



ONTAP データのバックアップとリストア Cloud Backup

NetApp
May 24, 2022

目次

ONTAP データのバックアップとリストア	1
Cloud Backup を使用して ONTAP クラスタのデータを保護します	1
Amazon S3 への Cloud Volumes ONTAP データのバックアップ	8
Cloud Volumes ONTAP データの Azure BLOB ストレージへのバックアップ	17
Cloud Volumes ONTAP データの Google Cloud Storage へのバックアップ	23
オンプレミスの ONTAP データの Amazon S3 へのバックアップ	29
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	42
オンプレミスの ONTAP データを Google Cloud Storage にバックアップする	51
オンプレミスの ONTAP データの StorageGRID へのバックアップ	59
ONTAP システムのバックアップの管理	66
バックアップファイルからの ONTAP データのリストア	82

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 以降では AWS と Azure 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できる、参照可能で検索可能なファイルカタログです。

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の保存先
AWS の Cloud Volumes ONTAP	Amazon S3
Azure の Cloud Volumes ONTAP	Azure Blob の略
Google の Cloud Volumes ONTAP	Google クラウドストレージ
オンプレミスの ONTAP システム	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID

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 *	* ファイルの復元 *
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	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
Azure Blob の略	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入
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
NetApp StorageGRID	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。

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）。

- ・ Browse & Restore を使用してファイルをリストアする場合は、リストアインスタンスが実行されている場合にのみ、コンピューティングコストについてクラウドプロバイダにお支払いください。

インスタンスは、バックアップファイルを参照してリストアする個々のファイルを探すときにのみ実行されます。コストを節約するために使用していない場合、インスタンスはオフになります。

- AWS では、Restore インスタンスはで実行されます ["m5n.xlarge インスタンス"](#) CPU × 4 、 16GB のメモリ、および EBS 専用インスタンスストレージオペレーティングシステムイメージは Amazon Linux 2 です。

m5n.xlarge インスタンスを使用できない領域では、代わりに m5.xlarge インスタンスで Restore が実行されます。

- Azure では、Restore 仮想マシンがで実行されます ["Standard_D4s_v3 VM"](#) CPU × 4 、 メモリ × 16 、 32GiB ディスク × 1 の場合。オペレーティングシステムイメージは CentOS 7.5) です。

インスタンスの名前は *Cloud-Restore-Instance_with Your Account ID Concatenated* です。例：
_Cloud-Restore-Instance-MyAccount 。

- Browse & Restore を使用してボリュームをリストアする場合は、個別のインスタンスや仮想マシンが必要ないため、コストは発生しません。
- 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。
 - AWSでは、 ["Amazon Athena"](#) および ["AWS 接着剤"](#) リソースは新しいS3バケットに導入される。
 - Googleでは、新しいバケットが導入され、が展開されます ["Google Cloud BigQueryサービス"](#) アカウント/プロジェクトレベルでプロビジョニングされます。
- (ONTAP 9.10.1以降を使用するAWSでサポートされる) 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あたり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。もう 1 つの選択肢は、年間契約を取得することです。これは AWS でのみ利用できます。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3つのライセンスオプションがあります。従量課金制 (PAYGO) サブスクリプションと、AWS Marketplaceでの年間契約、お客様所有のライセンスの使用 (BYOL) です。PAYGOサブスクリプションを取得した場合は、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"。

年間契約（AWS のみ）

AWS Marketplace では、12 カ月、24 カ月、または 36 カ月間の契約が 2 件提供されます。

- 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」プラン。
- Cloud Volumes ONTAP とクラウドバックアップをバンドルできる「CVO Professional」プラン。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）。

"毎年の AWS 契約を設定する方法をご確認ください"。

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

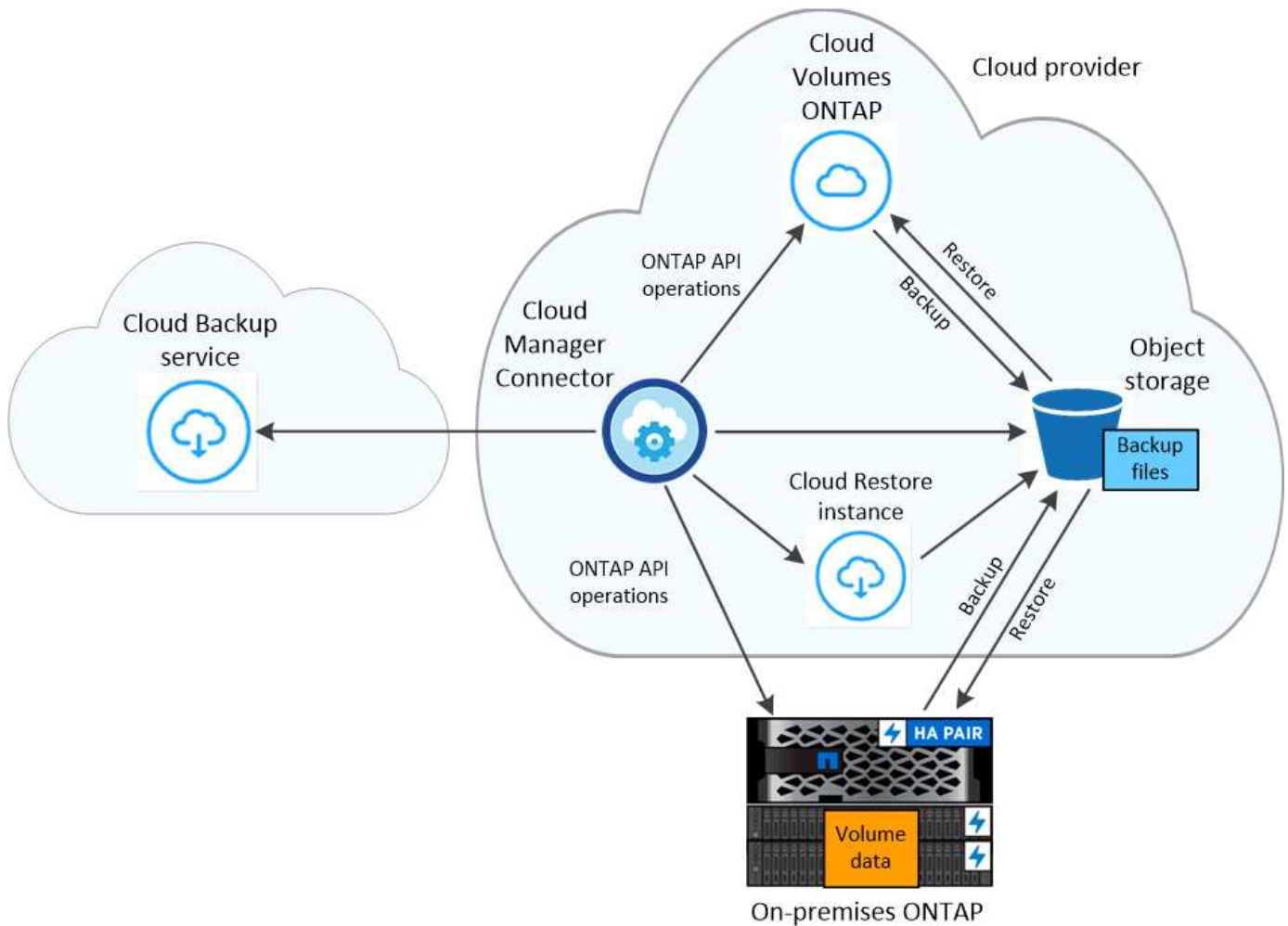
Cloud Volumes ONTAP またはオンプレミスの ONTAP システムでクラウドバックアップを有効にすると、サービスはデータのフルバックアップを実行します。ボリューム Snapshot はバックアップイメージに含まれません。初期バックアップ後は、追加のバックアップはすべて差分になります。つまり、変更されたブロックと新しいブロックのみがバックアップされます。これにより、ネットワークトラフィックを最小限に抑えることができます。

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-clusteruuiid」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。

- AWS では、Cloud Manager によって有効になります **"Amazon S3 ブロックのパブリックアクセス機能"** を S3 バケットに配置します。
- 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
- GCP では、Cloud Manager は Google Cloud Storage バケット用のストレージアカウントを持つ新規または既存のプロジェクトを使用します。
- 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。

あとでクラスター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

- AWS では、バックアップは `_Standard_storage` クラスから開始し、30 日後に `_Standard-Infrequent Access_storage` クラスに移行します。

クラスタが ONTAP 9.10.1 以降を使用している場合は、古いバックアップを S3 Glacier Deep Archive_storage のいずれかに階層化して、特定の日数が経過したらコストをさらに最適化することができます。"[AWS アーカイブストレージの詳細は、こちらをご覧ください](#)"。

- 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](#)"。

- GCP では、バックアップはデフォルトで `_Standard_storage` クラスに関連付けられています。

また、`lower cost_Nearline_storage` クラスまたは `_Coldline_or_Archive_storage` クラスを使用することもできます。Google のトピックを参照してください "[ストレージクラス](#)" ストレージクラスの変更については、を参照してください。

- 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できるためには、クラスタで ONTAP 9.10.1 以降（現在は AWS と Azure でサポート）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' ではサポートされていません
- 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。

Amazon S3 への Cloud Volumes ONTAP データのバックアップ

Cloud Volumes ONTAP から Amazon S3 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。

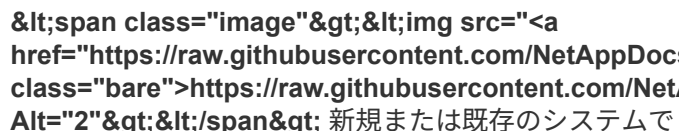
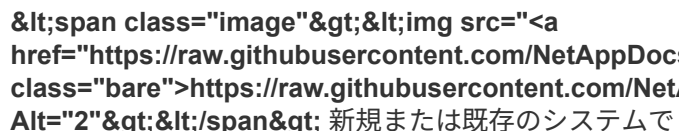
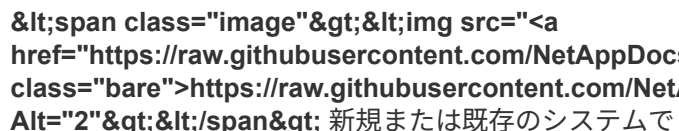
クイックスタート

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>
Alt="one " 設定のサポートを確認します

- Cloud Volumes ONTAP 9.6 以降を AWS で実行している。
- 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"](#)、["AWS 年間契約"](#)または ["アクティブ化されます"](#) NetApp の Cloud Backup BYOL ライセンス。
- Cloud Manager Connector に権限を提供する IAM ロールには、最新のからの S3 権限が含まれています ["Cloud Manager ポリシー"](#)。

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png>  <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png>  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。



ボタンを示すスクリーンショット"]

バックアップを作成する AWS アカウントとリージョンを選択します。また、デフォルトの Amazon S3 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。

バックアップはデフォルトで S3 Standard ストレージに格納されます。クラスタが ONTAP 9.10.1 以降を使用している場合は、S3 Glacier または S3 Glacier Deep 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

☐ Hourly
 Number of backups to retain

☒ Daily
 Number of backups to retain

☐ Weekly
 Number of backups to retain

☐ Monthly
 Number of backups to retain

Archival Policy

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.

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

S3 Glacier
 S3 Glacier Deep Archive

S3 Bucket

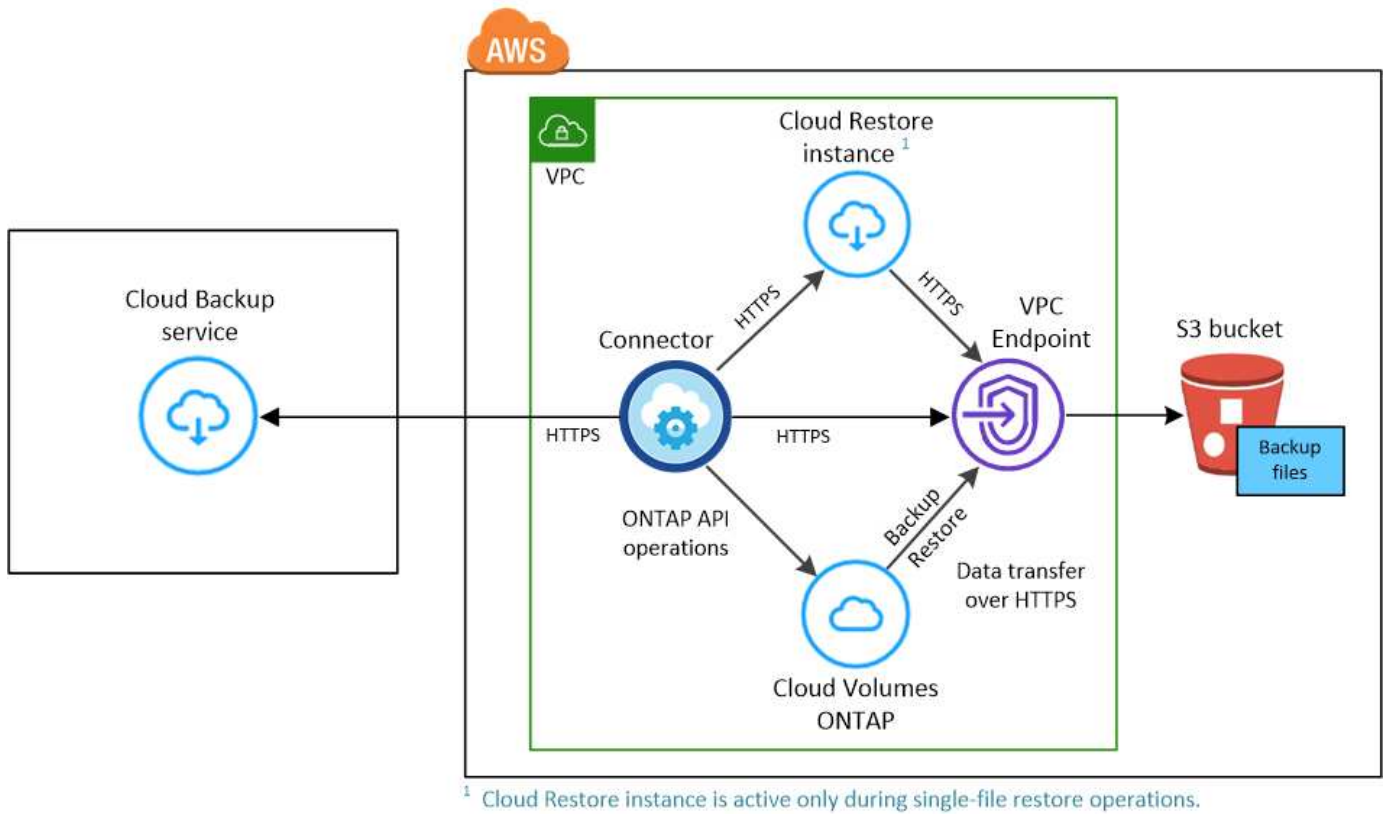
Cloud Manager will create the S3 bucket for you.

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

S3 へのボリュームのバックアップを開始する前に、次の要件を読み、サポートされている構成になってい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。



クラウドに導入されたクラウドリストアインスタンスは、コネクタと同じサブネットに配置されます。

サポートされている **ONTAP** のバージョン

Cloud Volumes ONTAP 9.6 以降

ライセンス要件

Cloud Backup 従量課金制のライセンスの場合は、AWS Marketplace で Cloud Manager サブスクリプションを購入して、Cloud Volumes ONTAP とクラウドバックアップを導入できます。必要です "[この Cloud Manager サブスクリプションに登録してください](#)" Cloud Backup を有効にする前に、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 Volumes ONTAP データとオンプレミスの ONTAP データの両方をバックアップできる年間契約の場合は、から登録する必要があります "[AWS Marketplace のページ](#)" 次に "[サブスクリプションを AWS クレデンシャルに関連付けます](#)"。

Cloud Volumes ONTAP とクラウドバックアップをバンドルできる年間契約については、Cloud Volumes ONTAP 作業環境の作成時に年間契約を設定する必要があります。このオプションでは、オンプレミスのデータをバックアップすることはできません。

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用の AWS アカウントが必要です。

サポートされている **AWS** リージョン

Cloud Backup はすべての AWS 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](#)" AWS GovCloud リージョンを含む。

別の **AWS** アカウントでバックアップを作成する場合の必須のセットアップです

デフォルトでは、Cloud Volumes ONTAP システムに使用されるアカウントと同じアカウントを使用してバックアップが作成されます。バックアップに別の AWS アカウントを使用する場合は、が必要です ["AWS ポータルにログインして、2 つのアカウントをリンクできます"](#)。

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

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。この場合は、暗号化管理キーがすでに設定されている必要があります。 ["独自のキーの使用方法を参照してください"](#)。

AWS Backup 権限が必要です

Cloud Manager に権限を提供する IAM ロールが必要です 最新の S3 権限を含める ["Cloud Manager ポリシー"](#)。

ポリシーの具体的な権限を次に示します。

```

{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
},

```

バージョン 3.9.15 以降を使用してコネクタを導入した場合、これらの権限はすでに IAM ロールに含まれている必要があります。そうでない場合は、不足している権限を追加する必要があります。検索とリストアに必要な「アテナ」と「グルー」の権限を明確に示します。

AWS Restore 権限が必要です

以下の EC2 権限は、Cloud Manager にアクセス許可を付与する IAM ロールに対して必要です。この権限は、Browse & Restore 処理で Cloud Restore インスタンスを起動、停止、終了できるようにします。

```
"Action": [
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "ec2:TerminateInstances"
]
```

AWS 環境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

Cloud Restore インスタンスには、アウトバウンドのインターネットアクセスが必要です。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、インスタンスがアウトバウンドのインターネットアクセスを使用して次のエンドポイントに接続していることを確認してください。

エンドポイント	目的
\ http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/x86_64/4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff3be50e9222/	クラウドリストアインスタンス AMI 用の CentOS パッケージ。
\ https://download.docker.com/linux/centos/docker-ce.repo	Docker Engine パッケージを提供します。
¥ http://cloudmanagerinfraprod.azurecr.io ¥ https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance のイメージリポジトリ。

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 "[AWS での Cloud Volumes ONTAP の起動](#)" を Cloud Volumes ONTAP 参照してください。

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 Amazon Web Services 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. [詳細と資格情報] ページに入力します。
4. [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。



5. 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" AWS の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

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 * :

- a. バックアップの格納に使用する AWS アカウント。これは、Cloud Volumes ONTAP システムが配置されているアカウントとは異なる場合があります。

バックアップに別の AWS アカウントを使用する場合は、が必要です "[AWS ポータルにログインして、2 つのアカウントをリンクできます](#)"。

- b. 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。

- c. デフォルトの Amazon S3 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 AWS アカウントから選択してデータの暗号化を管理するか。 ("[独自の暗号化キーの使用方法を参照してください](#)")。

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。

- 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、S3 Glacier または S3 Glacier Deep Archive ストレージにバックアップを階層化して一定の日数後にコストを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"。

4. Select Volumes (ボリ्यू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リ्यूムを選択します。特定のボリ्यू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、それらのボリ्यूムにあとから適用できます。

<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

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

- 。すべてのボリ्यूムをバックアップするには、タイトル行 (☒ Volume Name)。
- 。個々のボリ्यूムをバックアップするには、各ボリ्यूムのボックス (☒ Volume_1)。

5. 今後追加されるすべてのボリ्यूムでバックアップを有効にする場合は、「今後のボリ्यू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" AWS の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

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

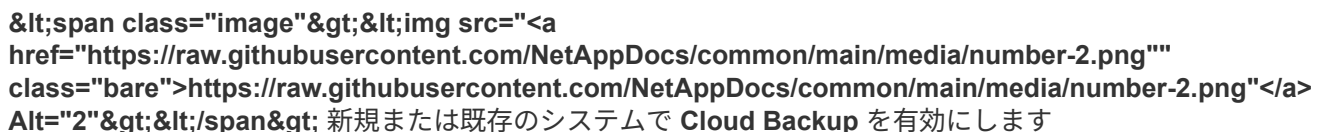
Cloud Volumes ONTAP から Azure Blob Storage へのデータのバックアップを開始するには、いくつかの手順を実行します。

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。

 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"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。

 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。

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

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

☐ Hourly

Number of backups to retain

24

☒ Daily

Number of backups to retain

30

☐ Weekly

Number of backups to retain

52

☐ 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

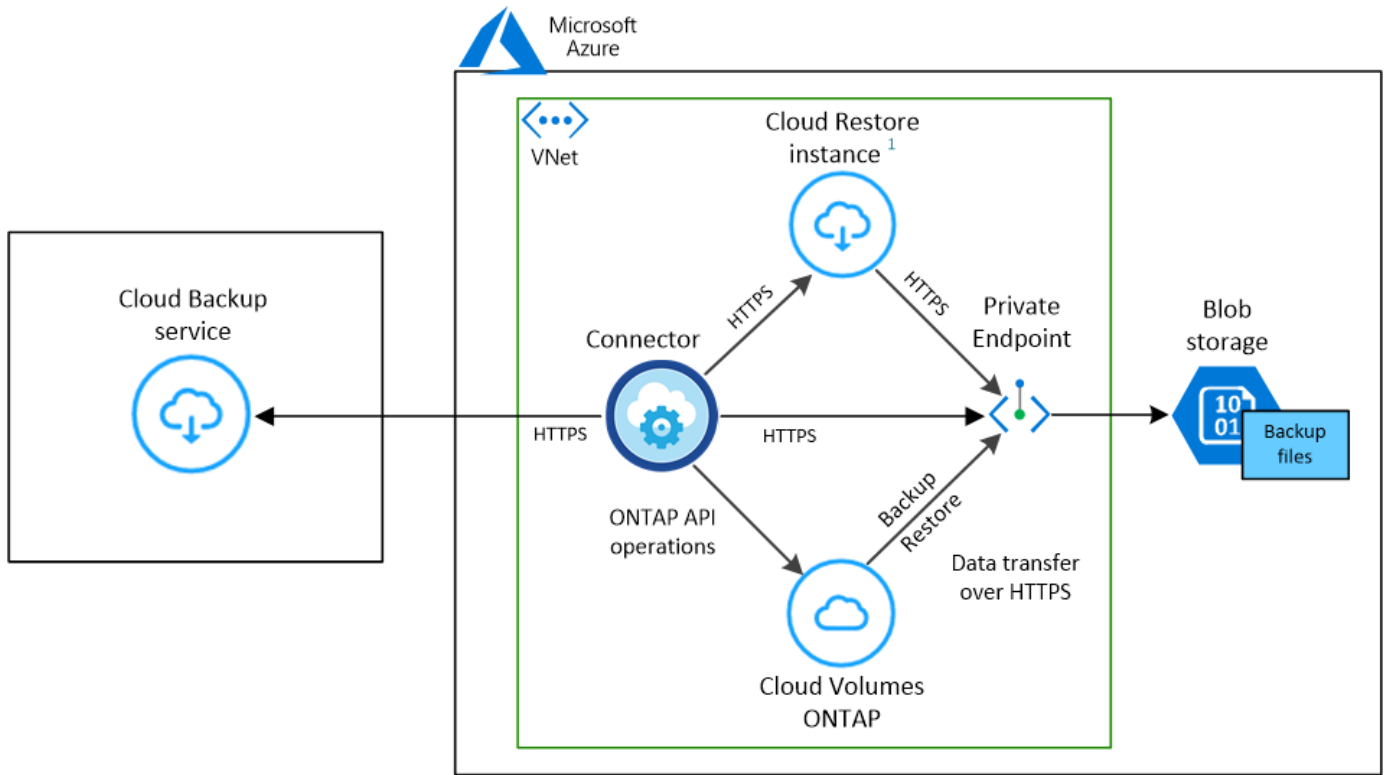
Cloud Manager will create the storage account after you complete the wizard

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。



¹ Cloud Restore instance is active only during single-file restore operations.

クラウドに導入された Cloud Restore 仮想マシンは、コネクタと同じサブネットに配置されます。

サポートされている **ONTAP** のバージョン

Cloud Volumes ONTAP 9.7P5 以降

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。

別の **Azure** サブスクリプションでバックアップを作成するために必要なセットアップ

デフォルトでは、バックアップは Cloud Volumes ONTAP システムと同じサブスクリプションを使用して作成されます。バックアップに別の Azure サブスクリプションを使用する場合は、が必要です "[Azure ポータルにログインして、2 つのサブスクリプションをリンクできます](#)"。

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法を参照してください](#)"。

Azure 環境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

Cloud Restore 仮想マシンには、アウトバウンドのインターネットアクセスが必要です。仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、インスタンスがアウトバウンドのインターネットアクセスを使用して次のエンドポイントに接続していることを確認してください。

エンドポイント	目的
¥ http://olcentgbl.trafficmanager.net ¥ https://olcentgbl.trafficmanager.net	Cloud Restore 仮想マシン用の CentOS パッケージが用意されています。
\ https://download.docker.com/linux/centos/docker-ce.repo	Docker Engine パッケージを提供します。
¥ http://cloudmanagerinfraprod.azurecr.io ¥ https://cloudmanagerinfraprod.azurecr.io	Cloud Restore 仮想マシンのイメージリポジトリ。

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 * :

- a. 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。

バックアップに別の Azure サブスクリプションを使用する場合は、が必要です "[Azure ポータルにログインして、2 つのサブスクリプションをリンクできます](#)"。

- b. 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。
- c. 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。
- d. 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。

Cloud Volumes ONTAP データの Google Cloud Storage へのバックアップ

Cloud Volumes ONTAP から Google Cloud 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>
Alt="one"  設定のサポートを確認します

- GCP で Cloud Volumes ONTAP 9.7P5 以降を実行しています。
- バックアップを保存するストレージスペースの有効な GCP サブスクリプションがあります。

- Google Cloud Project に、事前定義された Storage Admin ロールを持つサービスアカウントがあります。
- 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。

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png> **Alt="2"**; 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、新しい作業環境ウィザードを完了すると有効にできます。
- 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。



バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project を選択します。

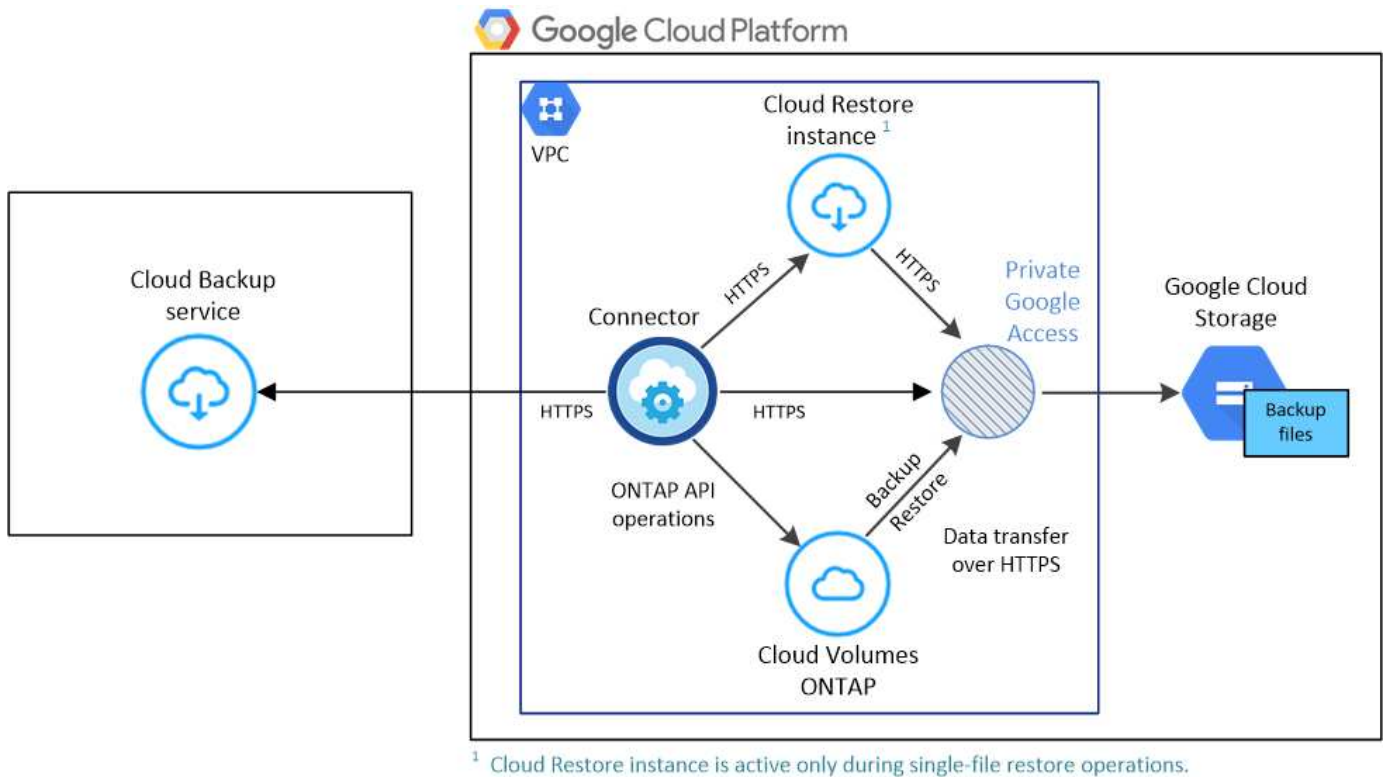
デフォルトポリシーでは、毎日ボリュームがバックアップされ、各ボリュームの最新の 30 個のバックアップコピーが保持されます。毎時、毎日、毎週、または毎月のバックアップに変更するか、システム定義のポリシーの中からオプションを追加する 1 つを選択します。保持するバックアップコピーの数を変更することもできます。

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。

要件

Google Cloud ストレージ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。

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

Cloud Volumes ONTAP 9.7P5 以降

サポートされる **GCP** リージョン

Cloud Backup はすべての GCP 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"](#)。

ライセンス要件

クラウドバックアップは従量課金制のライセンスで、を使用したサブスクリプション ["GCP Marketplace"](#) は、Cloud Backup を有効にする前に必要です。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、バックアップを保存するストレージスペースの Google サブスクリプションが必要です。

GCP サービスアカウント

事前定義された Storage Admin ロールを持つサービスアカウントが Google Cloud Project に必要です。 "[サービスアカウントの作成方法について説明します](#)"。

コネクタの権限を確認または追加します

Cloud Backupの検索とリストア機能を使用するには、Connectorの役割に特定の権限を付与して、Google Cloud BigQueryサービスにアクセスできるようにする必要があります。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

手順

1. インチ "[Cloud Console の略](#)"をクリックし、* Roles * ページに移動します。
2. ページ上部のドロップダウンリストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタムロールをクリックします。
4. 役割の権限を更新するには、* 役割の編集 * をクリックします。
5. [権限の追加 *] をクリックして、次の新しい権限を役割に追加します。

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. [更新 (Update)] をクリックして、編集したロールを保存する。

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 Cloud Volumes ONTAP システムを新規に作成したときに有効にすることができます。

サービスアカウントがすでに設定されている必要があります。Cloud Volumes ONTAP システムの作成時にサービスアカウントを選択しなかった場合は、システムをオフにして、GCP コンソールから Cloud Volumes ONTAP にサービスアカウントを追加する必要があります。

を参照してください "[GCP での Cloud Volumes ONTAP の起動](#)" を Cloud Volumes ONTAP 参照してください。

手順

1. [作業環境] ページで、[* 作業環境の追加 *] をクリックし、画面の指示に従います。
2. * 場所を選択 * : 「* Google Cloud Platform * 」を選択します。

3. * タイプを選択 * : 「 * Cloud Volumes ONTAP * 」 (シングルノードまたはハイアベイラビリティ) を選択します。
4. * 詳細と認証情報 * : 次の情報を入力します。
 - a. 使用するプロジェクトがデフォルトのプロジェクト (Cloud Manager が配置されているプロジェクト) と異なる場合は、 * Edit Project * をクリックして新しいプロジェクトを選択します。
 - b. クラスタ名を指定します。
 - c. サービスアカウント * スイッチを有効にし、事前定義されたストレージ管理者ロールを持つサービスアカウントを選択します。これは、バックアップと階層化を有効にするために必要です。
 - d. クレデンシャルを指定します。

GCP Marketplace のサブスクリプションが登録されていることを確認します。

Details & Credentials

Project1 MPAWSSubscription1222 Edit Project

Google Cloud Project Marketplace Subscription

Details

Working Environment Name (Cluster Name)

TamiVSA

Service Account ⓘ ☒

Service Account Name

ServiceAccount1

+ Add Labels Optional Field | Up to four labels

Credentials

User Name

admin

Password

Confirm Password

5. * サービス : **Cloud Backup Service** は有効のままにして、【 続行 】をクリックします。

Services

Backup to Cloud ☒ ▼

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 を参照してください ["GCP での Cloud Volumes ONTAP の起動"](#)。

Cloud Backup はシステム上で有効になり、毎日作成したボリュームをバックアップし、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 "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" Google の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

既存のシステムでの **Cloud Backup** の有効化

Cloud Backup は、作業環境からいつでも直接有効にすることができます。

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。

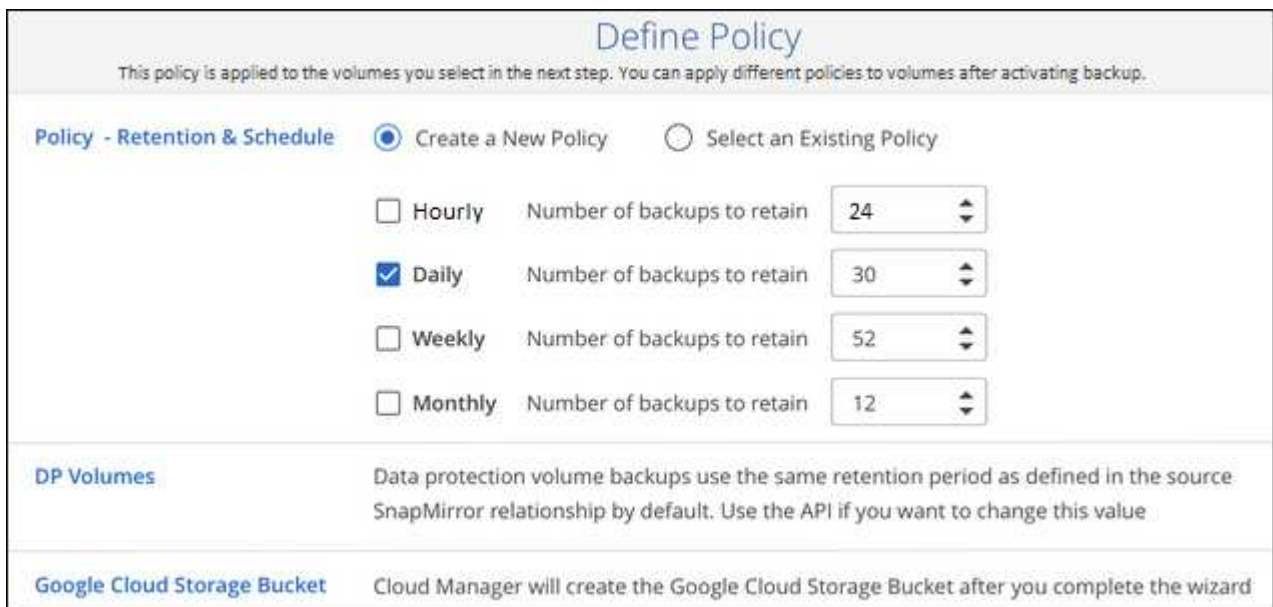


2. Google Cloud Storage バケットをバックアップ用に作成する Google Cloud Project とリージョンを選択し、* Next * をクリックします。



プロジェクトには、事前定義された Storage Admin ロールを持つサービスアカウントが必要です。

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。

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 ["バックアップファイルからボリュームまたはファイルをリストアする"](#) Google の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

オンプレミスの ONTAP データの Amazon S3 へのバックアップ

オンプレミスの ONTAP システムから Amazon S3 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。各手順の詳細については、このトピックの以降のセクションを参照してください。

オンプレミスのONTAP クラスタをパブリックインターネット経由でAWS S3に直接接続するか、VPNとAWS Direct Connectのどちらを使用してトラフィックをAWS S3にルーティングするかを選択します。

[使用可能な接続方法を参照してください。](#)

AWS VPC にすでにコネクタが導入されている場合は、すべてのポートが設定されます。ない場合は、ONTAP データを AWS S3 ストレージにバックアップするために、AWS でコネクタを作成する必要があります。また、コネクタのネットワーク設定をカスタマイズして AWS S3 に接続できるようにする必要があります。

[コネクタの作成方法および必要なネットワーク設定の定義方法を参照してください。](#)

Cloud Manager で ONTAP クラスタを検出し、クラスタが最小要件を満たしていることを確認し、クラスタが AWS S3 に接続できるようにネットワーク設定をカスタマイズします。

[オンプレミスの ONTAP クラスタを準備する方法をご確認ください。](#)

S3 バケットの作成と管理、リストアインスタンスを使用したデータのリストアを実行するためのコネクタの権限を設定します。さらに、オンプレミスの ONTAP クラスタの権限を設定して、S3 バケットに対してデータの読み取りと書き込みを行えるようにします。

必要に応じて、デフォルトの Amazon S3 暗号化キーを使用する代わりに、データ暗号化用に独自のカスタム管理キーを設定することもできます。[AWS S3 環境で ONTAP バックアップを受け取る準備を整える方法をご紹介します。](#)

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] をクリックします。次に、セットアップウィザードに従って、デフォルトのバックアップポリシーおよび保持するバックアップの数を定義し、バックアップするボリュームを選択します。

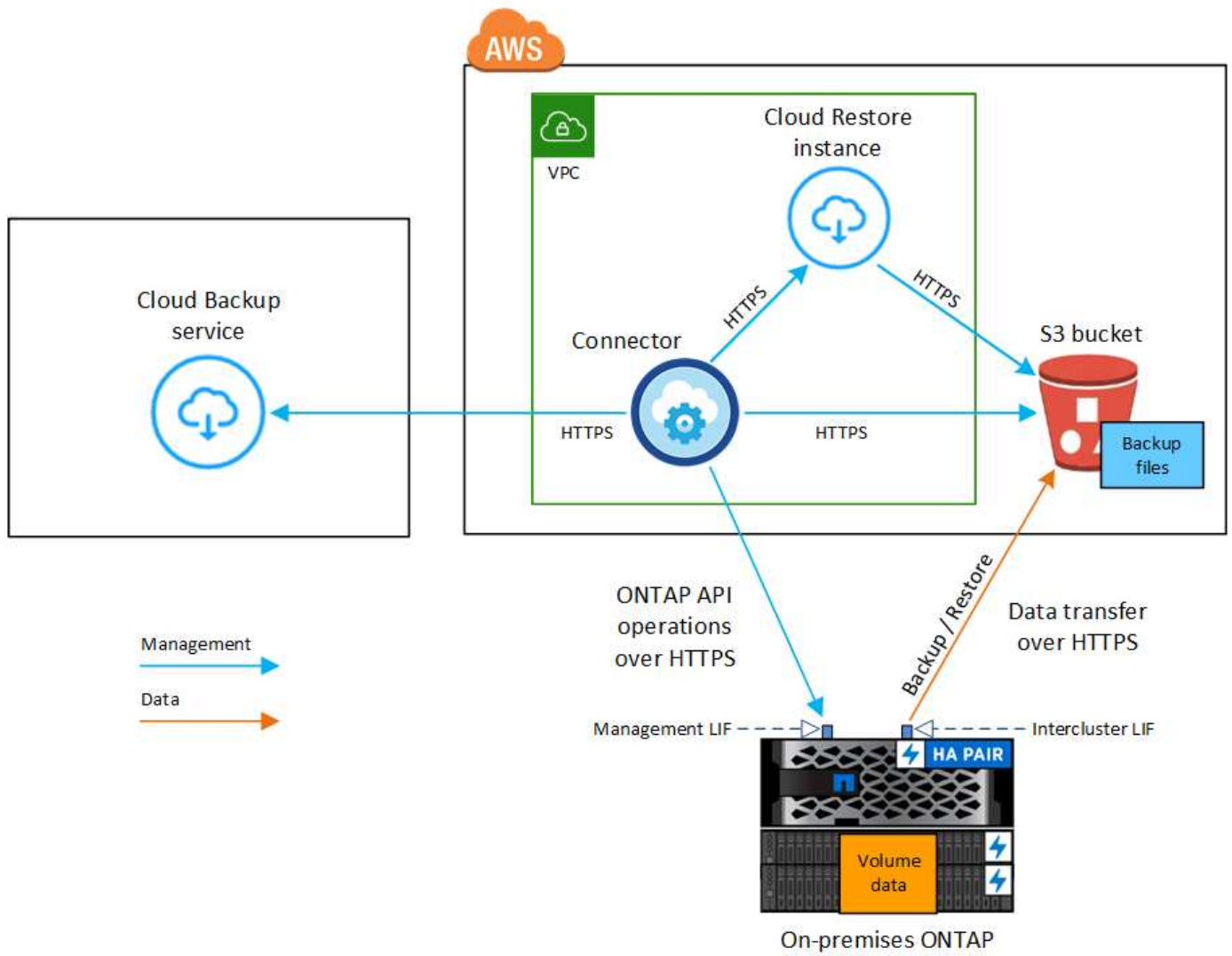
[ボリュームで Cloud Backup をアクティブ化する方法をご覧ください。](#)

接続オプションのネットワークダイアグラム

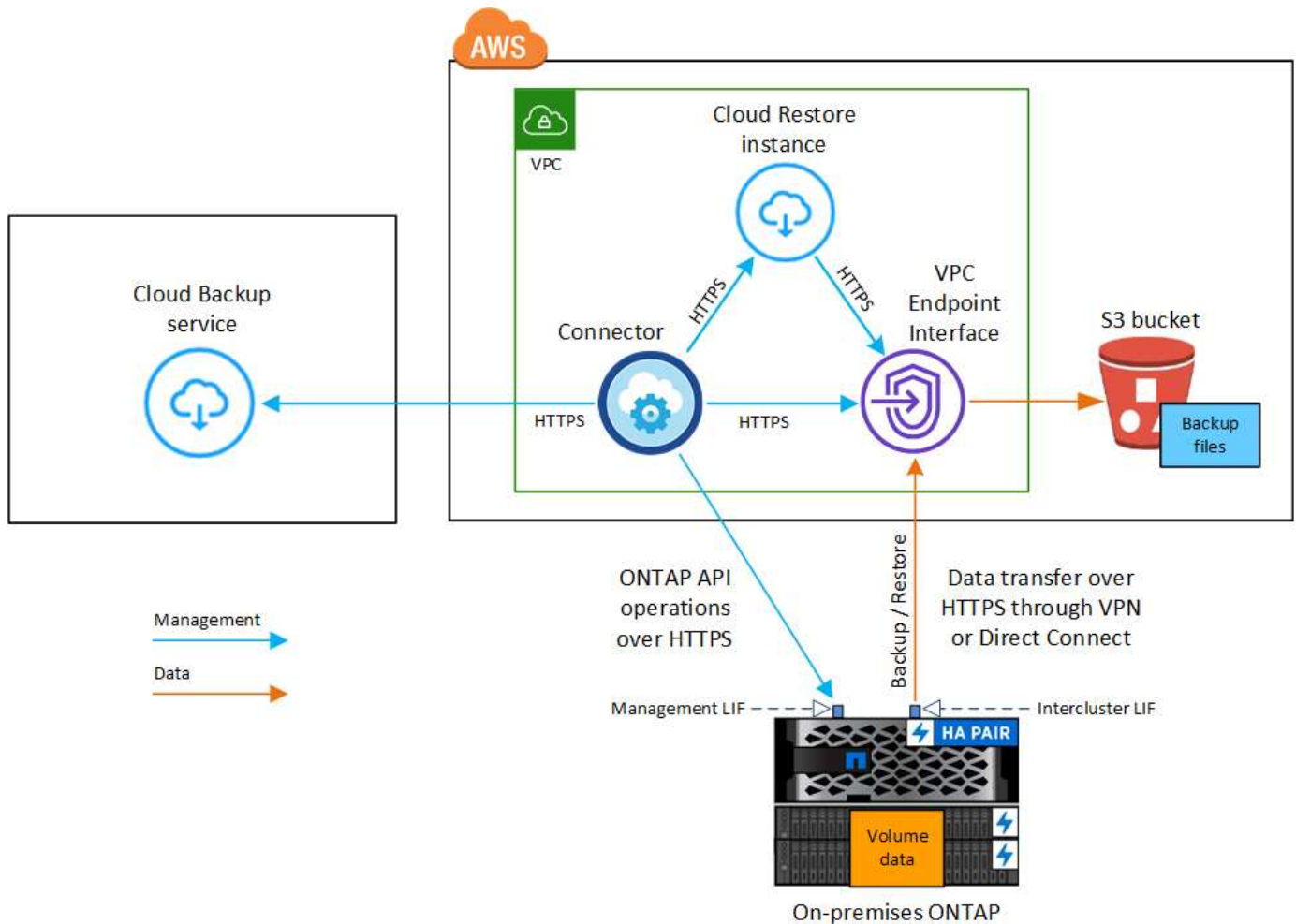
オンプレミスの ONTAP システムから AWS S3 へのバックアップを設定する際に使用できる接続方法は 2 つあります。

- パブリック接続 - パブリック S3 エンドポイントを使用して、ONTAP システムを AWS S3 に直接接続します。
- プライベート接続 - VPN または AWS Direct Connect を使用して、プライベート IP アドレスを使用する VPC エンドポイントインターフェイス経由で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。



クラウドにクラウドリストアインスタンスが導入されている場合、クラウドリストアインスタンスはコネクタと同じサブネットに配置されます。

コネクタを準備します

Cloud Manager Connector は、Cloud Manager 機能のメインソフトウェアです。ONTAP データのバックアップとリストアにはコネクタが必要です。

コネクタの作成または切り替え

AWS VPC にすでにコネクタが導入されている場合は、すべてのポートが設定されます。ない場合は、AWS S3 ストレージに ONTAP データをバックアップするために、AWS で新しいコネクタを作成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や、別のクラウドプロバイダに導入されているコネクタは使用できません。

- "コネクタについて説明します"
- "コネクタの使用を開始する"
- "AWS でコネクタを作成します"

コネクタのネットワーク要件

- 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経由でのCloud Backup Service およびS3オブジェクトストレージへのHTTPS接続（エンドポイントのリストを参照） ["こちらをご覧ください"](#)
 - ONTAP クラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- ["コネクタにS3バケットを管理する権限があることを確認します"](#)。
- ONTAP クラスタからVPCへのDirect ConnectまたはVPN接続が確立されている状態で、コネクタとS3の間の通信をAWS内部ネットワークのままにする場合は、S3へのVPCエンドポイントインターフェイスを有効にする必要があります。 [VPC エンドポイントインターフェイスの設定方法を参照してください](#)。

ONTAP クラスタを準備

Cloud Manager で ONTAP クラスタを検出

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。クラスタを追加するには、クラスタ管理 IP アドレスと admin ユーザアカウントのパスワードが必要です。

["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

- クラスタには、コネクタからクラスタ管理 LIF へのインバウンド HTTPS 接続が必要です。
- 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。これらのクラスタ間 LIF がオブジェクトストアにアクセスできる必要があります。

クラスタは、バックアップおよびリストア処理のために、インタークラスタ LIF から Amazon S3 ストレージへのポート 443 経由のアウトバウンド 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なく、応答するだけです。

- クラスタ間 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。これらの LIF が関連付

けられている IPspace を選択します。これは、「デフォルト」の IPspace または作成したカスタム IPspace です。

「default」以外の IPspace を使用する場合は、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。

IPspace内のすべてのクラスター間LIFがオブジェクトストアにアクセスできる必要があります。現在のIPspaceに対してこれを設定できない場合は、すべてのクラスター間LIFがオブジェクトストアにアクセスできる専用のIPspaceを作成する必要があります。

- ボリュームが配置されている Storage VM 用に DNS サーバが設定されている必要があります。方法を参照してください ["SVM 用に DNS サービスを設定"](#)。
- ファイアウォールルールを必要に応じて更新して、ONTAP からオブジェクトストレージへのクラウドバックアップ接続をポート 443 経由で許可し、Storage VM から DNS サーバへの名前解決トラフィックをポート 53（TCP / UDP）経由で許可します。
- AWSでS3接続にプライベートVPCインターフェイスエンドポイントを使用している場合は、HTTPS / 443 を使用するために、S3エンドポイント証明書をONTAP クラスターにロードする必要があります。 [VPC エンドポイントインターフェイスのセットアップ方法を参照して、S3 証明書をロードしてください](#)。
- ["ONTAP クラスターにS3バケットへのアクセス権限があることを確認します"](#)。

ライセンス要件を確認

- クラスターでCloud Backupをアクティブ化するには、事前に従量課金制（PAYGO）のCloud Manager MarketplaceでAWSから提供するか、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 ["AWS Cloud Manager Marketplace のサービス"](#) クラウドバックアップを使用できます。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。
 - 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"](#)。
- バックアップを格納するオブジェクトストレージスペース用の AWS サブスクリプションが必要です。

すべてのリージョンで、オンプレミスシステムから Amazon S3 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"](#) AWS GovCloud 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。

AWS 環境を準備

S3 権限をセットアップする

次の 2 つの権限セットを設定する必要があります。

- S3 バケットの作成と管理、およびリストアインスタンスを使用したデータのリストアを実行するコネクタの権限。
- オンプレミスの ONTAP クラスターの権限。 S3 バケットに対してデータの読み取りと書き込みを行うことができます。

手順

1. (最新のから) 次の S3 権限を確認します **"Cloud Manager ポリシー"** は、コネクタに権限を付与する IAM ロールの一部です。

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",
    "glue:CreateTable",
    "glue:CreateDatabase",
    "glue:GetPartitions",
    "glue:BatchCreatePartition",
    "glue:BatchDeletePartition"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
}
```

バージョン 3.9.15 以降を使用してコネクタを導入した場合、これらの権限はすでに IAM ロールに含まれている必要があります。そうでない場合は、不足している権限を追加する必要があります。検索とリストアに必要な「アテナ」と「グルー」の権限を具体的に指定します。を参照してください **"AWS のドキュメント：「Editing IAM policies」**。

2. Browse & Restore 操作で Cloud Restore インスタンスを起動、停止、および終了できるように、コネクタに権限を付与する IAM ロールに次の EC2 権限を追加します。

```
"Action": [  
    "ec2:DescribeInstanceTypeOfferings",  
    "ec2:StartInstances",  
    "ec2:StopInstances",  
    "ec2:TerminateInstances"  
],
```

3. サービスをアクティブ化すると、バックアップウィザードにアクセスキーとシークレットキーの入力を求められます。これらのクレデンシャルは、ONTAP がデータをバックアップして S3 バケットにリストアできるように ONTAP クラスタに渡されます。そのためには、次の権限を持つ IAM ユーザを作成する必要があります。

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

を参照してください ["AWS ドキュメント：「Creating a Role to Delegate Permissions to an IAM User」](#) を参照してください。

Cloud Restore インターネットアクセスを確認します

仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、Cloud Restore インスタンスがアウトバウンドのインターネットアクセスを使用して次のエンドポイントに接続していることを確認してください。

エンドポイント	目的
\ http://amazonlinux.us-east-1.amazonaws.com/2/extras/docker/stable/ x86_64 /4bf88ee77c395ffe1e0c3ca68530dfb3a683ec65a4a1ce9c0ff3be50e9222/	クラウドリストアインスタンス AMI 用の CentOS パッケージ。
\ https://download.docker.com/linux/centos/docker-ce.repo	Docker Engine パッケージを提供します。
¥ http://cloudmanagerinfraprod.azurecr.io ¥ https://cloudmanagerinfraprod.azurecr.io	Cloud Restore Instance のイメージリポジトリ。

データ暗号化用に、お客様が管理する**AWS**キーをセットアップ

デフォルトのAmazon S3暗号化キーを使用してオンプレミスクラスとS3バケット間でやり取りされるデータを暗号化する場合は、デフォルトのインストールでそのタイプの暗号化が使用されるため、すべての暗号化キーが設定されます。

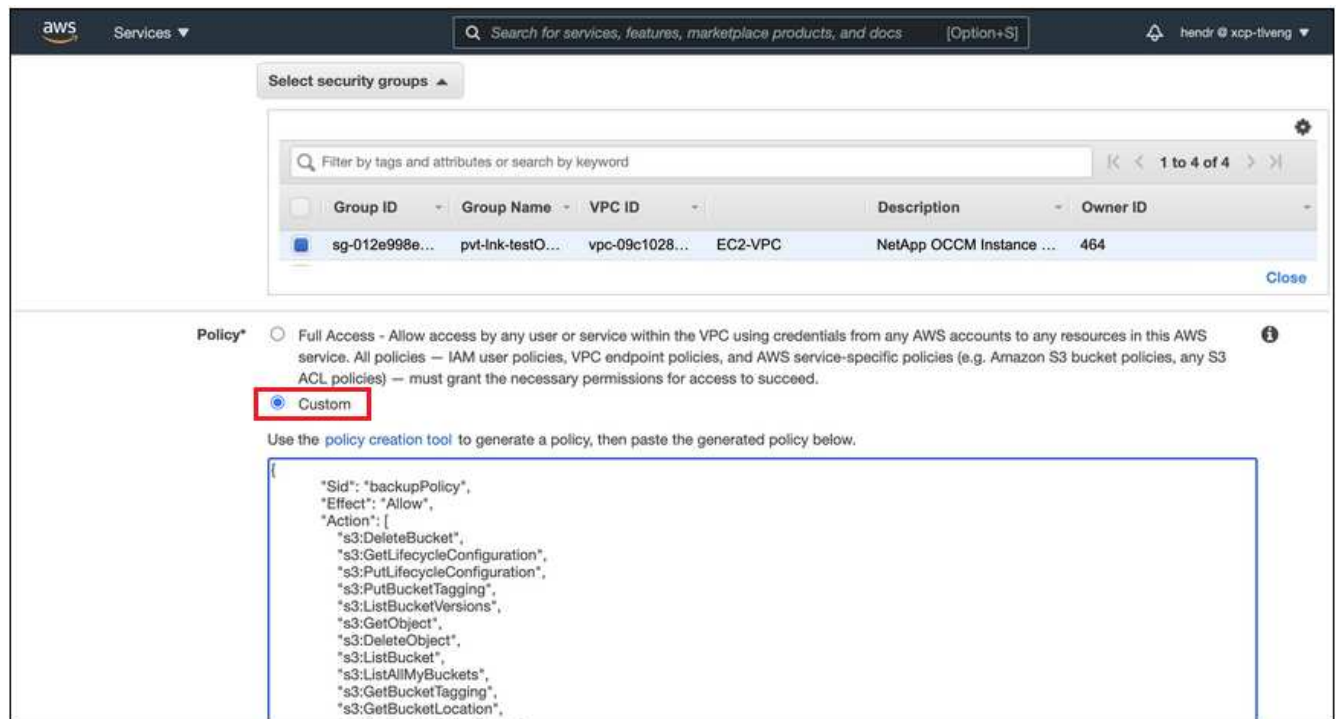
デフォルトのキーではなく、お客様が管理する独自のキーを使用してデータ暗号化を行う場合は、クラウドバックアップウィザードを開始する前に、暗号化で管理されるキーがすでにセットアップされている必要があります。"[独自のキーの使用方法を参照してください](#)"。

VPCエンドポイントインターフェイスを使用して、システムにプライベート接続を設定します

標準のパブリックインターネット接続を使用する場合は、すべてのアクセス権がコネクタによって設定され、他に必要な操作はありません。このタイプの接続がに表示されます "[最初のダイアグラム](#)"。

オンプレミスのデータセンターからVPCへのインターネット接続をよりセキュアにする場合は、バックアップアクティブ化ウィザードでAWS PrivateLink接続を選択できます。VPNまたはAWS Direct Connectを使用して、プライベートIPアドレスを使用するVPCエンドポイントインターフェイス経由でオンプレミスシステムに接続する場合は、この環境が必要です。このタイプの接続がに表示されます "[2番目の図](#)"。

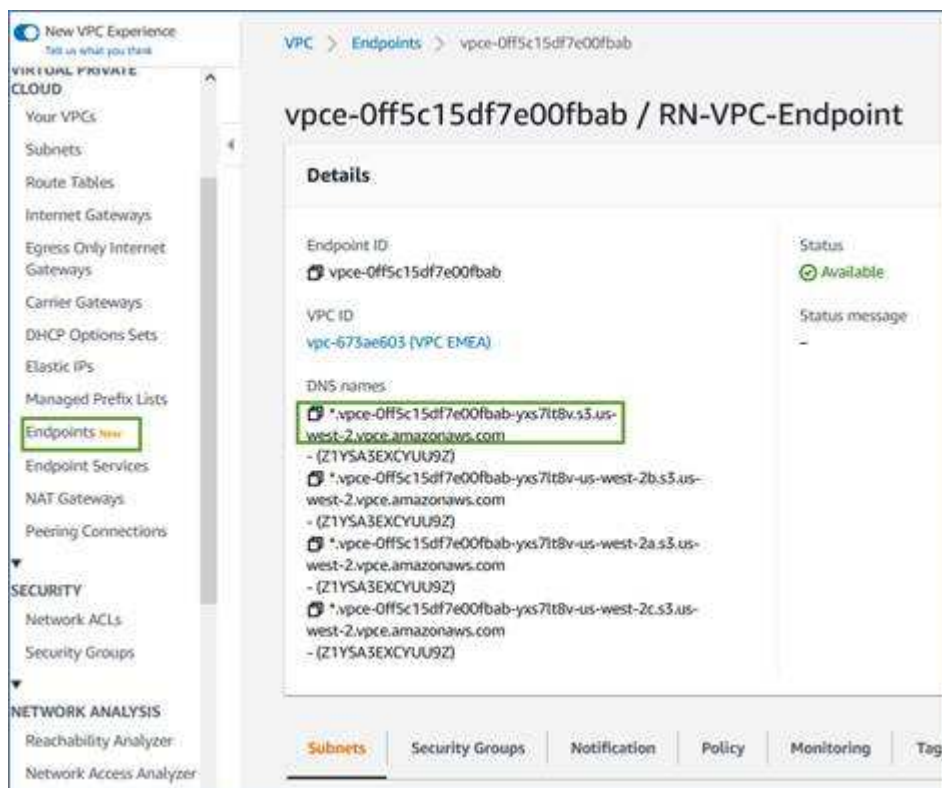
1. Amazon VPC コンソールまたはコマンドラインを使用して、インターフェイスエンドポイント設定を作成します。"[AWS PrivateLink for Amazon S3 の使用に関する詳細を参照してください](#)"。
2. Cloud Manager Connector に関連付けられているセキュリティグループの設定を変更します。このポリシーを「Custom」（「Full Access」から）に変更する必要があります。また、変更する必要があります [バックアップポリシーから S3 権限を追加します](#) 前に示したように、



プライベートエンドポイントとの通信にポート80（HTTP）を使用している場合は、すべて設定されます。クラスターで Cloud Backup を有効にすることができます。

ポート443（HTTPS）を使用してプライベートエンドポイントと通信する場合は、VPC S3エンドポイントから証明書をコピーし、次の4つの手順でONTAP クラスターに追加する必要があります。

3. AWS コンソールからエンドポイントの DNS 名を取得します。



4. VPC S3 エンドポイントから証明書を取得します。これは、で行います **"Cloud Manager Connector をホストする VM にログインします"** 実行するコマンドエンドポイントの DNS 名を入力するときは、先頭に「*」を追加して、「*」を置き換えます。

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. このコマンドの出力から、S3 証明書のデータ（BEGIN / END CERTIFICATE タグを含む、との間のすべてのデータ）をコピーします。

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvboZ/oO2NWLLFCqI+xmKLCMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. ONTAP クラスタの CLI にログインし、次のコマンドを使用してコピーした証明書を適用します（代わりに独自の Storage VM 名を指定します）。

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
Please enter Certificate: Press <Enter> when done
```

Cloud Backup を有効にします

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 Amazon Web Services 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. バックアップの格納に使用する AWS アカウント、AWS Access Key、および Secret Key。

アクセスキーとシークレットキーは、ONTAP クラスタに S3 バケットへのアクセスを付与するために作成した IAM ユーザ用のものです。

b. バックアップを格納する AWS リージョン。

c. デフォルトの Amazon S3 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 AWS アカウントから選択して、データの暗号化を管理できます。 ("[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。AWS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）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、以前に設定した AWS PrivateLink を使用するかどうかを選択します。 "[AWS PrivateLink for Amazon S3 の使用に関する詳細を参照してください](#)"。

Networking

IPspace

IP_Space_1

☒ Private Link Configuration

Select Private Link

Name	VPC	Endpoint ID
<input type="radio"/> Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/> Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

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。
- 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、S3 Glacier または S3 Glacier Deep Archive ストレージにバックアップを階層化して一定の日数後にコストを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 Number of backups to retain 24

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain 52

☐ Monthly Number of backups to retain 12

Archival Policy

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.

☒ Tier Backups to Archival

Archive after (Days) 30

Storage Class S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

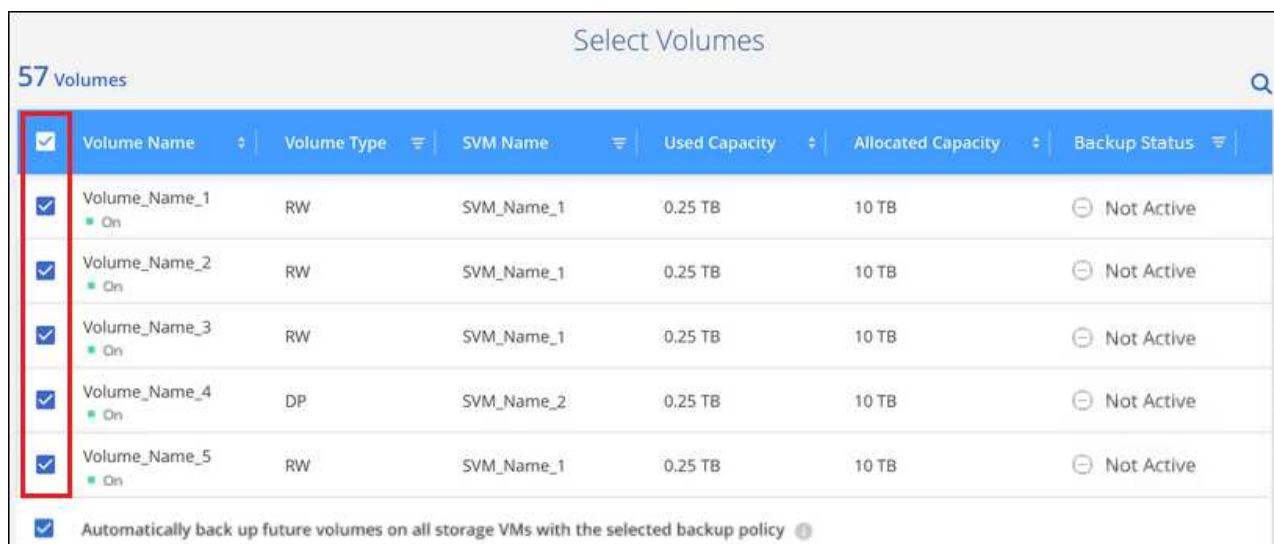
S3 Bucket Cloud Manager will create the S3 bucket for you.

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 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

☒ 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" AWS の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。

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。

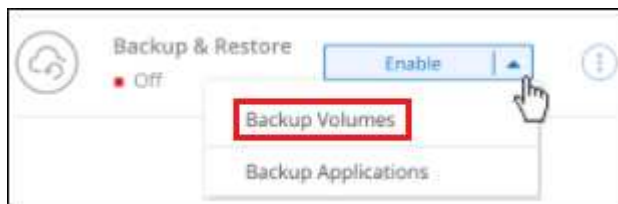
クイックスタート

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 and options:

- Policy - Retention & Schedule:**
 - Buttons: **Create a New Policy** (selected) and **Select an Existing Policy**.
 - Hourly:** ☐ Number of backups to retain: 24
 - Daily:** ☒ Number of backups to retain: 30
 - Weekly:** ☐ Number of backups to retain: 52
 - Monthly:** ☐ Number of backups to retain: 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):** 30
 - Access Tier:** Azure Archive
- 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。

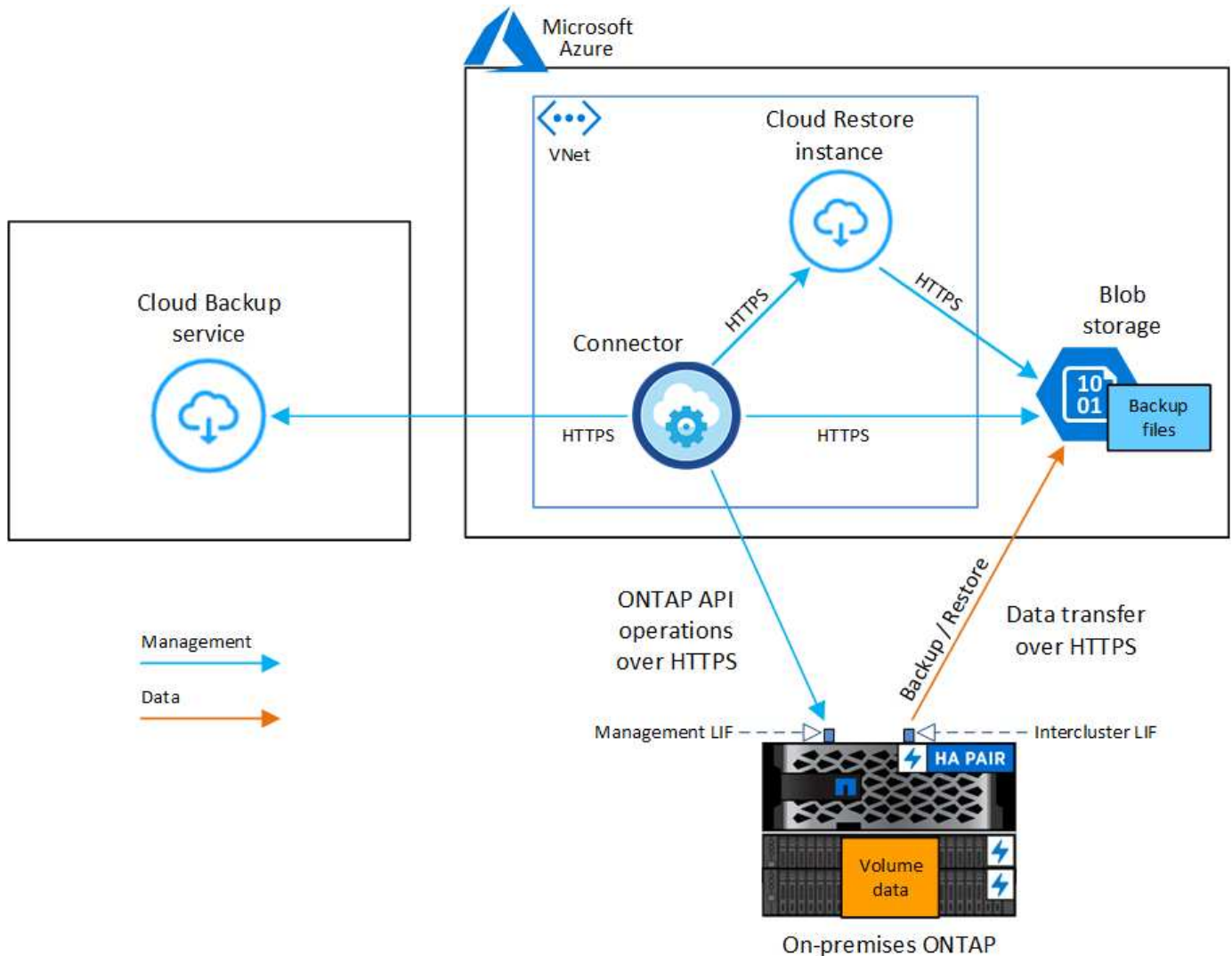
要件

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。

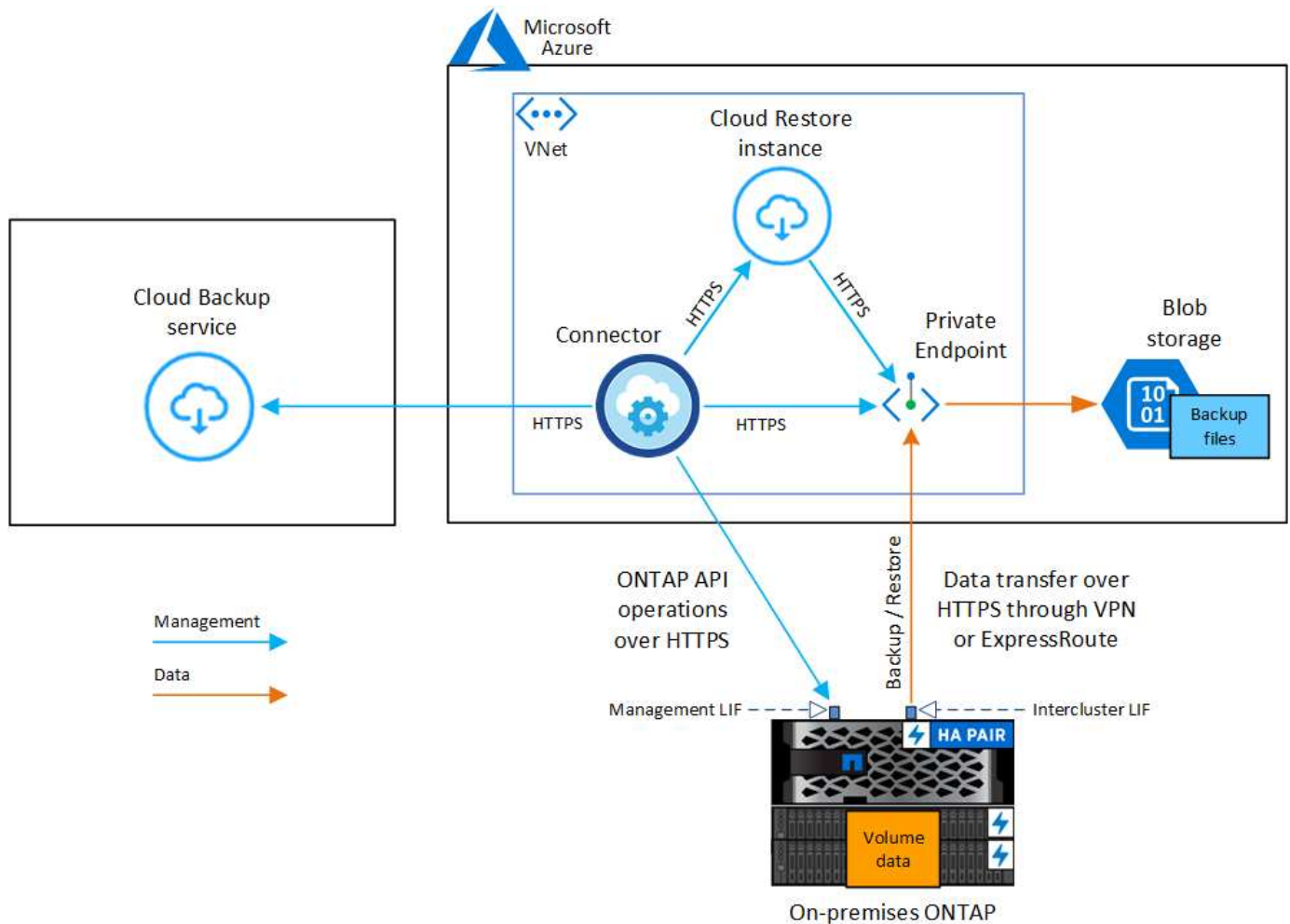
オンプレミスの ONTAP システムから Azure Blob へのバックアップを設定する場合は、2 つの接続方法を使用できます。

- 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、パブリック接続の方法と、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、プライベート接続方法と、コンポーネント間の準備に必要な接続を示しています。



クラウドにクラウドリストアインスタンスが導入されている場合、クラウドリストアインスタンスはコネクタと同じサブネットに配置されます。

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
- SnapMirror ライセンス（Premium Bundle または Data Protection Bundle に含まれます）。
- 注：* Cloud Backup を使用する場合は、「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プ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リブするか、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. 仮想ネットワークまたは物理ネットワークでインターネットアクセスにプロキシサーバを使用している場合は、Cloud Restore 仮想マシンでアウトバウンドのインターネットアクセスを有効にして、次のエンドポイントに接続してください。

エンドポイント	目的
¥ http://olcentgbl.trafficmanager.net ¥ https://olcentgbl.trafficmanager.net	Cloud Restore 仮想マシン用の CentOS パッケージが用意されています。
\ https://download.docker.com/linux/centos/docker-ce.repo	Docker Engine パッケージを提供します。
¥ http://cloudmanagerinfraprod.azurecr.io ¥ https://cloudmanagerinfraprod.azurecr.io	Cloud Restore 仮想マシンのイメージリポジトリ。

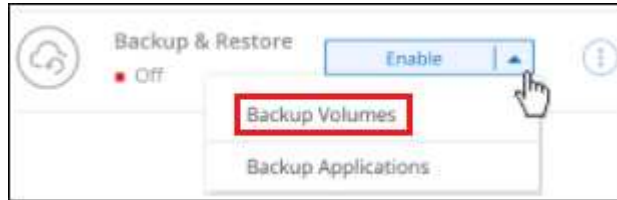
2. Microsoft が管理するデフォルトの暗号化キーではなく、アクティベーションウィザードで、独自のカスタム管理キーを使用してデータを暗号化します。この場合、Azure サブスクリプション、キー・ボールド名、およびキーが必要です。 "[独自のキーの使用方法を参照してください](#)"。
3. オンプレミスのデータセンターから VNet へのパブリックインターネット経由での接続をより安全にするには、アクティベーションウィザードで Azure Private Endpoint を設定するオプションがあります。この場合、この接続用の VNet とサブネットについて理解しておく必要があります。 "[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](#)")。

A screenshot of the 'Provider Settings' form for Azure. It contains several fields: 'Azure Subscription' (dropdown menu with 'Azure_Subscription_1'), 'Region' (dropdown menu with 'Default_CM_Region'), 'Resource Group' (radio buttons for 'Create a new' and 'Use an existing', with 'Use an existing' selected), and 'Encryption' (radio buttons for 'Microsoft-managed' and 'Customer-managed', with 'Microsoft-managed' selected). Below the 'Resource Group' section, there is a dropdown menu labeled 'Select an Existing Resource Group' with 'Resource_Group_1' selected.

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"](#)。

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)。

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

☒ 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 データを Google Cloud Storage にバックアップする

オンプレミスの ONTAP システムから Google Cloud 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。

「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。
- クラスタから Google ストレージ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。
- コネクタに、Google ストレージおよびクラスタへの必要なネットワーク接続がある。
- バックアップを格納するオブジェクトストレージスペース用の有効な Google サブスクリプションが必要です。
- ONTAP クラスタがデータをバックアップおよびリストアできるように、アクセスキーとシークレットキーを持つ Google アカウントを用意しておきます。

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 Google Cloud を選択し、プロバイダ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。

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

DP Volumes

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

Google Cloud Storage Bucket

Cloud Manager will create the Google Cloud Storage Bucket 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。

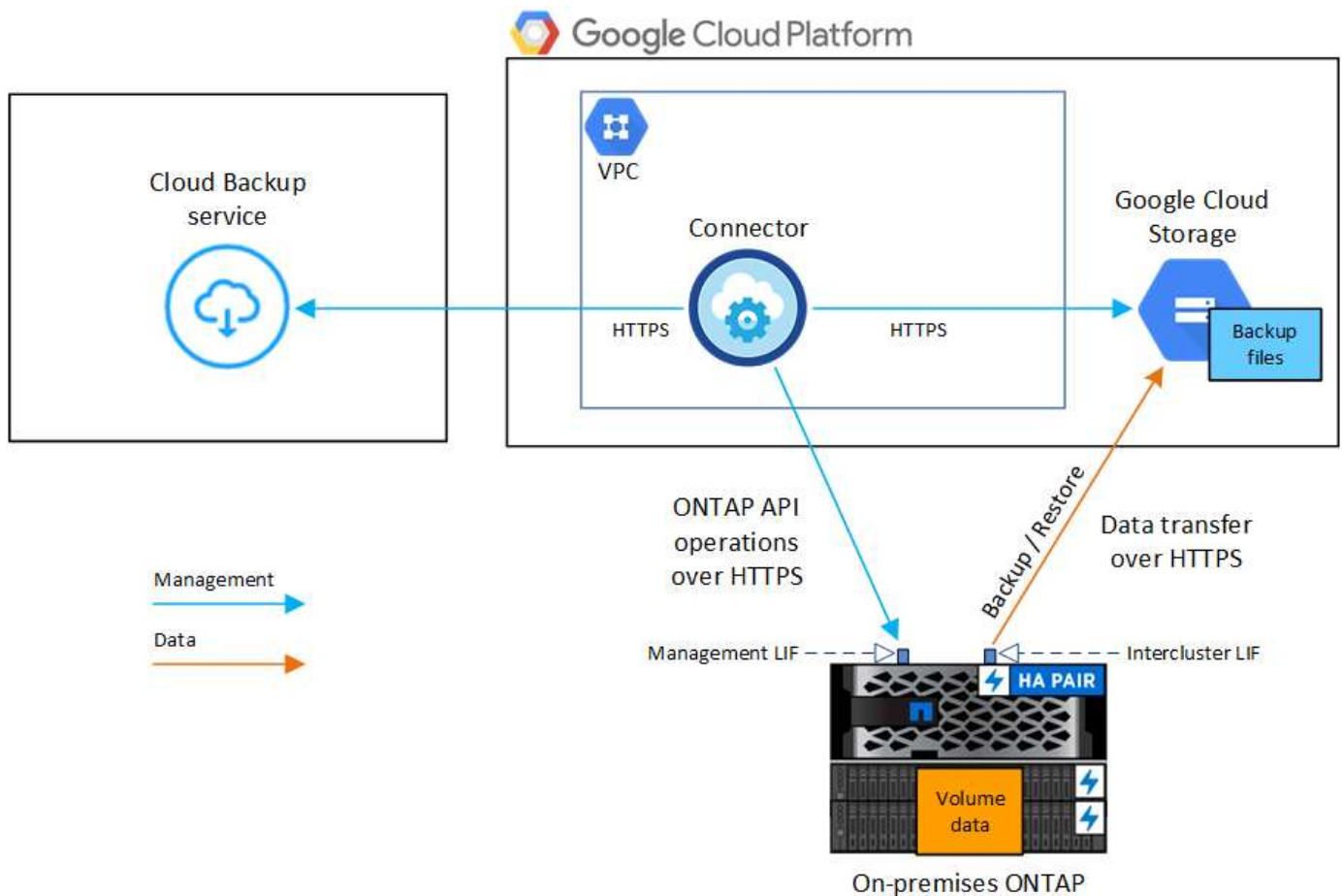
要件

オンプレミスボリュームを Google Cloud ストレージ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。

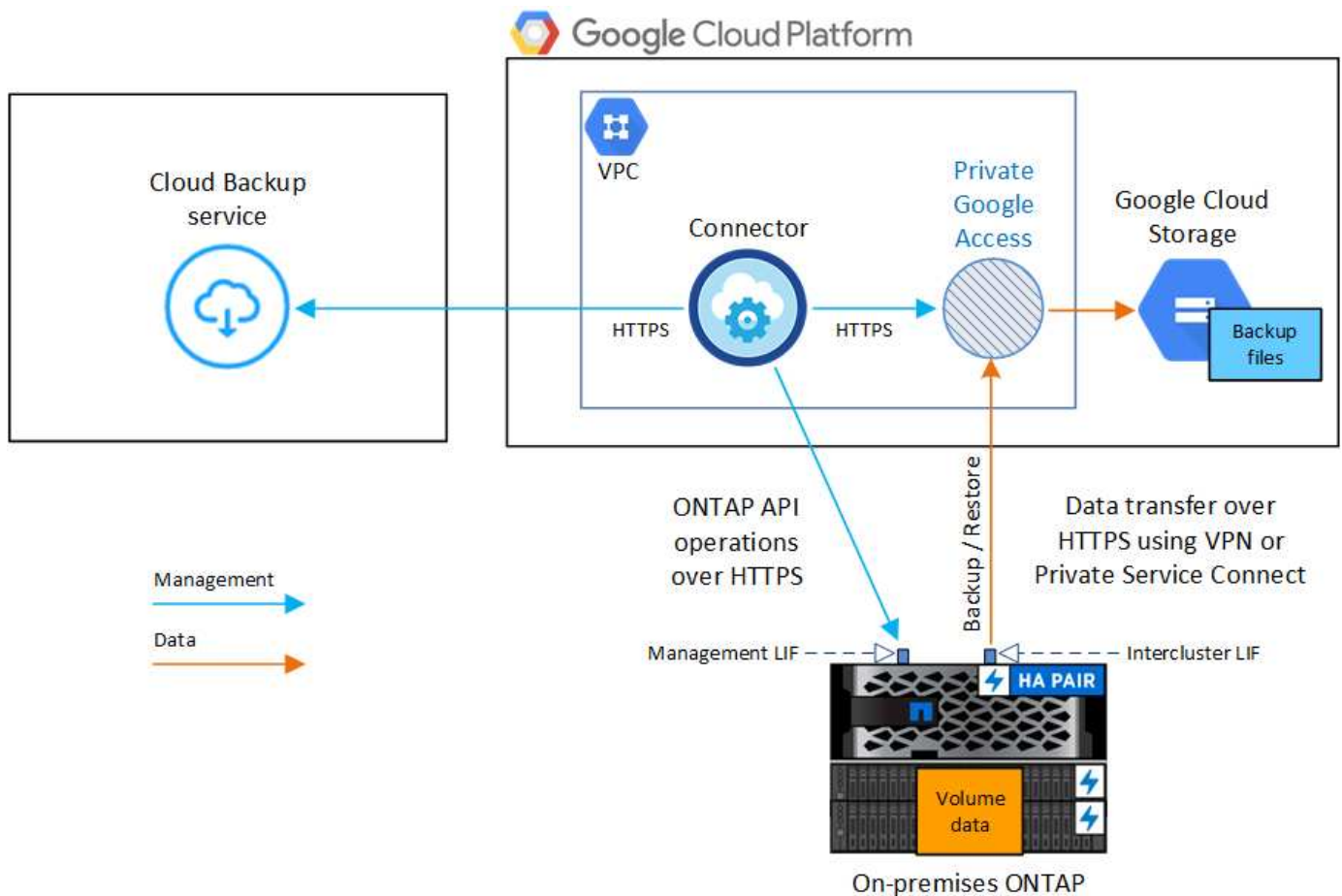
オンプレミスの ONTAP システムから Google Cloud Storage へのバックアップを設定する際に使用できる接続方法は 2 つあります。

- パブリック接続 - パブリック Google エンドポイントを使用して、ONTAP システムを Google Cloud Storage に直接接続します。
- プライベート接続 - VPN またはプライベートサービス接続を使用して、プライベート IP アドレスを使用するプライベート Google アクセスインターフェイスを介してトラフィックをルーティングします。

次の図は、パブリック接続の方法と、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、プライベート接続方法と、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
- 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、クラスタ間 LIF から Google Cloud ストレージへのバックアップおよびリストア処理用に、ポート 443 経由で 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。このコネクタは、Google Cloud Platform VPC 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 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。Google Cloud Storage にデータをバックアップする場合は、Connector を Google Cloud Platform VPC に配置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](#)"
- "[GCP 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 Google Cloud 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. Connector を配置するサブネットに Private Google Access を有効にします。"[プライベート Google アクセス](#)" ONTAP クラスタから VPC への直接接続が確立されており、Connector と Google Cloud Storage 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は、が必要です。

プライベート Google アクセスは、内部（プライベート）IP アドレスのみ（外部 IP アドレスは使用しない）を持つ VM インスタンスで機能します。

コネクタの権限を確認または追加します

Cloud Backupの検索とリストア機能を使用するには、Connectorの役割に特定の権限を付与して、Google Cloud BigQueryサービスにアクセスできるようにする必要があります。以下の権限を確認し、ポリシーを変更する必要がある場合は手順に従います。

手順

1. インチ ["Cloud Console の略"](#)をクリックし、* Roles * ページに移動します。
2. ページ上部のドロップダウンリストを使用して、編集するロールを含むプロジェクトまたは組織を選択します。
3. カスタムロールをクリックします。
4. 役割の権限を更新するには、* 役割の編集 * をクリックします。
5. [権限の追加 *] をクリックして、次の新しい権限を役割に追加します。

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. [更新 (Update)] をクリックして、編集したロールを保存する。

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、事前に従量課金制 (PAYGO) のCloud Manager Marketplace製品をGoogleから購入するか、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 ["Google"](#) 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"](#)。
- バックアップを格納するオブジェクトストレージスペース用の Google 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Google Cloud Storage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"](#)。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。

Google Cloud Storage でバックアップを準備しています

バックアップを設定するときは、Storage Admin の権限があるサービスアカウントにストレージアクセスキーを指定する必要があります。サービスアカウントを使用すると、Cloud Backup でバックアップの格納に使用する Cloud Storage バケットを認証してアクセスできます。キーは、Google Cloud Storage がリクエストを発行しているユーザーを認識できるようにするために必要です。

手順

1. "事前定義されたストレージ管理者を含むサービスアカウントを作成します ロール"。
2. に進みます "GCP Storage Settings (GCP ストレージ設定) " サービスアカウントのアクセスキーを作成します。
 - a. プロジェクトを選択し、* 互換性 * をクリックします。まだ有効にしていない場合は、[相互運用アクセスを有効にする *] をクリックします。
 - b. [サービスアカウントのアクセスキー *] で、[サービスアカウントのキーの作成 *] をクリックし、作成したサービスアカウントを選択して、[キーの作成 *] をクリックします。

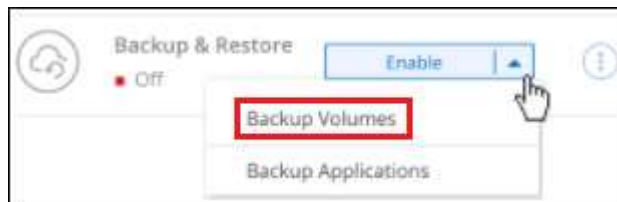
Cloud Backup でキーを入力する必要があるのは、あとでバックアップサービスを設定するときです。

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 Google Cloud を選択し、* 次へ * 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. バックアップ用に Google Cloud Storage バケットを作成する Google Cloud Project。（プロジェクトには、事前定義された Storage Admin ロールを持つサービスアカウントが必要です）。
 - b. バックアップの保存に使用する Google Access Key および Secret Key。
 - c. バックアップが保存される Google リージョン。
 - d. 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。

Provider Settings

Provider Information	Location & Connectivity
Google Cloud Project <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Cloud Manager Default Project</div>	Region <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Cloud Manager Default Region</div>
Google Cloud Access Key <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Enter Google Cloud Access Key</div>	IPspace <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">IP_Space_1</div>
Google Cloud Secret Key <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">Enter Google Cloud Secret Key</div>	

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。Googleが提供する従量課金制（PAYGO）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）か、ネットアップが提供する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. [\[Define Policy\]](#) ページで、既存のバックアップスケジュールと保持期間の値を選択するか、新しいデフォルトバックアップポリシーを定義して、[\[* 次へ *\]](#)をクリックします。

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

DP Volumes Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

Google Cloud Storage Bucket Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

を参照してください ["既存のポリシーのリスト"](#)。

6. **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						

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。

7. 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 "バックアップファイルからボリュームまたはファイルをリストアする" Google の Cloud Volumes ONTAP システムやオンプレミスの ONTAP システムに接続できます。


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

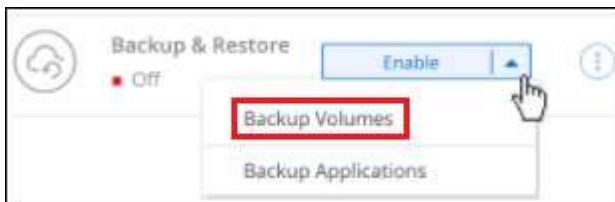
これらの手順を実行すると、すぐに作業を開始できます。また、残りのセクションまでスクロールして詳細を確認することもできます。

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>
 <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。

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

Select Policy

Default Policy (30 Daily)
▼

DP Volumes

Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value

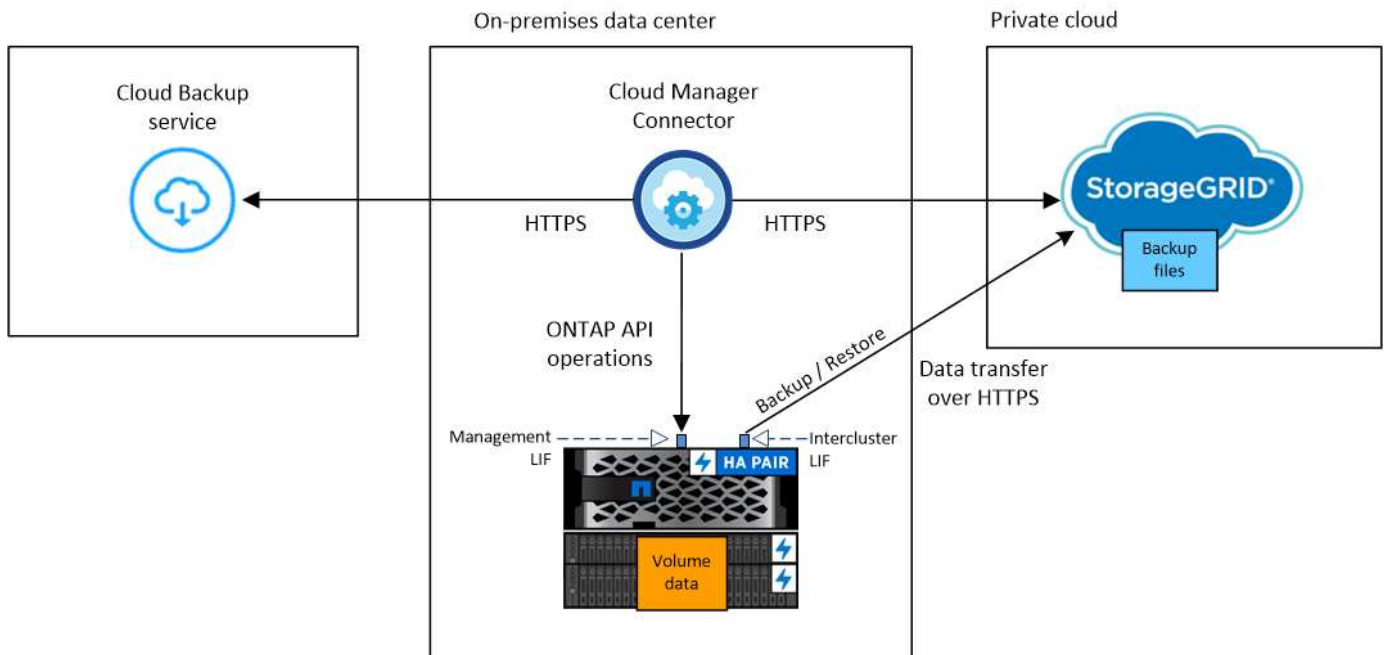
Select Volumes（ボリュームの選択）ページで、デフォルトのバックアップポリシーを使用してバックアップするボリュームを特定します。特定のボリュームに異なるバックアップポリシーを割り当てる場合は、あとから追加のポリシーを作成してボリュームに適用できます。

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。



この図では、StorageGRID の使用時には現在単一ファイルのリストアがサポートされていないため、クラウドリストアインスタンスは示されていません。

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
- 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 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、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"](#)
- ["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。
 - 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

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"]

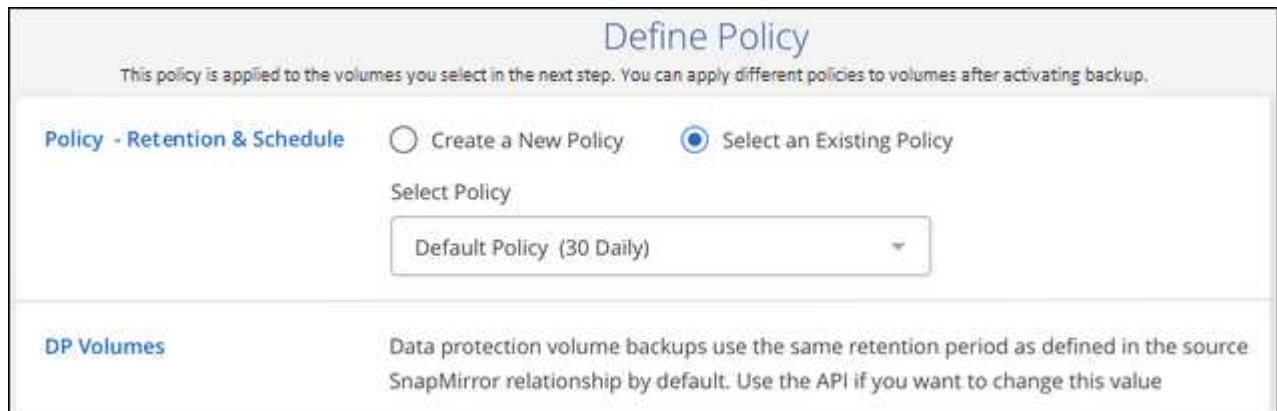
2. プロバイダとして * StorageGRID * を選択し、* Next * をクリックして、プロバイダの詳細を入力します。
 - a. StorageGRID サーバの FQDN と ONTAP が StorageGRID との HTTPS 通信に使用するポート。例：「3.eng.company.com:8082」
 - b. バックアップを格納するバケットへのアクセスに使用するアクセスキーとシークレットキー。
 - c. バックアップするボリュームが配置されている ONTAP クラスタ内の IPspace。この IPspace のクラスタ間 LIF には、アウトバウンドのインターネッ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

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。

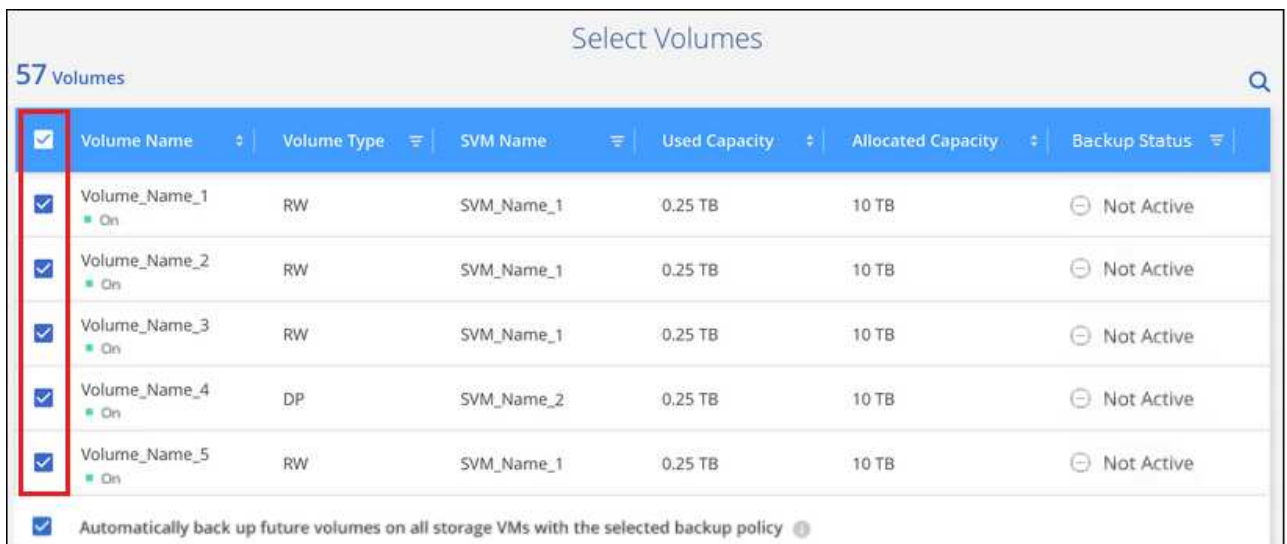


The screenshot shows the 'Define Policy' interface. At the top, it says 'This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.' Below this, there are two radio buttons: 'Create a New Policy' (unselected) and 'Select an Existing Policy' (selected). Under 'Select an Existing Policy', there is a dropdown menu labeled 'Select Policy' with 'Default Policy (30 Daily)' selected. At the bottom, there is a section titled 'DP Volumes' with the text: 'Data protection volume backups use the same retention period as defined in the source SnapMirror relationship by default. Use the API if you want to change this value'.

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）。



The screenshot shows the 'Select Volumes' page with a table of 57 volumes. The first column has a checkbox for selecting all volumes, which is checked. The table has columns: Volume Name, Volume Type, SVM Name, Used Capacity, Allocated Capacity, and Backup Status. The first five rows are highlighted with a red box, showing volumes Volume_Name_1 through Volume_Name_5. All have 'On' status and 'Not Active' backup status. At the bottom, there is a checkbox 'Automatically back up future volumes on all storage VMs with the selected backup policy' which is checked.

<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

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 ["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"](#) オンプレミスの ONTAP シ

システム上の新しいボリュームへの移動。

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。



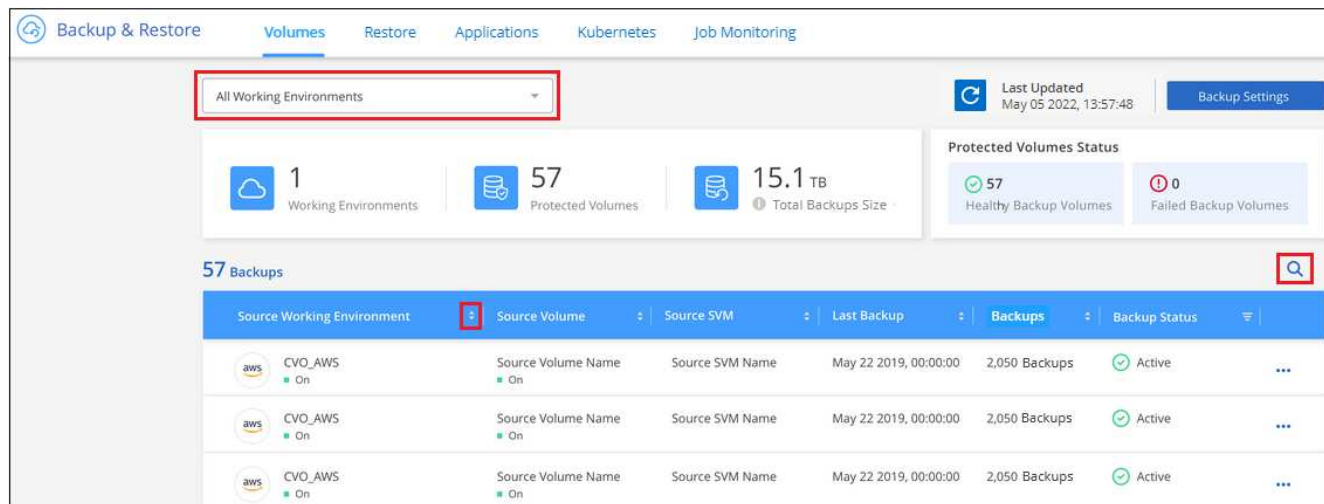
バックアップファイルをクラウドプロバイダ環境から直接管理したり変更したりしないでください。ファイルが破損し、サポートされていない構成になる可能性があります。

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。

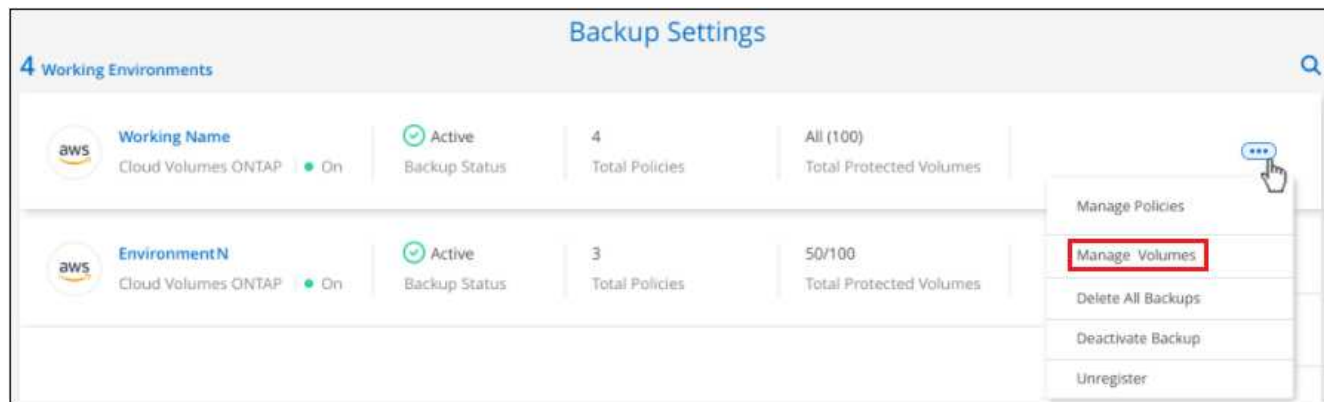
手順

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。



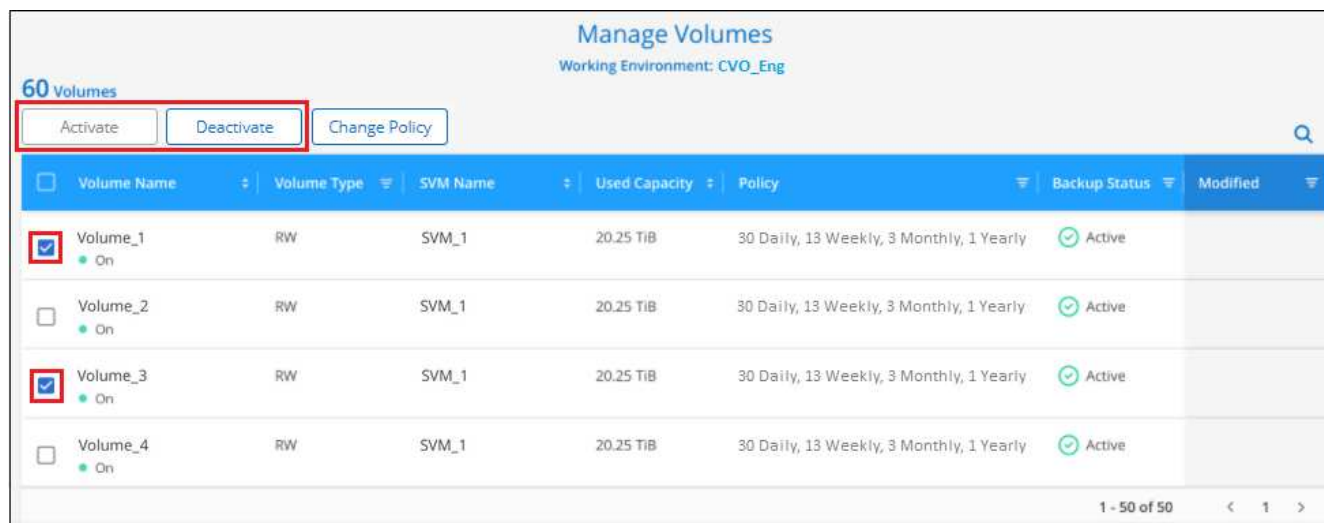
ボタンを示すスクリーンショット。"]

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

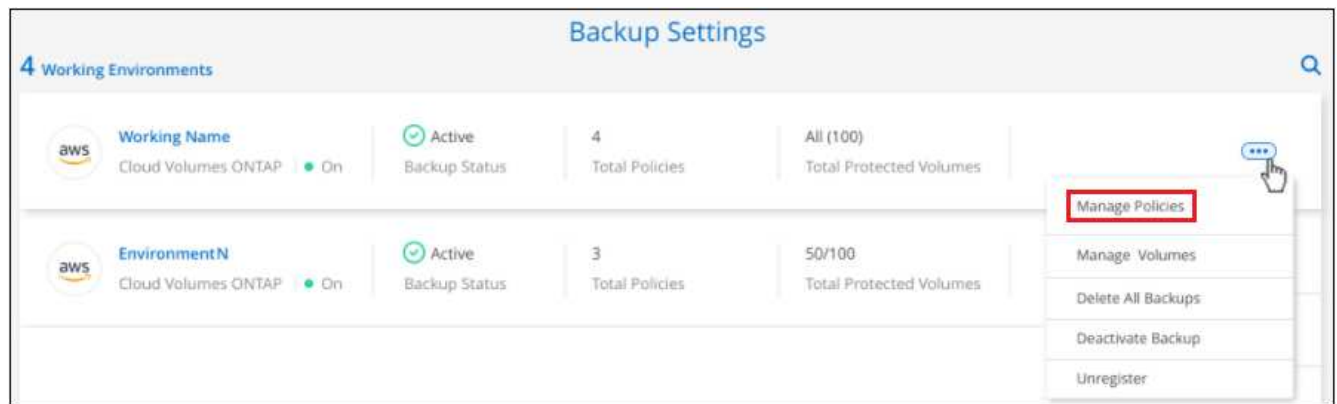
作業環境でボリュームに現在適用されているバックアップポリシーの属性を変更することができます。バックアップポリシーを変更すると、そのポリシーを使用している既存のすべてのボリュームが対象になります。

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 以降が実行されており、クラウドストレージに AWS または Azure 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のアーカイブストレージへの階層化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](#)". "AWS 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](#)".

アーカイブへのバックアップの階層化を停止した場合、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その階層に残ります。アーカイブされたバックアップ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。

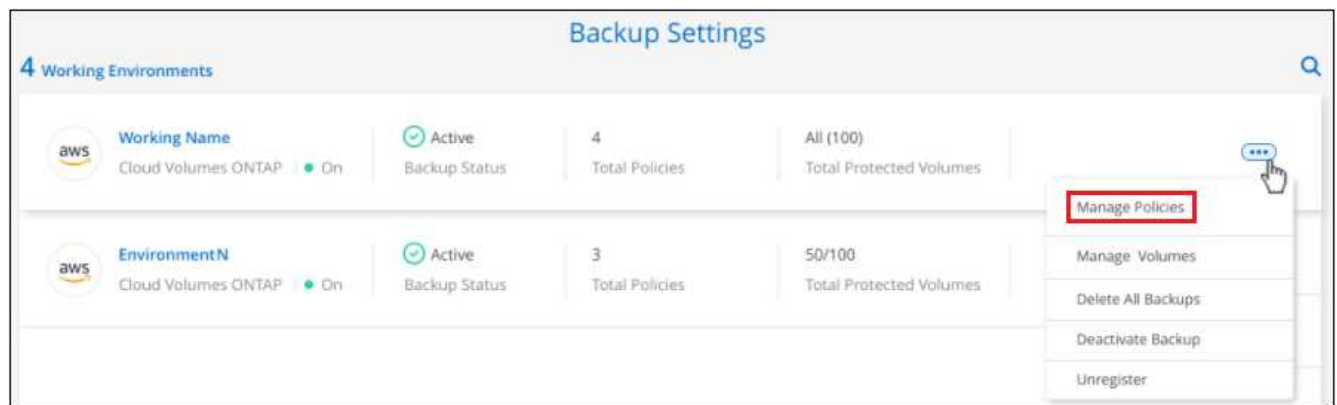
作業環境内の特定のボリュームに新しいバックアップポリシーを適用する場合は、最初にそのバックアップポリシーを作業環境に追加する必要があります。すると [その作業環境内のボリュームにポリシーを適用します](#)。

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。

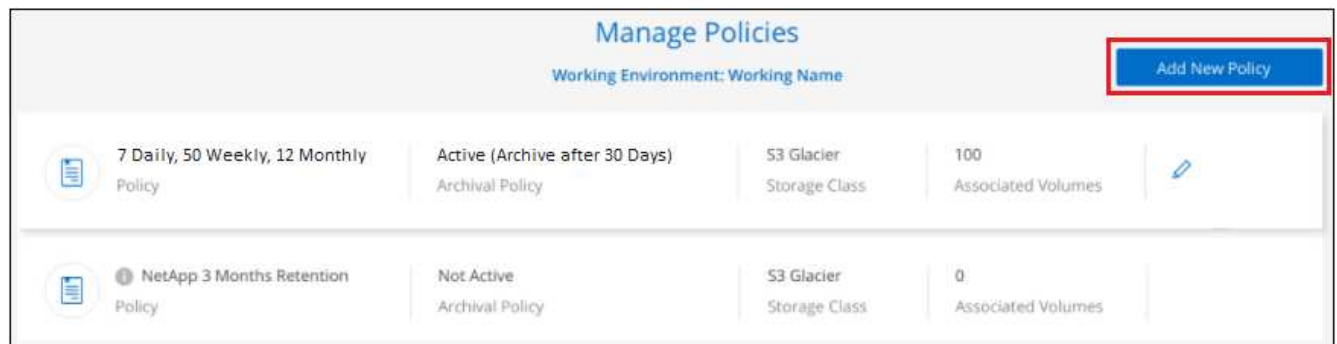


2. [Backup Settings] ページで、をクリックします ... アイコン"] 新しいポリシーを追加する作業環境で、[ポリシーの管理] を選択します。



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。

Add New Policy

Working Environment: Working Name

Policy - Retention & Schedule

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

クラスターで ONTAP 9.10.1 以降が実行されており、クラウドストレージに AWS または Azure 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のアーカイブストレージへの階層化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](#)"。"AWS 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](#)"。

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

Archival Policy

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.

☒ Tier Backups to Archival

Archive after (Days): Storage Class: S3 Glacier

S3 Glacier
 S3 Glacier Deep Archive

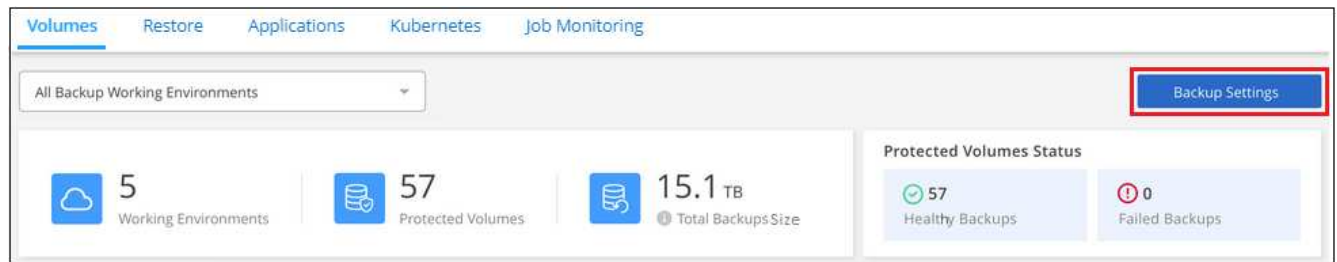
既存のボリュームに割り当てられているポリシーを変更する

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している必要があります。 [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](#)。

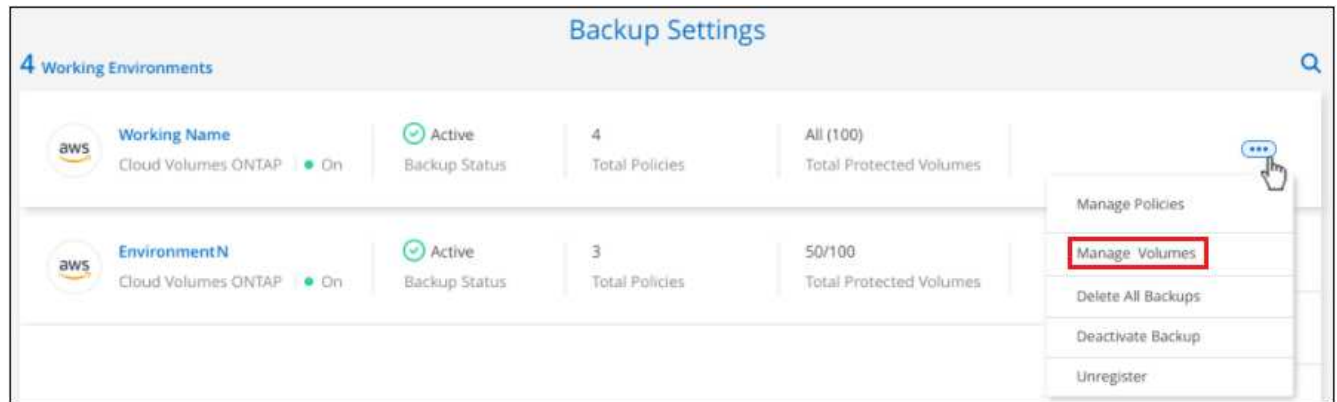
手順

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。



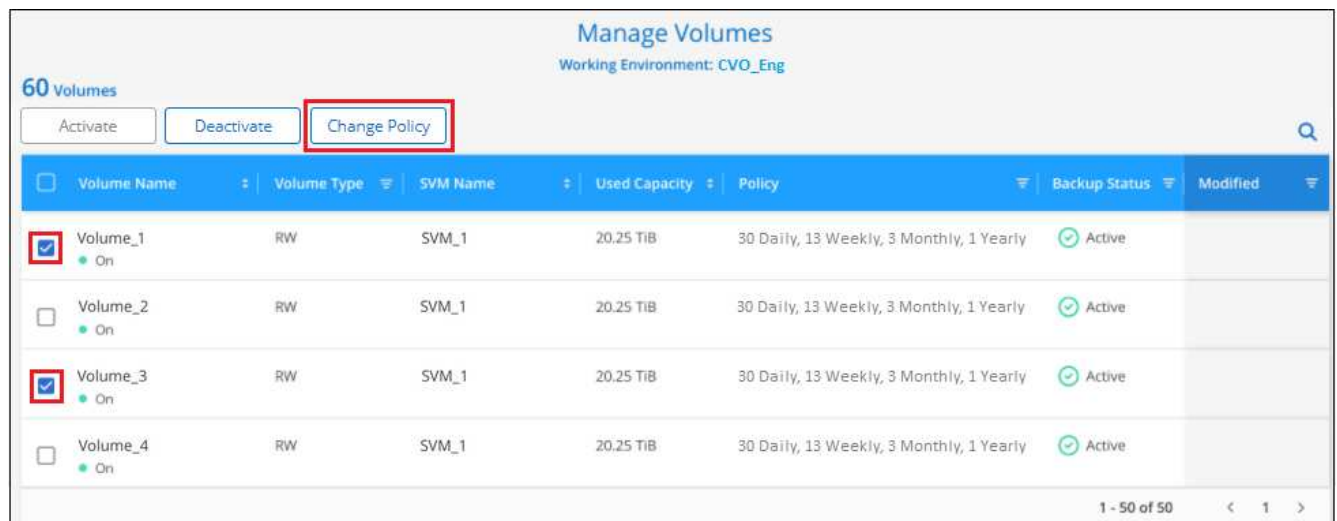
ボタンを示すスクリーンショット。"]

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。

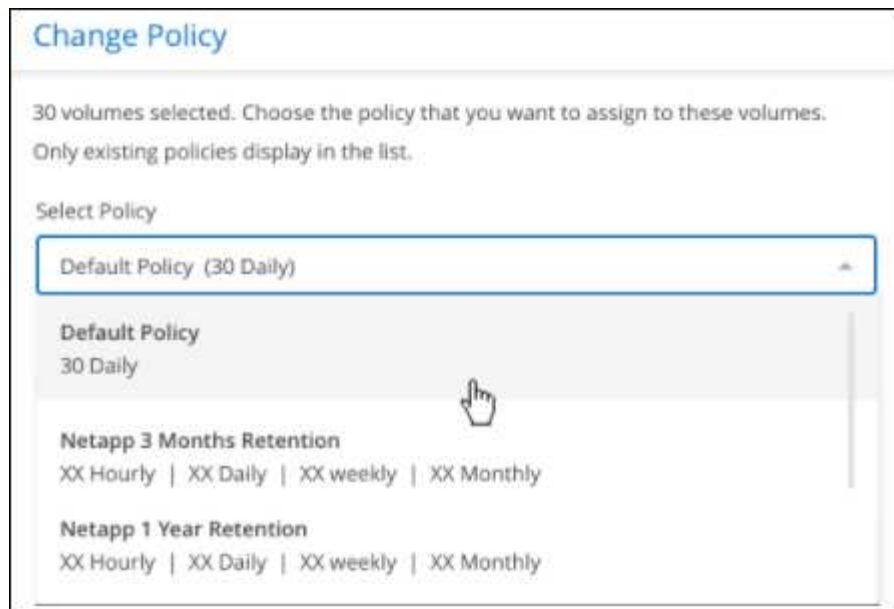


ページの [ボリュームの管理] ボタンを示すスクリーンショット。"]

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

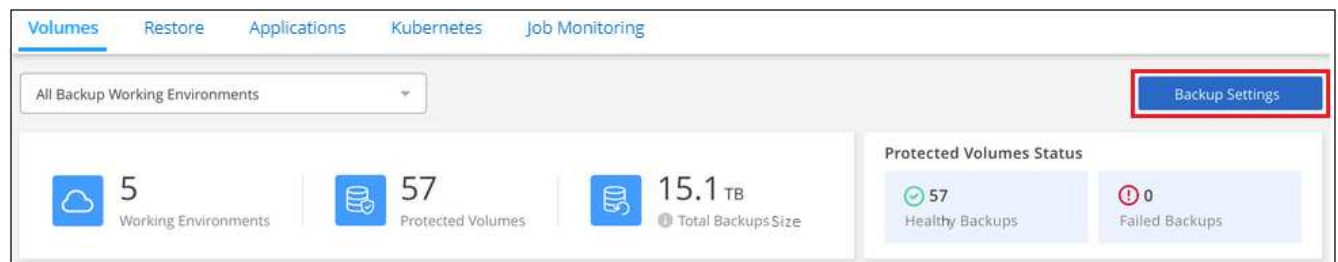
ONTAP クラスタでクラウドバックアップを初めてアクティブ化したときに、新しく作成したボリュームにバックアップポリシーを自動的に割り当てるオプションを選択していない場合は、あとで_Backup Settings_pageでこのオプションを選択できます。新しく作成したボリュームにバックアップポリシーを割り当てると、すべてのデータを確実に保護できます。

ボリュームに適用するポリシーがすでに存在している必要があります。 [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。

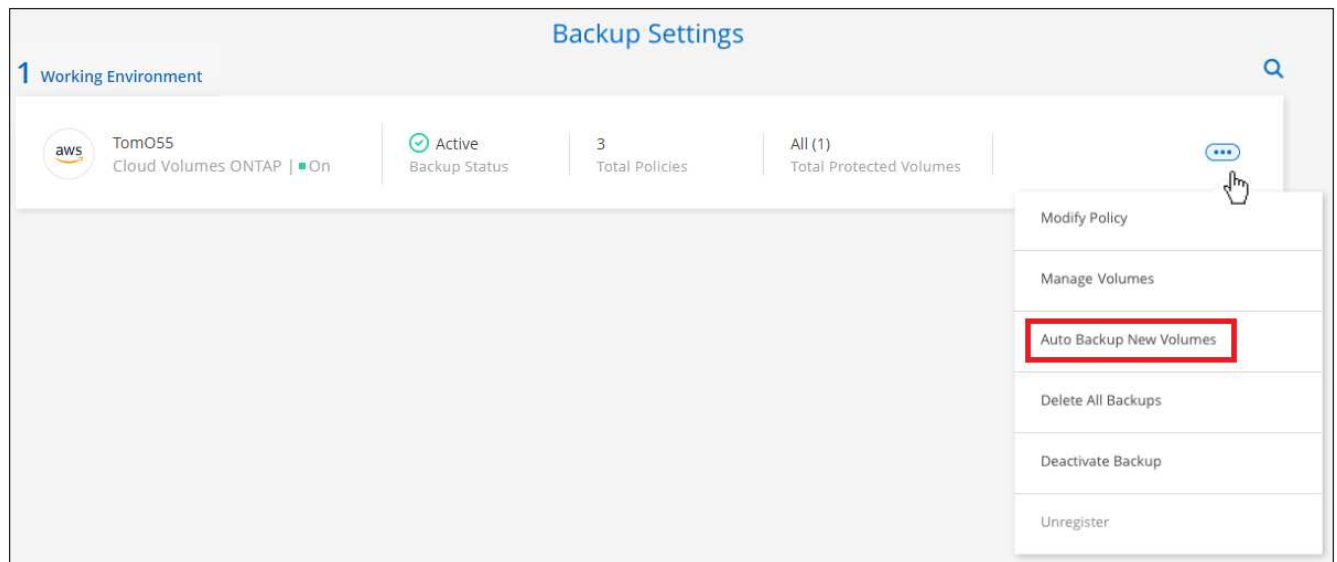
手順

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。

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。

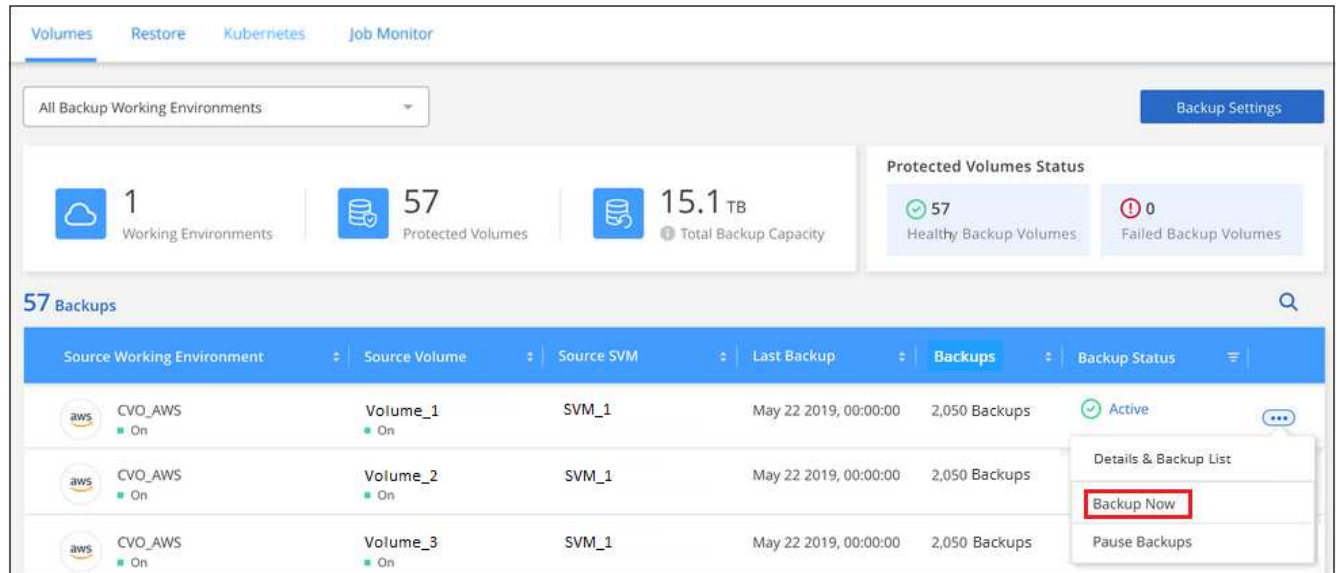
アドホックバックアップを作成する場合、ソースボリューム上にSnapshotが作成されることに注意してください。このSnapshotは通常のSnapshotスケジュールの一部ではないため、offのままになりません。バックアップの完了後に、このSnapshotをソースボリュームから手動で削除できます。これにより、このSnapshotに関連するブロックが解放されます。スナップショットの名前は'CBS-snapshot-adhoc-'で始まります "ONTAP CLIを使用してSnapshotを削除する方法を参照してください"。



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。

The screenshot shows the 'Volumes' tab in the Cloud Backup console. At the top, there are navigation links: Volumes, Restore, Kubernetes, and Job Monitor. Below them is a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The main dashboard displays three key metrics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. To the right, a 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a '57 Backups' section features a table with columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. The table lists three backups for 'CVO_AWS' on 'Volume_1', 'Volume_2', and 'Volume_3', all with 'SVM_1' and 'May 22 2019, 00:00:00' as the last backup. A context 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、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。

The screenshot shows the 'Details & Backup List' view for a specific 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 '2,050 Backups' section features a table with columns: Backup Name, Date, and Size. The table lists three backups: 'Backup_2020_Jan' (May 22 2019, 00:00:00, 19,001), 'Backup_2020_Mar' (May 22 2019, 00:00:00, 19,002), and 'Backup_2020_Apr' (May 22 2019, 00:00:00, 19,009). A search bar and 'Actions' button are also visible.

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。



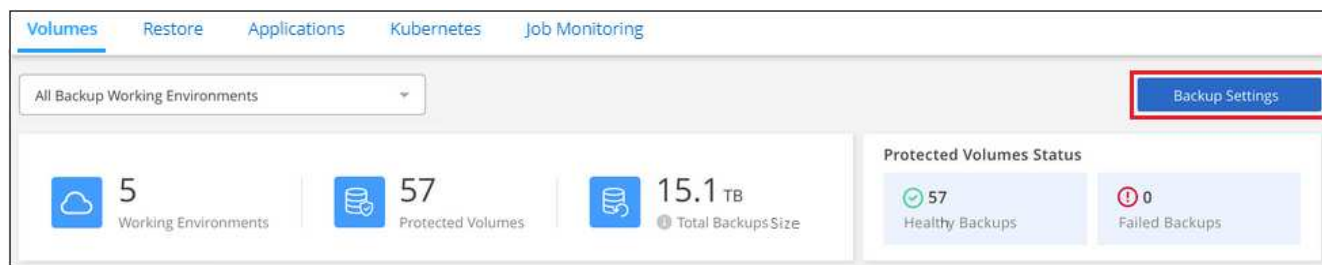
バックアップがある作業環境またはクラスタを削除する場合は、システムを削除する前に * バックアップを削除する必要があります。システムを削除しても、Cloud Backup はバックアップを自動的に削除しません。また、システムを削除した後でバックアップを削除するための UI で現在サポートされていません。残りのバックアップについては、引き続きオブジェクトストレージのコストが発生します。

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](#)。

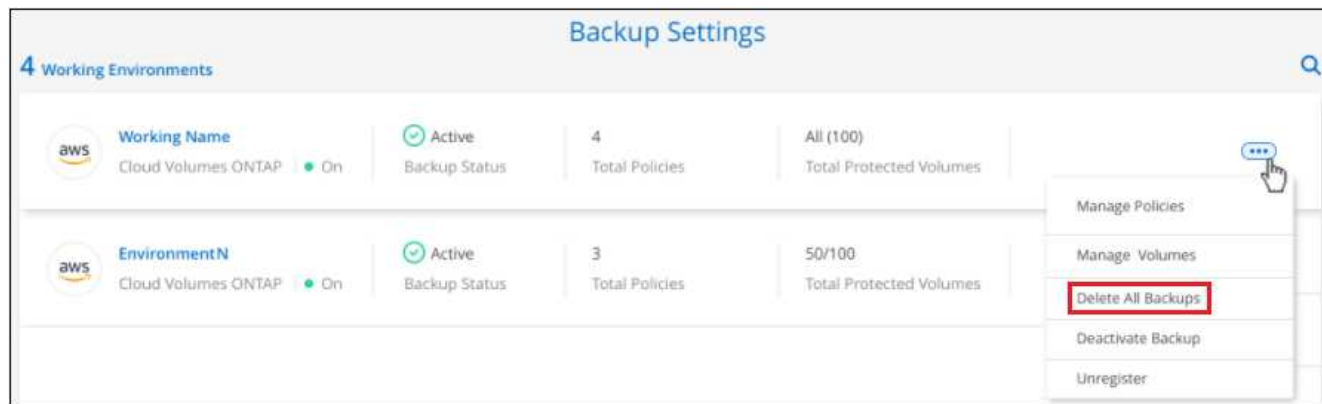
手順

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。

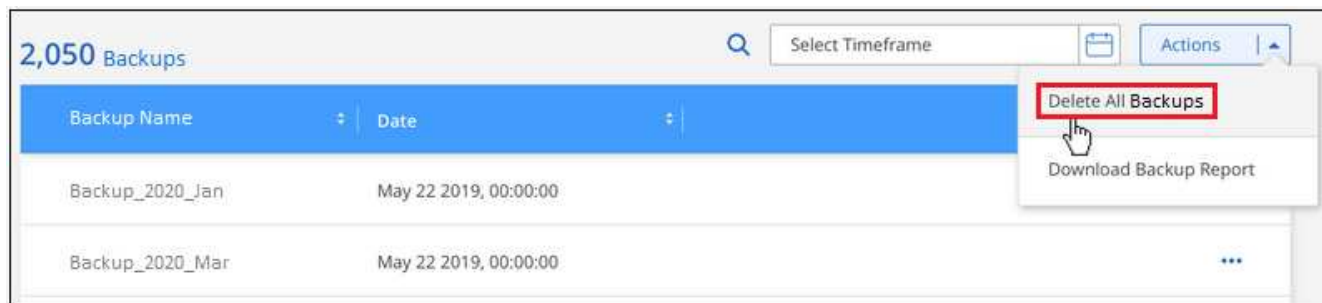
The screenshot shows the 'Volumes' tab in a backup management console. At the top, there are tabs for 'Volumes', 'Restore', 'Kubernetes', and 'Job Monitor'. Below these is a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The main area displays summary statistics: 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 section titled '57 Backups' contains a table with columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. The table lists three backup entries for 'CVO_AWS' working environment. A dropdown menu is open for the first entry, 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 & Backup List' view. It is divided into three main sections: 'Source', 'Destination', and 'Backup Information'. The 'Source' section includes fields for Working Environment, Type, Provider, Volume, and SVM. The 'Destination' section includes Cloud Provider, Region, Bucket, and Account ID. The 'Backup Information' section includes Relationship Status, Last Backup, Lag Duration, Backups, and Backup Policy. Below these sections is a table titled '2,050 Backups' with columns: Backup Name, Date, and Size. The table lists three backup entries: Backup_2020_Jan, Backup_2020_Mar, and Backup_2020_Apr.

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。



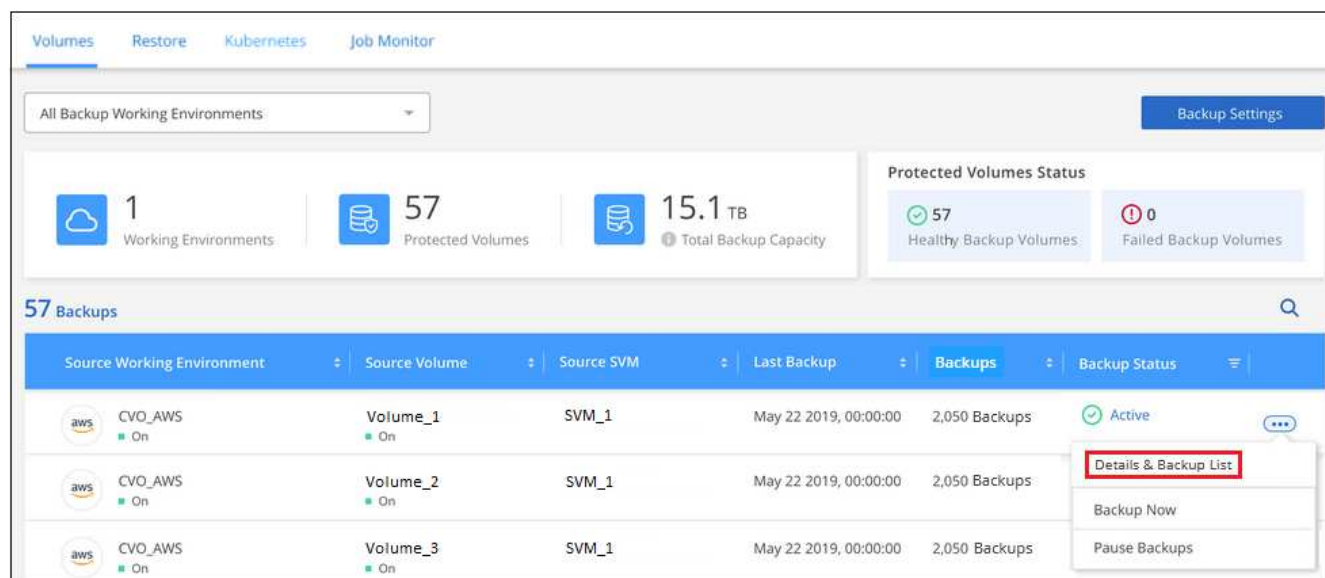
3. 確認ダイアログボックスで、ボリューム名を入力し、* 削除 * をクリックします。

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。

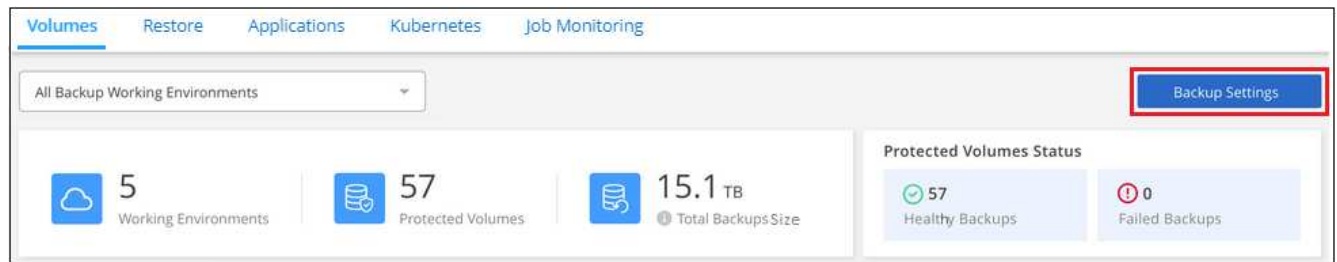
作業環境での Cloud Backup の無効化

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**。

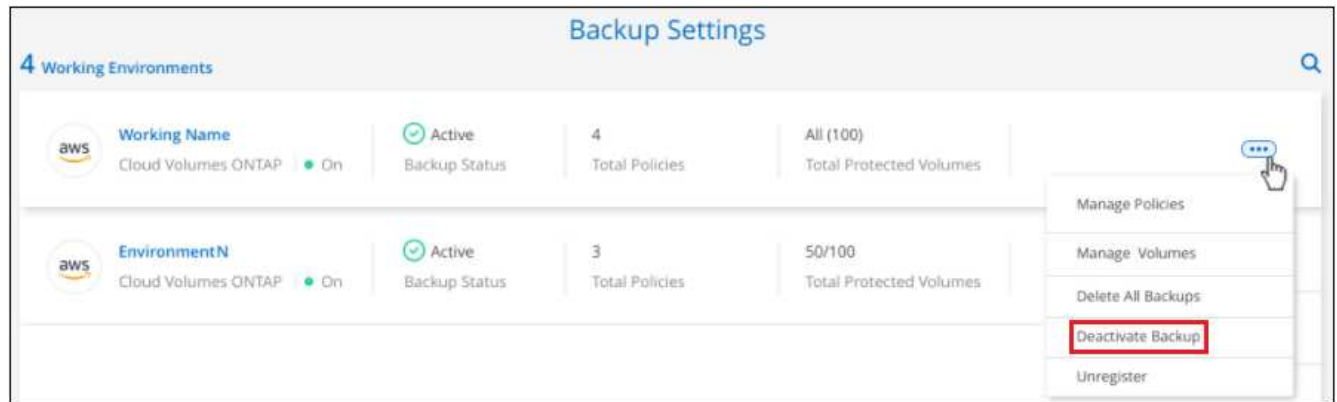
手順

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。

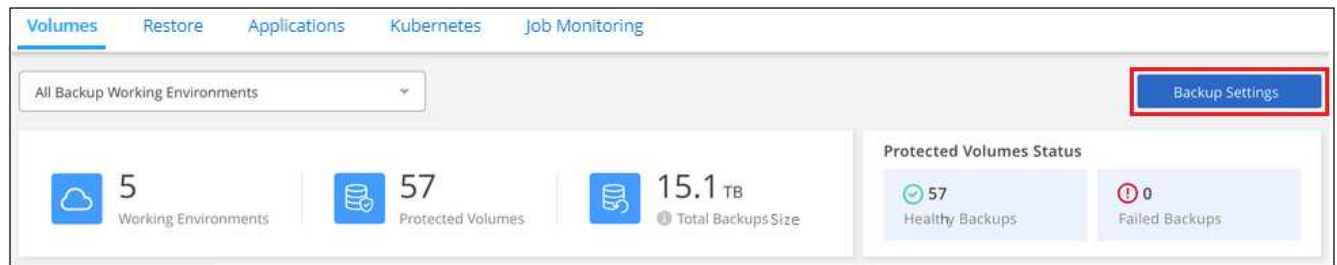
Cloud Backup の登録を解除する前に、次の手順をこの順序で実行する必要があります。

- 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。

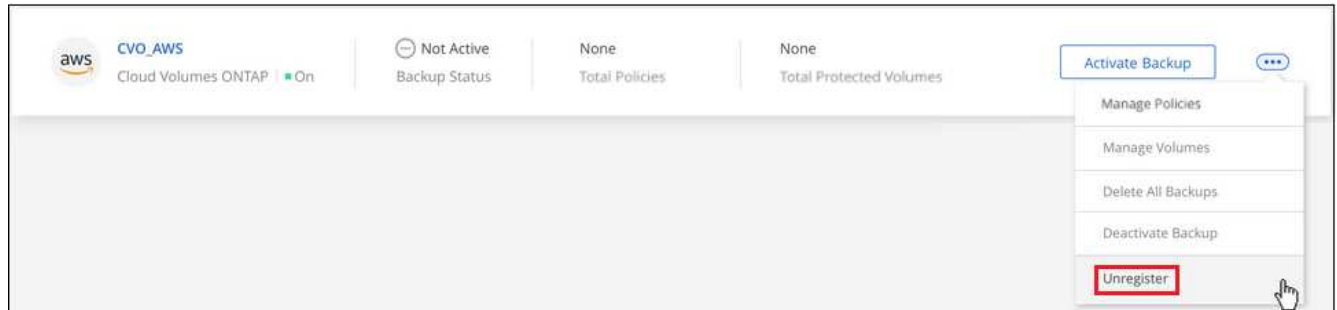
手順

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。

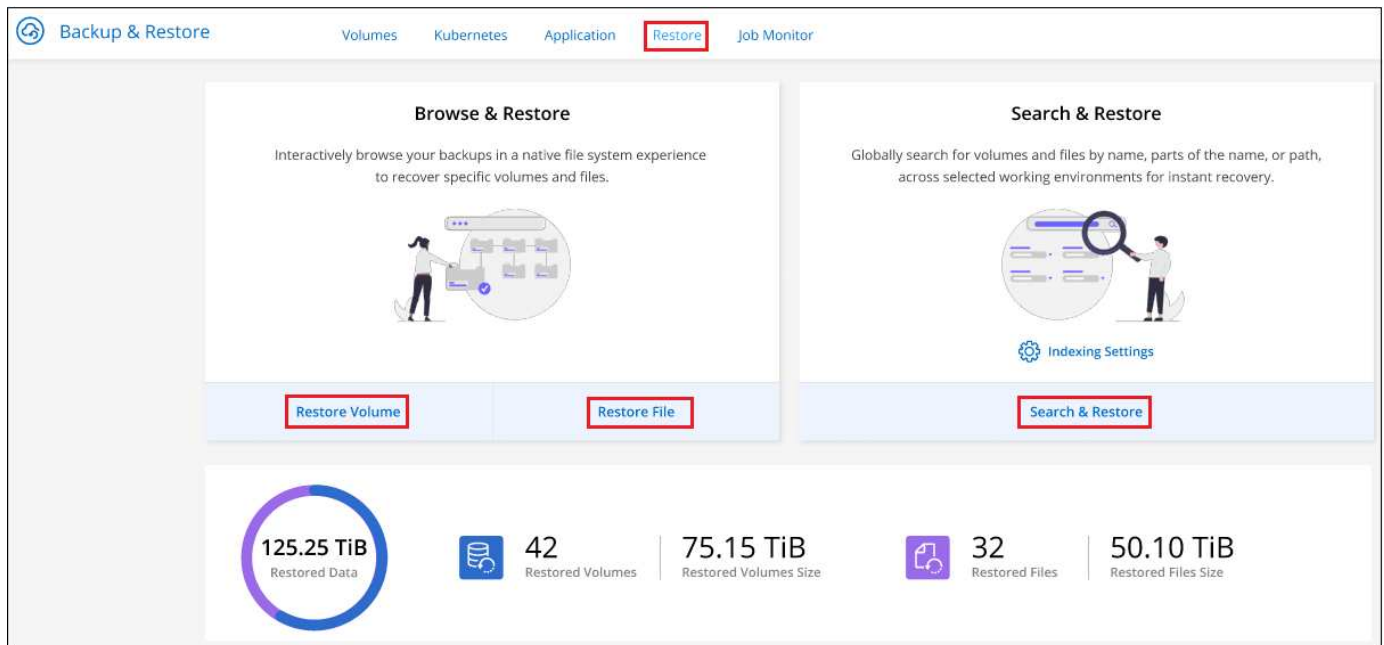
バックアップファイルから本番用システムにデータをリストアするには、有効な Cloud Backup ライセンスが必要です。

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。ファイルのリストアは、Amazon S3 と Azure Blob 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
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
ファイルのリストアには、Cloud Restore インスタンスが別途必要です	Cloud Restore インスタンスは不要です

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
個々のファイルのバックアップを参照するときに、Cloud Restore インスタンスに関連するコスト	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 以降の AWS および Azure で利用可能）にある場合、リストア処理にはより長い時間がかかり、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](#)". "[AWS 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 *	* ファイルの復元 *
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	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
Azure Blob の略	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入	オンプレミスの Azure ONTAP システムに Cloud Volumes ONTAP を導入
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	
NetApp StorageGRID	オンプレミスの ONTAP システム	

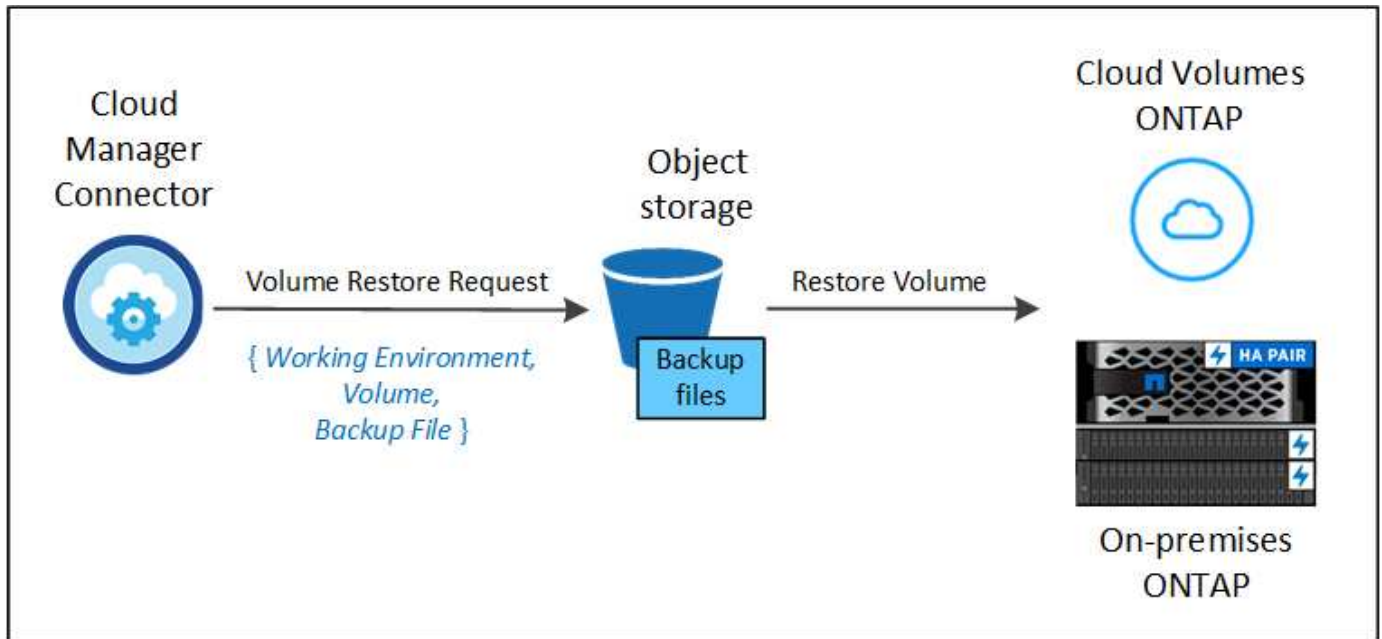
「オンプレミス ONTAP システム」とは、FAS、AFF、ONTAP Select の各システムを指します。



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

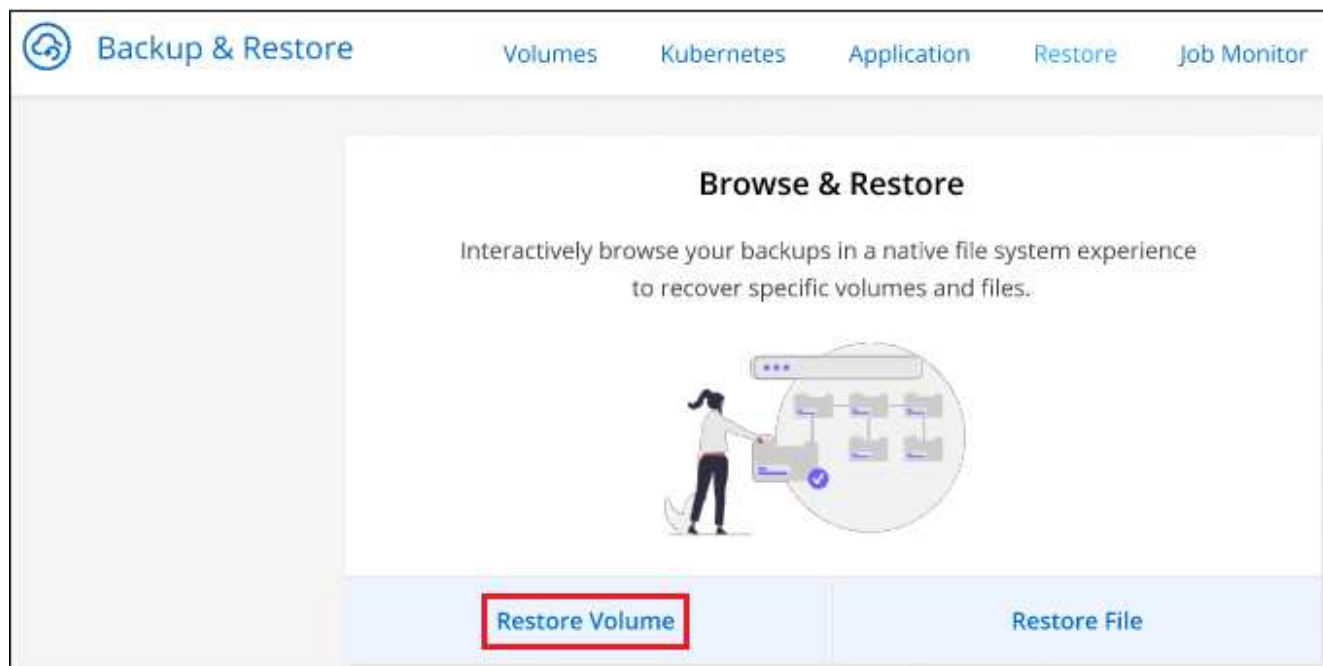
January 2022

 NetApp

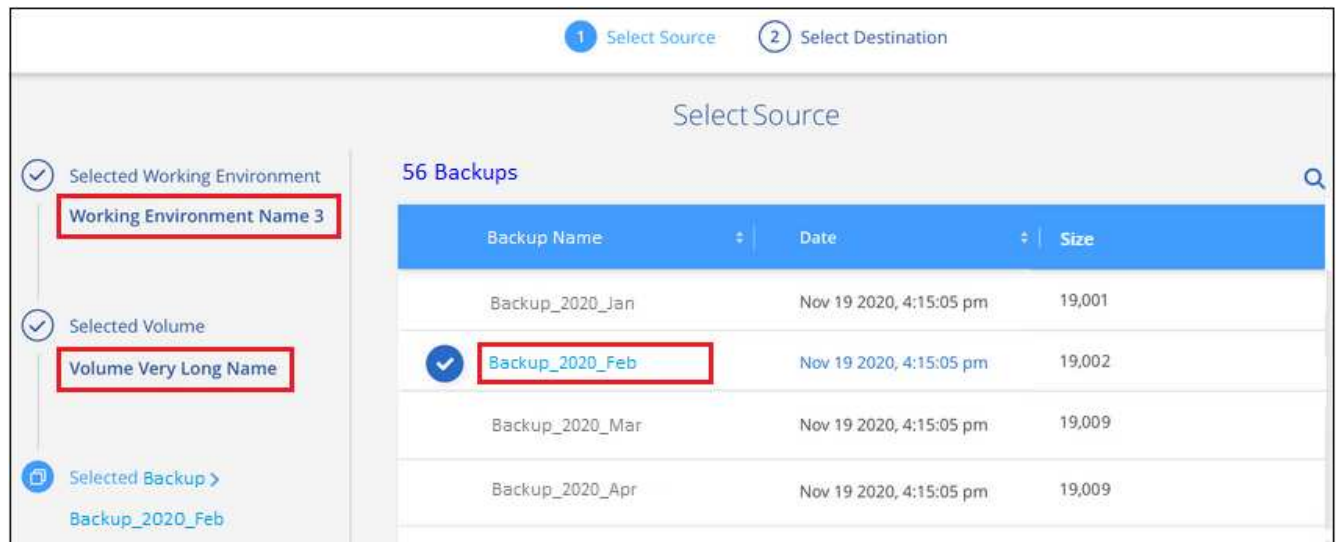


手順

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。

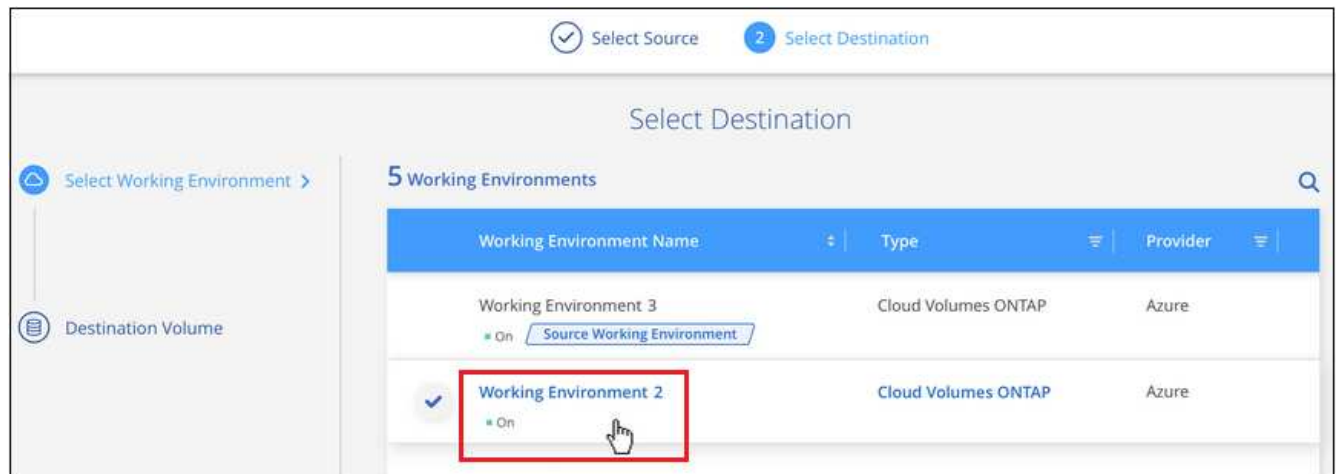


4. [ソースの選択] ページで 'リストアするボリュームのバックアップ・ファイルに移動しますリストア元の日付 / 時刻スタンプを含む * Working Environment *、* Volume *、および * Backup * ファイルを選択します。



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。

- Amazon S3 からリストアする場合、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、ONTAP クラスタに S3 バケットへのアクセスを許可するために作成したユーザのアクセスキーとシークレットキーを入力します。さらに、必要に応じて、セキュアなデータ転送を行うためのプライベート VPC エンドポイントを選択できます。
- 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。
- Google Cloud Storage からリストアする場合は、オブジェクトストレージ、バックアップが格納されているリージョン、およびデスティネーションボリュームが配置される ONTAP クラスタ内の IPspace にアクセスするために、Google Cloud Project とアクセスキーとシークレットキーを選択します。
- StorageGRID からリストアする場合は、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。

- 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。

Select Destination							
<div>✓ Selected Working Environment Working Environment Name 2</div> <div>📁 Destination Volume > General_restore</div>	<div>Message: A new volume will be created in the working environment based on the backup you selected</div> <div>Volume Name: General_restore</div> <div>Storage VM: svm1</div> <div>Restore Priority: Low</div> <div>Volume Information:<table><tr><td>Volume Size:</td><td>50.00 GB</td></tr><tr><td>Backup Policy:</td><td>CloudBackupService</td></tr><tr><td>Protocol:</td><td>NFS</td></tr></table></div>	Volume Size:	50.00 GB	Backup Policy:	CloudBackupService	Protocol:	NFS
Volume Size:	50.00 GB						
Backup Policy:	CloudBackupService						
Protocol:	NFS						

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](#)。"AWS 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](#)。"

- 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。

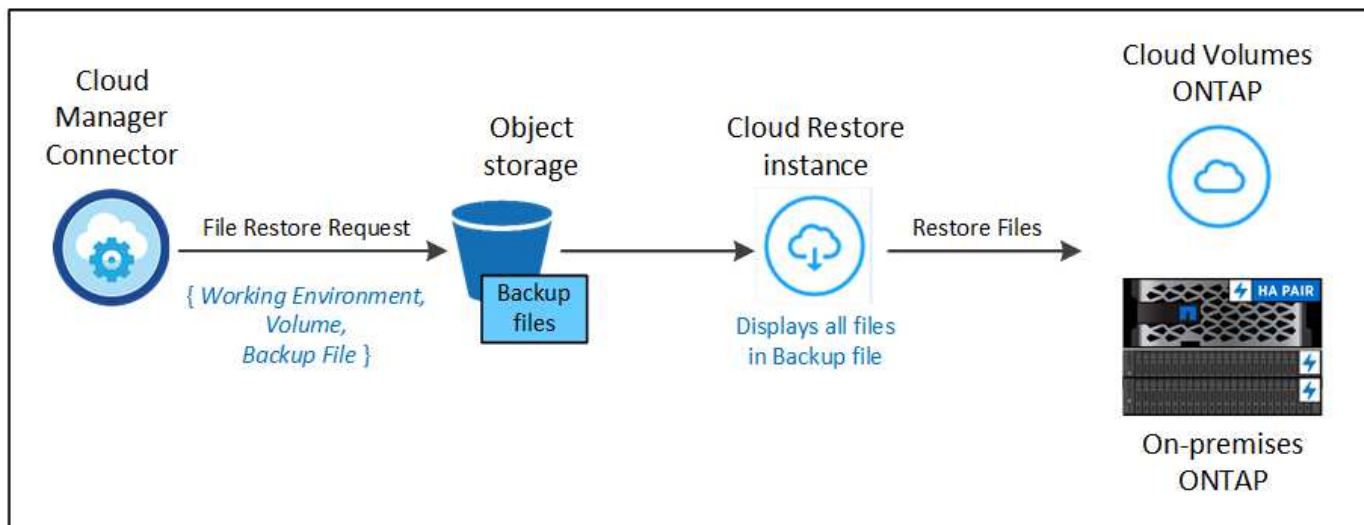
前提条件

- 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。
- 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場合は、別のリストアインスタンス / 仮想マシンを使用します。を参照してください ["ファイルリストア処理用に導入されるインスタンスのタイプ"](#) また、環境の準備が整っていることを確認します。
- Amazon S3 のバックアップからファイルをリストアするには、Cloud Manager に権限を付与するユーザーロールに特定の AWS EC2 権限を追加する必要があります。また、特定のエンドポイントへのアウトバウンドインターネットアクセスを許可する必要があります。 ["構成ファイルをリストアする準備ができていることを確認します"](#)。
- AWS のクロスアカウントリストアを実行するには、AWS コンソールで手動の操作が必要です。AWS のトピックを参照してください ["クロスアカウントバケットの権限を付与しています"](#) を参照してください。
- Azure Blob でのバックアップからファイルのリストアでは、特定のエンドポイントへのアウトバウンドインターネットアクセスが可能であることが必要です。 ["構成ファイルをリストアする準備ができていることを確認します"](#)。

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. Restore インスタンスが起動し、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。
 - 注：リストアインスタンスは、ファイルを初めてリストアするときにクラウドプロバイダの環境に導入されます。
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、非アクティブ状態が続くと Restore インスタンスがシャットダウンされてコストが削減されます。

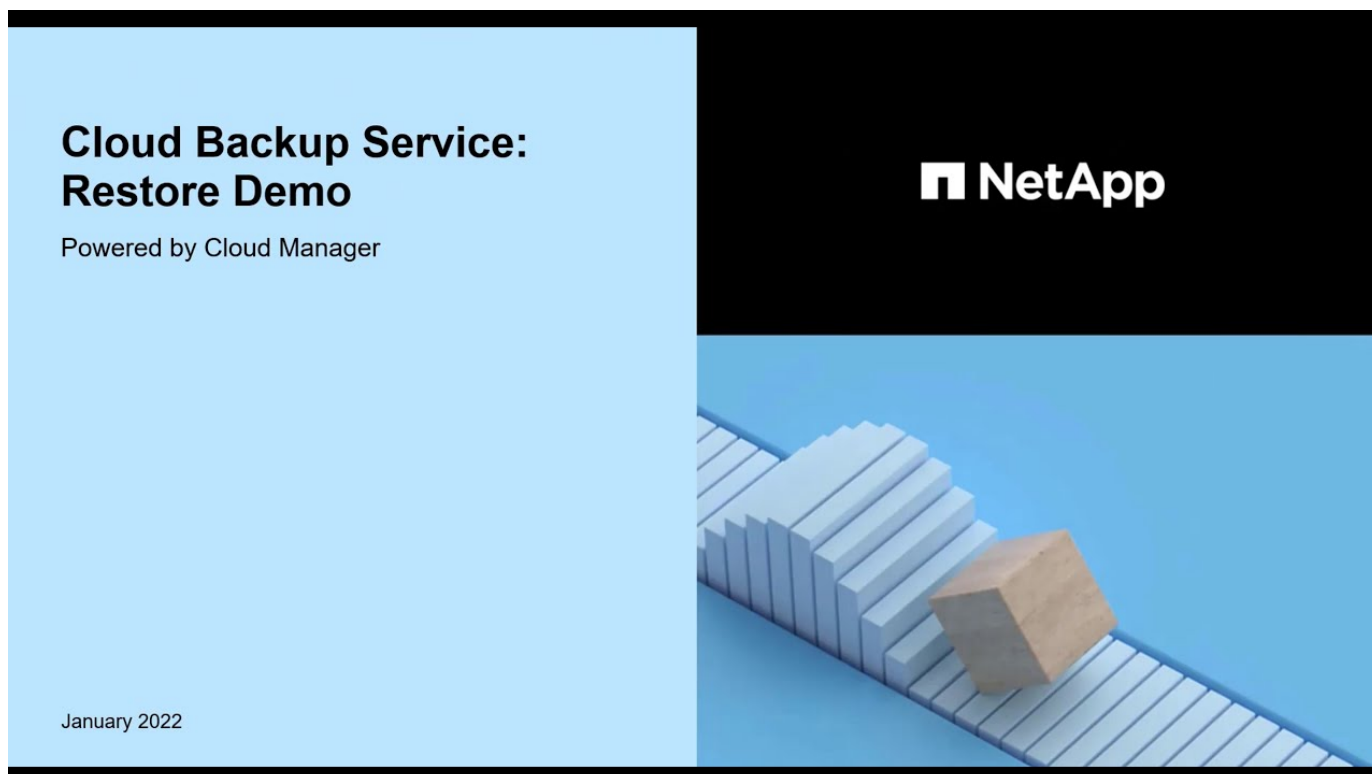


このように、ファイルのリストアを実行するには、作業環境名、ボリューム名、バックアップファイルの日付、およびファイル名を把握しておく必要があります。

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。

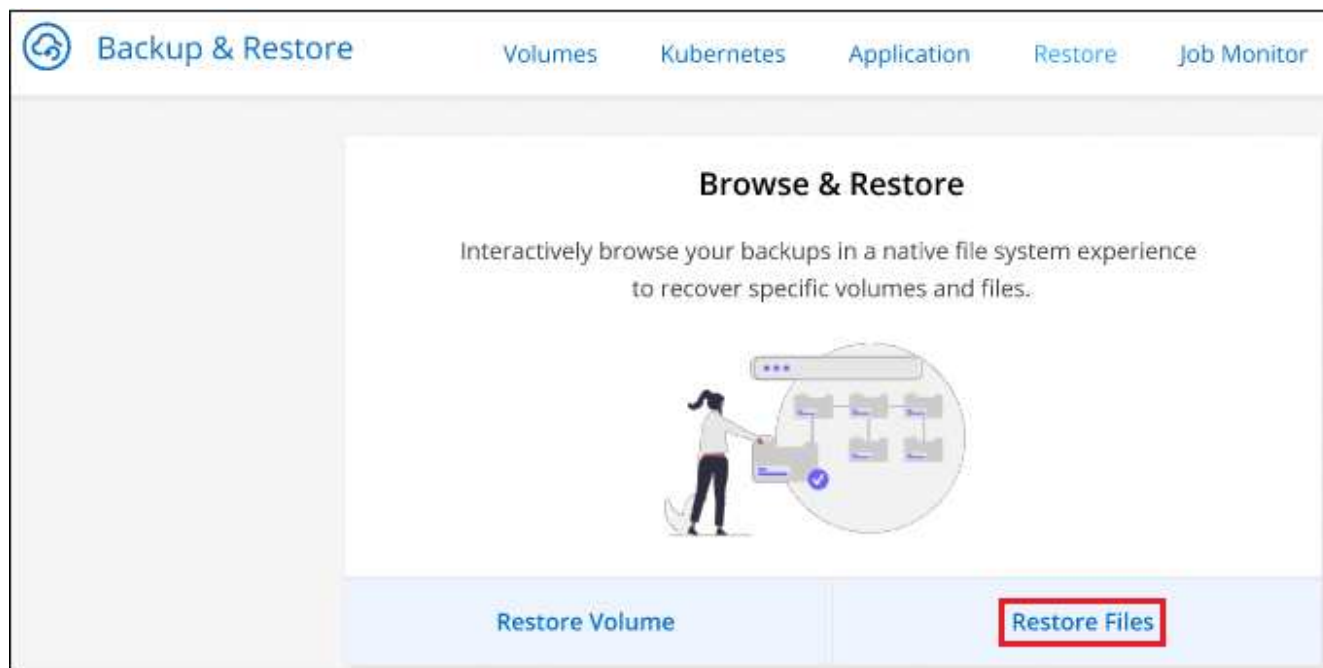
次のビデオでは、1つのファイルをリストアする手順を簡単に紹介します。



手順

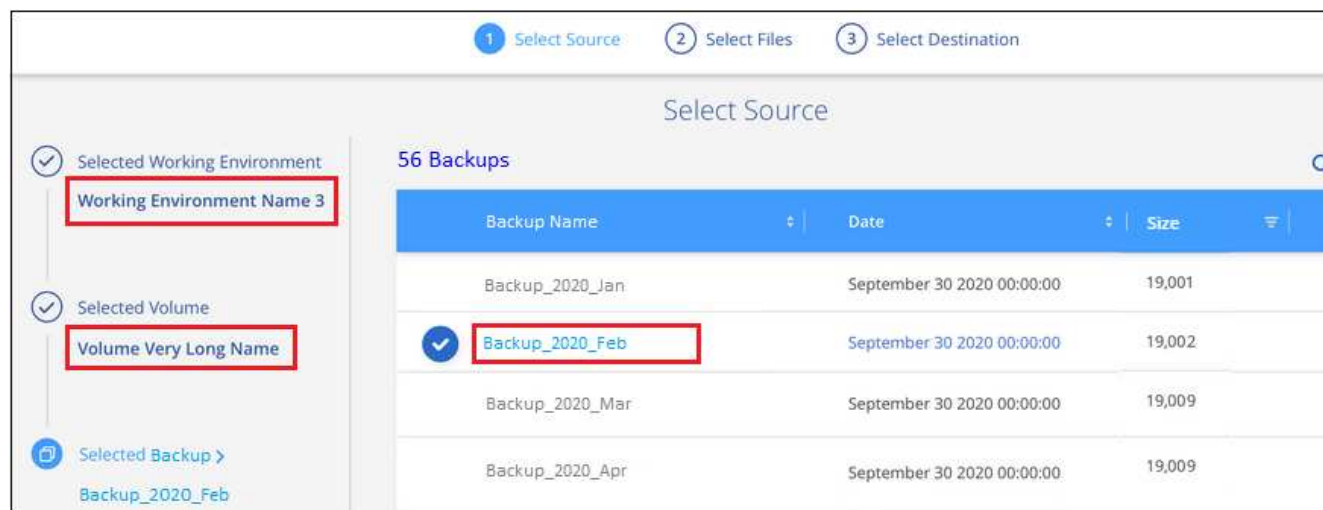
1. Backup & Restore * サービスを選択します。

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。



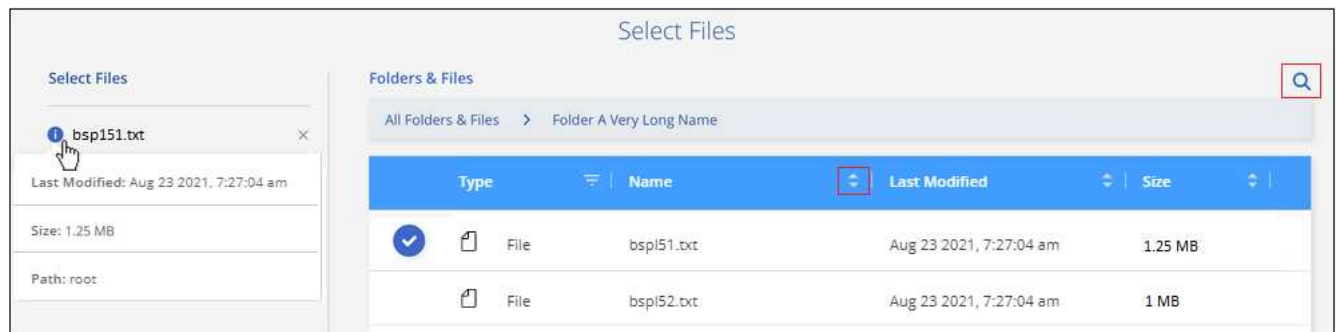
ボタンを選択するスクリーンショット。"]

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、リストアインスタンスが開始されます。数分後に、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。

。注：リストアインスタンスは、ファイルを初めてリストアするときにクラウドプロバイダの環境に導入されるため、初回のリストアには数分かかることがあります。

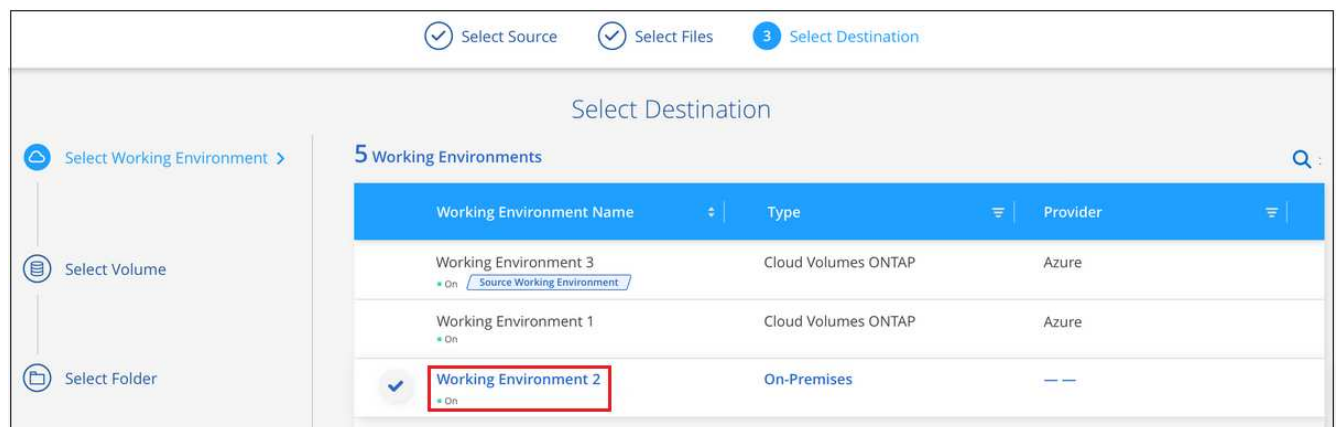


6. ファイルの選択 ページで、復元するファイルを選択し、* 続行 * をクリックします。ファイルの検索を支援するために、次の手順を実行します。

- 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。

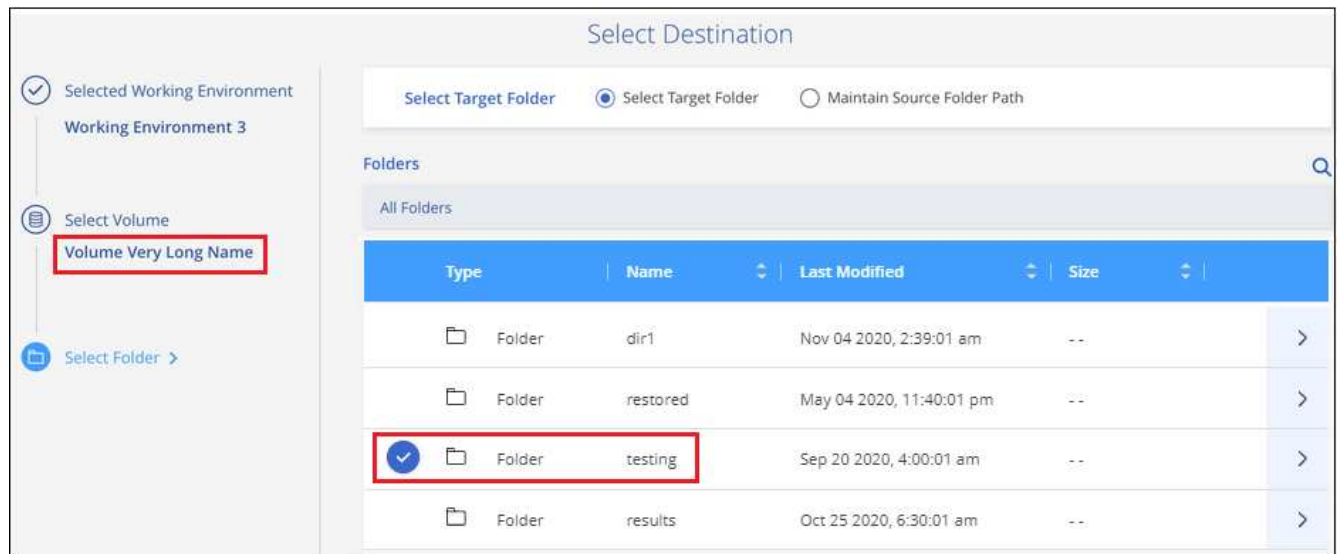
7. 保存先の選択ページで、ファイルを復元する * 作業環境 * を選択します。



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。

- Amazon S3 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 クラスタの IPspace と、オブジェクトストレージへのアクセスに必要な AWS Access Key および Secret Key を入力します。
- 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。

8. 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している必要があります。フォルダは作成されません。

9. 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。

リストア・インスタンスは、アクティブなときにのみコストが発生するように、一定の非アクティブ期間後にシャットダウンされます。

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 以降の AWS 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。

"AWS 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](#)。"

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。



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 *	* ファイルの復元 *
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	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
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

「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。
- AWS の要件：
 - Cloud Manager に権限を付与するユーザロールに、Amazon Athena 、 AWS Glue 、 および AWS S3 の特定の権限を追加する必要があります。 ["すべての権限が正しく設定されていることを確認します"](#)。

以前に設定したコネクタで Cloud Backup をすでに使用している場合は、ここで Athena 権限と Glue 権限を Cloud Manager ユーザロールに追加する必要があります。これらは新しい機能で、検索とリストアに必要です。
- Google Cloud の要件：
 - 特定の Google BigQuery 権限は、Cloud Manager に権限を付与するユーザーロールに追加する必要があります。 ["すべての権限が正しく設定されていることを確認します"](#)。

以前に設定したコネクタで Cloud Backup をすでに使用している場合は、ここで BigQuery 権限を Cloud Manager ユーザロールに追加する必要があります。これらは新しい機能で、検索とリストアに必要です。

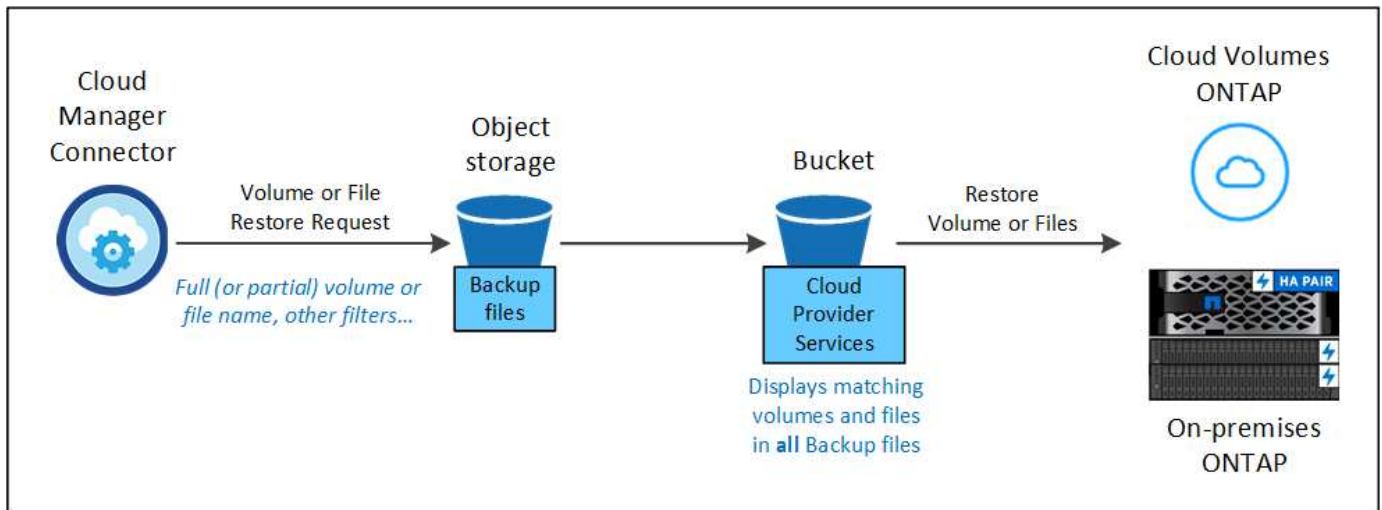
検索とリストアのプロセス

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。

- AWSに格納されたバックアップについては、新しいS3バケットとがプロビジョニングされます ["Amazon Athena インタラクティブクエリーサービス"](#) および ["AWS グルーサーバレスデータ統合サービス"](#)。
- Google Cloudに保存されているバックアップの場合、新しいバケットとがプロビジョニングされます ["Google Cloud BigQueryサービス"](#) アカウント/プロジェクトレベルでプロビジョニングされます。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。

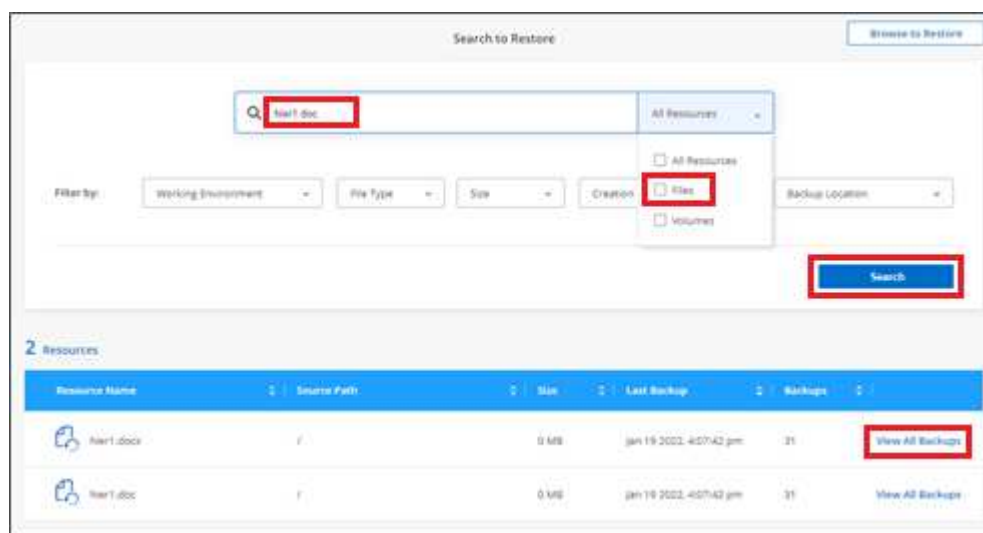
手順

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。



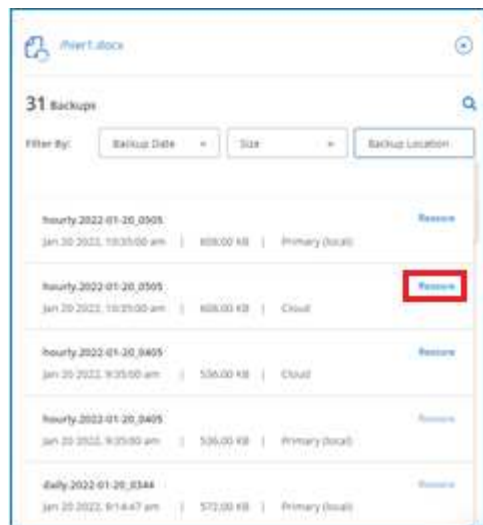
ボタンを選択するスクリーンショット。"]

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。



7. 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。

8. 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。

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。