合	[ * すべてのログ * ] を選択します。
特定の System Change Number ( SCN ) までリカバリする場合	[ * Until SCN ( System Change Number ) ] を選択します。
特定の日時までリカバリする必要がある	[ * 日付と時刻 * ] を選択します。  データベースホストのタイムゾーンの日付と時刻を指定する必要があります。
リカバリが不要である場合	[ * リカバリなし * ] を選択します。
外部アーカイブログの場所を指定する	アーカイブログが AFS 内にはない場合は、リカバリに必要なアーカイブログが格納されている場所を指定する必要があります。

b. リカバリ後にデータベースを開く場合は、チェックボックスを選択します。

RAC セットアップでは、リカバリに使用される RAC インスタンスのみがリカバリ後に開きます。


2. 詳細を確認して、\* リストア \* をクリックします。

## SQL Server データベースをリストアする

SQL Server データベースは、同じホストまたは代替ホストにリストアできます。ログバックアップのリカバリおよび可用性グループの再シードはサポートされていません。

### • 手順 \*

1. Cloud Manager UI で、\* Backup & Restore \* > \* Applications \* の順にクリックします。
2. [ \* フィルター条件 \* ] フィールドで、フィルター \* タイプ \* を選択し、ドロップダウンから \* SQL \* を選択します。
3. 「\* 詳細表示 \*」をクリックすると、使用可能なすべてのバックアップが表示されます。
4. バックアップを選択し、\* リストア \* をクリックします。
5. データベースファイルのリストア先を選択します。

オプション	説明
バックアップが作成されたホストにデータベースをリストアします	バックアップを作成した SQL Server にデータベースをリストアする場合は、このオプションを選択します。
データベースを代替ホストにリストアします	<p>バックアップを作成したホストと同じまたは別のホストの別の SQL Server にデータベースをリストアする場合は、このオプションを選択します。</p> <p>ホスト名を選択し、データベース名を指定し（オプション）、インスタンスを選択し、リストアパスを指定します。</p> <div style="display: flex; align-items: center;">  <div> <p>代替パスに指定するファイル拡張子は、元のデータベースファイルのファイル拡張子と同じにする必要があります。</p> </div> </div> <p>[ リストア範囲 ] ページに [ データベースを別のホストにリストアする * ] オプションが表示されない場合は、ブラウザキャッシュをクリアします。</p>

6. [ \* リストア前オプション \* ] ページで、次のいずれかのオプションを選択します。

- [ リストア時に同じ名前でデータベースを上書きする ] を選択して、同じ名前でデータベースをリストアします。
- データベースをリストアし、既存のレプリケーション設定を保持するには、「 \* SQL データベースのレプリケーション設定を保持 \* 」を選択します。

7. [ リストア後のオプション \* ] ページで、追加のトランザクションログをリストアするためのデータベース状態を指定するには、次のいずれかのオプションを選択します。

- 必要なすべてのバックアップを今すぐリストアする場合は、[ \* Operational 、 but unavailable ] を選択します。

これはデフォルトの動作で、コミットされていないトランザクションをロールバックすることでデータベースを使用可能な状態にします。バックアップを作成するまで追加のトランザクションログはリストアできません。

- コミットされていないトランザクションをロールバックせずにデータベースを非稼働状態のままにするには、[ **Non-operational, but available** ] を選択します。

追加のトランザクションログをリストアできます。データベースはリカバリされるまで使用できません。

- データベースを読み取り専用モードのままにするには、「 \* 読み取り専用モード 」と「 使用可能 \* 」を選択します。

コミットされていないトランザクションはロールバックされますが、ロールバックされた操作がスタンバイファイルに保存されるため、リカバリ前の状態に戻すことができます。



[ディレクトリを元に戻す] オプションが有効になっている場合は、さらに多くのトランザクションログがリストアされます。トランザクションログのリストア処理が失敗した場合は、変更をロールバックできます。詳細については、SQL Server のマニュアルを参照してください。

1. 詳細を確認して、\* リストア \* をクリックします。

# 仮想マシンのデータのバックアップとリストア

## 仮想マシンのデータを保護

SnapCenter Plug-in for VMware vSphereとCloud Managerを統合することで、仮想マシン上のデータを保護できます。データストアをクラウドにバックアップし、仮想マシンをオンプレミスのSnapCenter Plug-in for VMware vSphereにリストアする作業は簡単です。

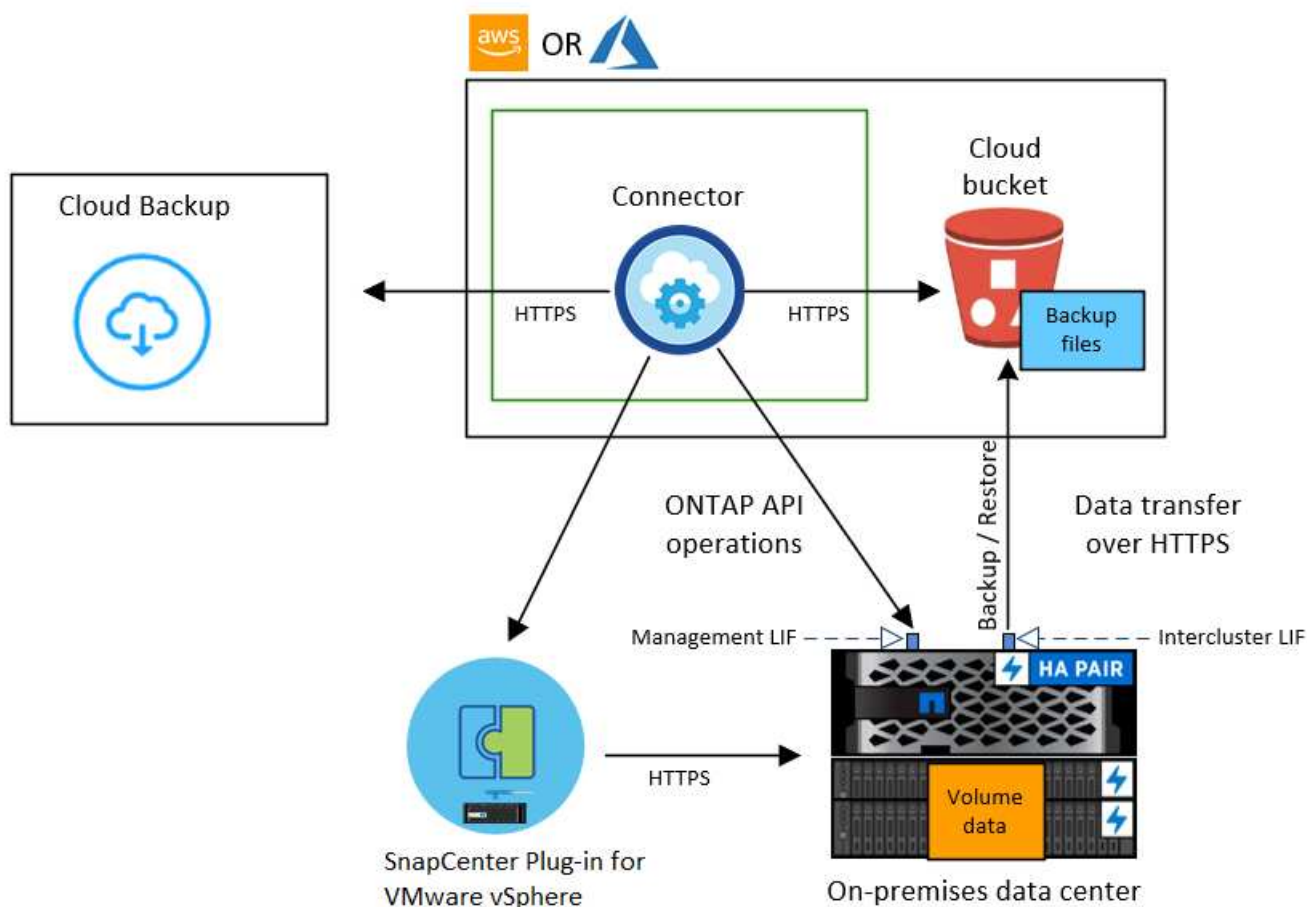
データストアは、Amazon Web Services S3またはMicrosoft Azure Blobにバックアップできます。

### 要件

データストアおよび仮想マシンをクラウドサービスにバックアップする前に、次の要件を確認し、サポートされる構成になっていることを確認してください。

- VMware vSphere 4.6P1以降用のSnapCenter プラグイン
- ONTAP 9.8 以降
- Cloud Manager 3.9以降
- VMware vSphere 4.6P1向けSnapCenter プラグインでは、少なくとも1つのバックアップを作成しておく必要があります。
- SnapCenter Plug-in for VMware vSphereで、Cloud ManagerのCloud Backup for Virtual Machinesポリシーと同じラベルまたは同じラベルの日単位、週単位、または月単位のポリシーが少なくとも1つ必要です。
- 組み込みのポリシーの場合は、スケジュール階層はSnapCenter Plug-in for VMware vSphereとクラウドのデータストアで同じである必要があります。
- FlexGroup ボリュームのバックアップとリストアはサポートされていないため、データストアにFlexGroup ボリュームがないことを確認してください。
- 暗号化されたボリュームのリストアはサポートされていないため、暗号化されたボリュームがないことを確認してください。
- 必要なリソースグループで「\*\_recent\*」を無効にします。リソースグループに対して「\*\_recent\*」が有効になっている場合、これらのリソースグループのバックアップをクラウドへのデータ保護に使用できず、それ以降はリストア処理に使用できません。
- 仮想マシンのリストア先のデータストアに、VMDK、VMX、VMSDなどのすべての仮想マシンファイルのコピーを格納できるだけの十分なスペースがあることを確認してください。
- リストア先のデータストアに、リストア処理でエラーが発生した場合に、restore\_xxx\_xxxxxx\_filename形式の古い仮想マシンファイルが存在しないことを確認してください。リストア処理を開始する前に古いファイルを削除してください。

次の図は、各コンポーネントとその間の準備に必要な接続を示しています。



## 保護ポリシー

データストアをクラウドにバックアップするには、Cloud Backup for Virtual Machineで定義されているいずれかのポリシーを使用する必要があります。



カスタムポリシーはサポートされません。

デフォルトのポリシーを表示するには、Cloud Managerで\* Backup & Restore > Virtual Machines > Policies \* をクリックします。

ポリシー名	ラベル	保持値
1 年ごとの LTR	毎日	366
5 年ごとの LTR	毎日	1830 年に
7 年ごとの LTR	毎週	370
10 年間の月単位 LTR	毎月	120

# データストアをクラウドにバックアップ

SnapCenter Plug-in for VMware vSphereとCloud Managerを統合することで、データストアをクラウドにバックアップできます。これにより、VM管理者はデータのバックアップとアーカイブを簡単かつ迅速に行えるようになり、ストレージ効率を高めてクラウドへの移行を促進できます。



すべてのが満たされていることを確認します **"要件"** データストアをクラウドにバックアップする前に、

## SnapCenter Plug-in for VMware vSphereの登録

データストアと仮想マシンをCloud Managerに表示するには、SnapCenter Plug-in for VMware vSphereをCloud Managerに登録する必要があります。SnapCenter Plug-in for VMware vSphereの登録は、管理者アクセス権を持つユーザのみが実行できます。



複数のSnapCenter Plug-in for VMware vSphereを登録できます。ただし、一度登録すると、SnapCenter Plug-in for VMware vSphereを削除できなくなります。

### 手順

1. Cloud Manager UIで、\* Backup & Restore > Virtual Machines \*をクリックします。
2. [設定]ドロップダウンから、[\* SnapCenter Plug-in for VMware vSphere\*]をクリックします。
3. [\* SnapCenter Plug-in for VMware vSphere\*の登録]をクリックします。
4. 次の情報を指定します。
  - a. SnapCenter Plug-in for VMware vSphereフィールドで、SnapCenter Plug-in for VMware vSphereのFQDNまたはIPアドレスを指定します。
  - b. Portフィールドで、SnapCenter Plug-in for VMware vSphereを実行しているポート番号を指定します。

SnapCenter Plug-in for VMware vSphereとCloud Backup for Applicationsの間で通信を行うためにポートが開いていることを確認する必要があります。


- c. Username and Passwordフィールドで、管理者ロールを持つユーザのクレデンシャルを指定します。
5. [\*Register] をクリックします。
    - 終了後 \*

[バックアップとリストア>仮想マシン]をクリックして、登録済みのSnapCenter Plug-in for VMware vSphereを使用して保護対象となるすべてのデータストアおよび仮想マシンを表示します。

## データストアをバックアップする

単一のポリシーを使用して、1つ以上のデータストアをクラウドに同時にバックアップできます。データストアに割り当てることができるのはデフォルトのポリシーだけです。

### 手順

1. Cloud Manager UIで、\* Backup & Restore > Virtual Machines \*をクリックします。
2. をクリックします  バックアップするデータストアに対応して、\*バックアップのアクティブ化\*をクリックします。
3. 作業環境を追加します。

データストアのバックアップを検出するONTAP クラスタを設定します。いずれかのデータストアの作業環境を追加したら、同じONTAP クラスタにある他のすべてのデータストアでその環境を再利用できます。

- a. SVMに対応する\* Add Working Environment \*をクリックします。
  - b. 作業環境の追加ウィザードで、次の手順を実行します。
    - i. ONTAP クラスタの IP アドレスを指定します。
    - ii. ONTAP クラスタユーザのクレデンシャルを指定してください。
  - c. \* 作業環境の追加 \* をクリックします。
4. クラウドプロバイダを選択して設定します。

#### **Amazon Web Services** を設定します

- a. AWS アカウントを指定します。
- b. AWS Access Keyフィールドで、データ暗号化のキーを指定します。
- c. AWS Secret Keyフィールドで、データ暗号化のパスワードを指定します。
- d. バックアップを作成するリージョンを選択します。
- e. 作業環境として追加した ONTAP クラスタの IP アドレスを指定します。

#### **Microsoft Azure** を設定

- a. Azure サブスクリプション ID を指定します。
- b. バックアップを作成するリージョンを選択します。
- c. 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。
- d. 作業環境として追加した ONTAP クラスタの IP アドレスを指定します。

5. [ポリシーの割り当て] ページで、ポリシーを選択して [次へ\*] をクリックします。
6. 詳細を確認し、\* バックアップのアクティブ化 \* をクリックします。

## 仮想マシンの保護を管理します

データをバックアップおよびリストアする前に、ポリシー、データストア、および仮想マシンを表示できます。データベース、ポリシー、またはリソースグループの変更に応じて、Cloud Manager UI から更新情報を更新できます。

## ポリシーを表示します

デフォルトの組み込みポリシーをすべて表示できます。各ポリシーについて詳細を表示すると、関連付けられているすべてのCloud Backup for Virtual Machinesポリシーと関連するすべての仮想マシンが表示されます。

1. [バックアップと復元]>[仮想マシン\*]をクリックします。
2. [\* 設定] ドロップダウンから、[ポリシー \*] をクリックします。
3. 詳細を表示するポリシーに対応する **View Details** をクリックします。

関連付けられているCloud Backup for Virtual Machinesポリシーとすべての仮想マシンが表示されます。

## データストアと仮想マシンを表示します

登録済みのSnapCenter Plug-in for VMware vSphereを使用して保護されているデータストアと仮想マシンが表示されます。

- このタスクについて \*
- 表示されるのはNFSデータストアのみです。
- SnapCenter Plug-in for VMware vSphereで少なくとも1つの正常なバックアップが作成されているデータストアのみが表示されます。

### 手順

1. Cloud Manager UIで、\* Backup & Restore > Virtual Machines > Settings > SnapCenter Plug-in for VMware vSphere \*をクリックします。
2. データストアおよび仮想マシンを表示するSnapCenter Plug-in for VMware vSphereをクリックします。

## SnapCenter Plug-in for VMware vSphereインスタンスを編集します

SnapCenter Plug-in for VMware vSphereの詳細をCloud Managerで編集できます

### 手順

1. Cloud Manager UIで、\* Backup & Restore > Virtual Machines > Settings > SnapCenter Plug-in for VMware vSphere \*をクリックします。
2. をクリックし、\*編集\*を選択します
3. 必要に応じて詳細を変更します
4. [保存 ( Save ) ] をクリックします。


## 保護ステータスを更新します

新しいボリュームがデータベースに追加された場合やポリシーまたはリソースグループに変更があった場合は、保護を更新する必要があります。

1. [バックアップと復元]>[仮想マシン\*]をクリックします。
2. [設定]ドロップダウンから、[\* SnapCenter Plug-in for VMware vSphere\*]をクリックします。
3. をクリックします ... 仮想マシンをホストしているSnapCenter Plug-in for VMware vSphereに対応しており、\*更新\*をクリックします。



新しい変更が検出されます。

4. をクリックします  データストアに対応し、\*更新保護\*をクリックして変更に対するクラウド保護を有効にします。

## ジョブを監視します

すべてのクラウドバックアップ処理に対してジョブが作成されます。すべてのジョブと、各タスクの一部として実行されるすべてのサブタスクを監視できます。

1. [バックアップと復元]>[ジョブの監視\*]をクリックします。

処理を開始すると、ジョブが開始されたことを示すウィンドウが表示されます。リンクをクリックするとジョブを監視できます。

2. プライマリタスクをクリックすると、これらの各サブタスクのサブタスクとステータスが表示されます。

## クラウドから仮想マシンをリストアします

仮想マシンをクラウドからオンプレミスのvCenterにリストアできます。バックアップは、作成された場所とまったく同じ場所にリストアされます。他の場所にバックアップをリストアすることはできません。仮想マシンはデータストアまたはVMビューからリストアできます。



データストア全体にまたがっている仮想マシンはリストアできません。



すべてのが満たされていることを確認します **"要件"** 仮想マシンをクラウドからリストアする前に、

### 手順

1. Cloud Managerで、\* Backup & Restore > Virtual Machines > SnapCenter Plug-in for VMware vSphere \* をクリックし、仮想マシンをリストアするSnapCenter Plug-in for VMware vSphereを選択します。



ソース仮想マシンが別の場所（vMotion）に移動された場合、ユーザがCloud Managerからその仮想マシンのリストアを実行すると、仮想マシンはバックアップが作成された元のソースの場所にリストアされます。

1. データストアからリストアするには：
  - a. をクリックします  リストアするデータストアに対応し、\*詳細の表示\*をクリックします。
  - b. リストアするバックアップに対応する\* Restore \*をクリックします。
  - c. バックアップからリストアする仮想マシンを選択し、\* Next \*（次へ）をクリックします。
  - d. 詳細を確認して、\* リストア \*をクリックします。
2. 仮想マシンからリストアするには：
  - a. をクリックします  リストアする仮想マシンに対応して、\*リストア\*をクリックします。
  - b. 仮想マシンのリストアに使用するバックアップを選択し、[次へ] をクリックします。
  - c. 詳細を確認して、\* リストア \*をクリックします。

VMiは、バックアップの作成元と同じ場所にリストアされます。

# Cloud Backup API

Web UIから使用できるクラウドバックアップ機能は、RESTful APIからも使用できます。

Cloud Backup Service には、次の8つのエンドポイントカテゴリが定義されています。

- バックアップ
- カタログ
- クラウド
- ジョブ
- 使用許諾
- リストア
- single file-level restore (SFR；単一ファイルレベルリストア)
- 作業環境

## はじめに

Cloud Backup APIを使用するには、ユーザトークン、Cloud CentralアカウントID、およびCloud Connector IDを取得する必要があります。

API呼び出しを行うときは、Authorizationヘッダーにユーザトークンを、x-agent-idヘッダーにCloud Connector IDを追加します。APIでCloud CentralアカウントIDを使用してください。

### 手順

1. NetApp Cloud Central からユーザトークンを取得します。

次のリンクからリフレッシュトークンを生成してください：<https://services.cloud.netapp.com/refresh-token/>リフレッシュトークンは、ユーザトークンを生成するために使用する英数字文字列です。

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
  "grant_type": "refresh_token",
  "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
  "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

2. NetApp Cloud CentralアカウントIDを取得します。

```
GET 'https://cloudmanager.cloud.netapp.com/tenancy/account' -H
'authority: cloudmanager.cloud.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

このAPIは、次のような応答を返します。アカウントIDを取得するには、\*[0].[accountPublicId]\*の出力を解析します。

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}].....
```

### 3. Cloud Manager Connector IDが含まれているx-agent-idを取得します。

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
-H 'authority: api.services.cloud.netapp.com' \
-H 'accept: application/json' \
-H 'accept-language: en-GB,en;q=0.9' \
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

このAPIは、次のような応答を返します。エージェントIDを取得するには、\*occcm.[0].[agent].[AgentID]\*の出力を解析します。

```
{
  "occms": [
    {
      "account": "account-OOnAR4ZS",
      "accountName": "cbs",
      "occ": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Z",
      "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Z",
      "status": "ready",
      "occName": "cbsgcpdevcntsg-asia",
      "primaryCallbackUri": "http://34.93.197.21",
      "manualOverrideUris": [],
      "automaticCallbackUris": [
        "http://34.93.197.21",
        "http://34.93.197.21/occmui",
        "https://34.93.197.21",
        "https://34.93.197.21/occmui",
        "http://10.138.0.16",
        "http://10.138.0.16/occmui",
        "https://10.138.0.16",
        "https://10.138.0.16/occmui",
        "http://localhost",
        "http://localhost/occmui",
        "http://localhost:1337",
        "http://localhost:1337/occmui",
        "https://localhost",
        "https://localhost/occmui",
        "https://localhost:1337",
        "https://localhost:1337/occmui"
      ],
      "createDate": "1652120369286",
      "agent": {
        "useDockerInfra": true,
        "network": "default",
        "name": "cbsgcpdevcntsg-asia",
        "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Zclients",
        "provider": "gcp",
        "systemId": "a3aa3578-bfee-4d16-9e10-"
      }
    }
  ]
}
```

## APIを使用した例

次の例は、AzureクラウドのEast-US-2リージョンで、daily、hourly、weeklyのラベルを設定したあと180日後にアーカイブした新しいポリシーを使用して、Working Environmentでバックアップをアクティブ化するAPI呼び出しを示しています。これにより、作業環境でのみバックアップが有効になりますが、ボリュームはバックアップされません。「auto-backup-enabled」を選択すると、システムにすでに存在するすべてのボリュームと、以降に追加されたボリュームがバックアップされます。

Cloud CentralアカウントID「account-DpTFcxN3」、Cloud Manager Connector ID「iZwFFeVCZjWnzGw8RgD0QNaNZvpP7lclients」、ユーザートークン「Bearer eJhbGciOiJI1zI1I1KUSCUZUZUZ56UZUZUZUSCH56UZUZUZUZUZUZUZUVZUGZUGZUGZ4WISZUGVC5WISLKUZWISLKUx4Q」が使用されています。

```

curl --location --request POST
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSXlPVFUzUWpZek1E...y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
  "provider": "AZURE",
  "backup-policy": {
    "archive-after-days": 180,
    "rule": [
      {
        "label": "hourly",
        "retention": "2"
      },
      {
        "label": "daily",
        "retention": "30"
      },
      {
        "label": "weekly",
        "retention": "52"
      }
    ]
  },
  "ip-space": "Default",
  "region": "eastus2",
  "azure": {
    "resource-group": "rn-test-backup-rg",
    "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
  }
}'

```

応答は、監視可能なジョブIDです。

```

{
  "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}

```



応答を監視します。

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzG1w8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ikp5rSXlPVFUzUWpZek1E...hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

応答。

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

「**status**」が「**completed**」になるまで監視します。

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

トークンの有効期限が切れた場合はどうすればよいですか。

NetApp Cloud Central のユーザトークンの有効期限が切れています。トークンを更新するには、手順 1 から API を再度呼び出す必要があります。

API 応答には、トークンの有効期限を示す「expires\_in」フィールドが含まれています。

## API リファレンス

各Cloud Backup APIのドキュメントは、から入手できます <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>。

# 参照

## AWS S3 アーカイブストレージクラスおよびリストアの読み出し時間

Cloud Backup は、2 つの S3 アーカイブストレージクラスとほとんどのリージョンをサポートします。

### Cloud Backup でサポートされている S3 アーカイブストレージクラスです

バックアップファイルが最初に作成される時は、S3\_Standard\_storage に格納されています。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、すぐにアクセスすることもできます。30 日経過すると、バックアップは S3\_Standard - Infrequent Access\_storage クラスに移行してコストを削減します。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、特定の日数（通常は 30 日以上）が経過したあとに S3 Glacier Deep Archive\_storage にバックアップを階層化して、コストをさらに最適化することができます。これらの階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。についてのセクションを参照してください [アーカイブストレージからのデータのリストア](#)。

このタイプのライフサイクルルールでクラウドバックアップを設定する場合は、AWS アカウントでバケットを設定する際にライフサイクルルールを設定しないでください。

["S3 ストレージクラスについて説明します"](#)。

### アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存すると、標準または標準の IA ストレージよりもはるかに低コストですが、リストア処理のためにアーカイブストレージ内のバックアップファイルからデータにアクセスすると、時間がかかり、コストがかかります。

**Amazon S3 Glacier** と **Amazon S3 Glacier Deep Archive** からデータをリストアするのにどれくらいのコストがかかりますか。

Amazon S3 Glacier からデータを読み出すときは 3 つのリストア優先度を選択でき、Amazon S3 Glacier Deep Archive からデータを読み出すときは 2 つのリストア優先度を選択できます。S3 Glacier Deep Archive のコストは S3 Glacier よりも低く：

アーカイブ階層	優先度とコストを復元します		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	高速な読み出し、コストの最大化	取得速度が低下し、コストが削減されます	読み出しに時間がかかり、コストを最小限に抑えます
* S3 Glacier Deep Archive *		高速な読み出し、コストの増大	取得速度が遅く、コストが最も低い

各メソッドには、GB 単位の取得料金とリクエストごとの料金が異なります。AWS リージョン別の S3 Glacier の詳細な価格設定については、[を参照してください "Amazon S3 の価格設定ページ"](#)。

**Amazon S3 Glacier** にアーカイブされているオブジェクトのリストアにはどれくらいの時間がかかりますか。

リストアの合計時間は、次の 2 つの要素で構成されます。

- **\* 取得時間 \***：アーカイブからバックアップファイルを取得して標準ストレージに保存する時間。これは、「水和」時間と呼ばれることもあります。取得時間は、選択したリストア優先度によって異なります。

アーカイブ階層	優先度と取得時間のリストア		
	* 高 *	* 標準 *	* 低 *
* S3 Glacier *	3 ～ 5 分	3 ～ 5 時間	5 ～ 12 時間
* S3 Glacier Deep Archive *		12 時間	48 時間

- **\* リストア時間 \***：Standard ストレージのバックアップファイルからデータをリストアする時間。アーカイブ層を使用しない場合、この時間は標準ストレージから直接実行される通常のリストア処理と同じです。

Amazon S3 Glacier と S3 Glacier Deep Archive の読み出しオプションの詳細については、を参照してください ["これらのストレージクラスに関する Amazon FAQ"](#)。

## Azure のアーカイブ階層およびリストアの読み出し時間

Cloud Backup は、1 つの Azure アーカイブアクセス階層とほとんどのリージョンをサポートします。

### クラウドバックアップでサポートされている **Azure Blob** アクセス階層

バックアップファイルが最初に作成されるときは、\_Cool\_ アクセス層に保存されます。この階層は、アクセス頻度の低いデータを格納するために最適化されていますが、必要に応じてすぐにアクセスできます。

ソースクラスタで ONTAP 9.10.1 以降が実行されている場合は、コストをさらに最適化するために、特定の日数（通常は 30 日以上）後に \_Cool\_ To Azure Archive\_storage からバックアップを階層化することを選択できます。この階層のデータは、必要なときにすぐにアクセスすることはできず、取得コストが高くなるため、アーカイブされたバックアップファイルからデータをリストアする頻度を考慮する必要があります。次のセクション About を参照してください [アーカイブストレージからのデータのリストア](#)。

このタイプのライフサイクルルールでクラウドバックアップを設定する場合は、Azure アカウントでコンテナを設定する際にライフサイクルルールを設定しないでください。

["Azure Blob アクセス階層の概要について説明します"](#)。

### アーカイブストレージからのデータのリストア

古いバックアップファイルをアーカイブストレージに保存するのは Cool ストレージよりもはるかに安価ですが、リストア処理用に Azure Archive のバックアップファイルからデータにアクセスするには時間がかかり、コストも高くなります。

**Azure Archive** からデータをリストアするのにどれくらいのコストがかかりますか？

Azure Archive からデータを取得する際に選択できるリストア優先度は 2 つあります。

- \* 高い \* : 高速な読み出し、コストの増大
- \* 標準 \* : 読み出し速度が遅く、コストが削減されます

各メソッドには、GB 単位の取得料金とリクエストごとの料金が異なります。Azure リージョン別の Azure Archive の詳細な価格設定については、を参照してください ["Azure の料金体系のページです"](#)。

**Azure Archive** にアーカイブされたデータをリストアするのにどれくらいの時間がかかりますか。

リストア時間は次の 2 つの要素で構成されます。

- \* 取得時間 \* : アーカイブされたバックアップファイルを Azure Archive から取得して Cool Storage に保存する時間。これは、「水和」時間と呼ばれることもあります。読み出し時間は、選択したリストア優先度によって異なります。
  - \* 高 \* : 1 時間未満
  - \* 標準 \* : 15 時間以内
- \* リストア時間 \* : Cool ストレージ内のバックアップファイルからデータをリストアする時間。この時間は、アーカイブ層を使用しないクールストレージからの一般的なリストア処理と同じです。

Azure Archive の読み出しオプションの詳細については、を参照してください ["Azure に関する FAQ です"](#)。

# 知識とサポート

## サポートに登録します

ネットアップテクニカルサポートでサポートケースをオープンするには、事前に Cloud Manager にネットアップサポートサイトのアカウントを追加し、サポートに登録しておく必要があります。

### NSS アカウントを追加します

サポートダッシュボードを使用すると、すべてのネットアップサポートサイトのアカウントを 1 箇所から追加および管理できます。

#### 手順

1. ネットアップサポートサイトのアカウントがない場合は、**"1 名で登録します"**。
2. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、**\* Support \*** を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

3. **[NSS Management] > [Add NSS Account]** をクリックします。
4. メッセージが表示されたら、**[\* Continue (続行) ]** をクリックして Microsoft ログインページにリダイレクトします。

ネットアップは、サポートとライセンスに固有の認証サービスのアイデンティティプロバイダとして Microsoft Azure Active Directory を使用しています。

5. ログインページで、ネットアップサポートサイトの登録 E 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。

Cloud Manager で NSS アカウントを使用することができます。

注：お客様レベルのアカウントである必要があります（ゲストや一時アカウントは使用できません）。



## アカウントを登録してサポートを受けてください

サポートの登録は、Cloud Manager のサポートダッシュボードで実行できます。

### 手順

1. Cloud Manager コンソールの右上にあるヘルプアイコンをクリックし、\* Support \* を選択します。



メニューのスクリーンショット。

サポートは最初に表示されるオプションです"]

2. [\* リソース ] タブで、[\* サポートに登録 \* ] をクリックします。
3. 登録する NSS 資格情報を選択し、\* 登録 \* をクリックします。

## ヘルプを表示します

ネットアップでは、Cloud Manager とその クラウド サービス をさまざまな方法でサポートしています。ナレッジベース（KB）記事やコミュニティフォーラムなど、24 時間 365 日利用可能な幅広いセルフサポートオプションをご用意しています。サポート登録には、Web チケット処理によるリモートテクニカルサポートが含まれます。

### セルフサポート

次のオプションは、1 日 24 時間、週 7 日間無料でご利用いただけます。

- ["ナレッジベース"](#)

Cloud Manager のナレッジベースで問題のトラブルシューティングに役立つ記事を検索してください。

- ["コミュニティ"](#)

Cloud Manager コミュニティに参加して、進行中のディスカッションに参加したり、新しいコミュニティを作成したりできます。

- [ドキュメント](#)

現在表示している Cloud Manager のドキュメント。

- mailto : [ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com) [ フィードバックメール ]

お客様のご意見をお考えください。Cloud Manager の改善に役立つフィードバックを送信します。

## ネットアップサポート

上記のセルフサポートオプションに加え、サポートを有効にしたあとに問題が発生した場合は、ネットアップサポートエンジニアと協力して解決できます。

### 手順

1. Cloud Manager で、 \* Help > Support \* の順にクリックします。
2. テクニカルサポートで利用可能なオプションのいずれかを選択します。
  - a. [ \* お問い合わせ \* ] をクリックして、ネットアップ・テクニカル・サポートの電話番号を検索してください。
  - b. [ \* 問題 を開く \* ] をクリックし、いずれかのオプションを選択して、[ \* 送信 \* ] をクリックします。

ネットアップの担当者がケースを確認し、すぐに対応を開始します。

# 法的通知

著作権に関する声明、商標、特許などにアクセスできます。

## 著作権

<http://www.netapp.com/us/legal/copyright.aspx>

## 商標

NetApp、NetApp のロゴ、および NetApp の商標ページに記載されているマークは、NetApp, Inc. の商標です。その他の会社名および製品名は、それぞれの所有者の商標である場合があります。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## 特許

ネットアップが所有する特許の最新リストは、次のサイトで入手できます。

<https://www.netapp.com/us/media/patents-page.pdf>

## プライバシーポリシー

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## オープンソース

通知ファイルには、ネットアップソフトウェアで使用され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記載されています。

- ["Cloud Manager 3.9 に関する注意事項"](#)
- ["Cloud Backup に関する通知です"](#)
- ["Single File Restore に関する注意事項を参照してください"](#)

## 著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

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、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、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

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、またはその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り特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

## 商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> 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。