



ONTAPボリュームのワークロードを保護する

NetApp Backup and Recovery

NetApp
February 27, 2026

目次

ONTAPボリュームのワークロードを保護する	1
NetApp Backup and Recoveryを使用してONTAPボリューム データを保護します	1
機能	2
バックアップおよび復元操作でサポートされているシステム	3
サポートされているボリューム	4
料金	4
ライセンス	5
NetApp Backup and Recoveryの仕組み	7
FabricPool階層化ポリシーの考慮事項	10
NetApp Backup and Recoveryで保護の旅を計画する	10
どの保護機能を使用するか	11
どのバックアップアーキテクチャを使用するか	12
スナップショット、レプリケーション、バックアップのデフォルトポリシーを使用しますか？	14
ポリシーはどこに保存されますか？	15
独自のオブジェクトストレージコンテナを作成しますか？	16
どのコンソールエージェント展開モードを使用していますか	17
NetApp Backup and Recoveryを使用してONTAPボリュームのバックアップポリシーを管理する	18
システムのポリシーを表示する	19
ポリシーを作成	19
ポリシーを編集する	21
ポリシーを削除する	21
詳細情報の参照	22
NetApp Backup and Recoveryのオブジェクトへのバックアップ ポリシー オプション	22
バックアップスケジュールオプション	22
DataLockとランサムウェア保護オプション	23
アーカイブ保存オプション	30
NetApp Backup and Recoveryの詳細設定でオブジェクト ストレージへのバックアップ オプションを管理する	31
クラスターレベルのバックアップ設定を表示する	31
オブジェクトストレージにバックアップをアップロードするために利用できるネットワーク帯域幅を 変更する	32
履歴スナップショットをバックアップファイルとしてエクスポートするかどうかを変更する	32
「年次」スナップショットをソースシステムから削除するかどうかを変更する	33
ランサムウェアスキャンを有効または無効にする	33
NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Amazon S3 にバックアップする	34
構成のサポートを確認する	34
ライセンス要件を確認する	35
コンソールエージェントを準備する	36

ボリュームを複製するためのONTAPネットワーク要件を確認する	39
Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする	39
ONTAPボリューム上のバックアップをアクティブ化する	40
NetApp Backup and Recoveryを使用して、Cloud Volumes ONTAPデータを Azure Blob	45
ストレージにバックアップします。	
構成のサポートを確認する	45
ライセンス要件を確認する	46
コンソールエージェントを準備する	46
ボリュームを複製するためのONTAPネットワーク要件を確認する	49
Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする	49
ONTAPボリューム上のバックアップをアクティブ化する	50
次の手順	55
NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Google Cloud Storage	55
にバックアップする	
構成のサポートを確認する	55
ライセンス要件を確認する	56
コンソールエージェントを準備する	57
ボリュームを複製するためのONTAPネットワーク要件を確認する	58
Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする	59
Google Cloud Storage をバックアップ先として準備する	60
ONTAPボリューム上のバックアップをアクティブ化する	62
次の手順	66
NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Amazon S3	66
にバックアップする	
接続方法を特定する	67
コンソールエージェントを準備する	68
ライセンス要件を確認する	69
ONTAPクラスタを準備する	69
Amazon S3をバックアップターゲットとして準備する	71
ONTAPボリューム上のバックアップをアクティブ化する	76
NetApp Backup and Recoveryを使用してオンプレミスの ONTAPデータを Azure Blob	80
ストレージにバックアップする	
接続方法を特定する	81
コンソールエージェントを準備する	82
ライセンス要件を確認する	85
ONTAPクラスタを準備する	85
Azure Blob をバックアップ先として準備する	87
ONTAPボリューム上のバックアップをアクティブ化する	87
NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Google Cloud Storage	
にバックアップする	92
接続方法を特定する	92
コンソールエージェントを準備する	94

コンソールエージェントのネットワークを準備する	95
ライセンス要件を確認する	96
ONTAPクラスタを準備する	96
Google Cloud Storage をバックアップ先として準備する	98
ONTAPボリューム上のバックアップをアクティブ化する	100
NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータをONTAP S3 にバックアップする	104
接続方法を特定する	105
コンソールエージェントを準備する	107
ライセンス要件を確認する	107
ONTAPクラスタを準備する	108
ONTAP S3をバックアップターゲットとして準備する	110
ONTAPボリューム上のバックアップをアクティブ化する	110
NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを StorageGRIDにバックアップします。	115
接続方法を特定する	115
コンソールエージェントを準備する	116
ライセンス要件を確認する	117
ONTAPクラスタを準備する	117
StorageGRIDをバックアップターゲットとして準備する	119
ONTAPボリューム上のバックアップをアクティブ化する	121
NetApp Backup and RecoveryでSnapMirrorを使用してボリュームを Cloud Resync に移行する	125
NetApp Backup and RecoverySnapMirrorからクラウド再同期への仕組み	126
手順に関する注意事項	128
SnapMirrorを使用してボリュームをCloud Resyncに移行する方法	128
ダークサイトでのNetApp Backup and Recovery構成データの復元	131
NetApp Backup and Recoveryデータを新しいコンソール エージェントに復元します	131
NetApp Backup and Recoveryを使用してONTAPシステムのバックアップを管理します	136
システム内のボリュームのバックアップステータスを表示します	137
システム内の追加ボリュームでバックアップを有効にする	137
既存のボリュームに割り当てられたバックアップ設定を変更する	138
いつでも手動でボリュームバックアップを作成	139
各ボリュームのバックアップのリストを表示する	140
オブジェクトストレージ内のボリュームバックアップでランサムウェアスキャンを実行する	140
ソースボリュームとのレプリケーション関係を管理する	140
既存のクラウドへのバックアップ ポリシーを編集する	141
新しいクラウドへのバックアップポリシーを追加する	142
バックアップの削除	143
ボリュームバックアップ関係を削除する	145
システムのNetApp Backup and Recoveryを非アクティブ化する	146
システムのNetApp Backup and Recoveryの登録を解除する	146

ONTAPバックアップからの復元	147
NetApp Backup and Recoveryを使用してバックアップファイルからONTAPデータを復元する	147
検索と復元を使用してONTAPバックアップから復元する	148
参照と復元を使用してONTAPデータを復元する	157

ONTAPボリュームのワークロードを保護する

NetApp Backup and Recoveryを使用してONTAPボリュームデータを保護します

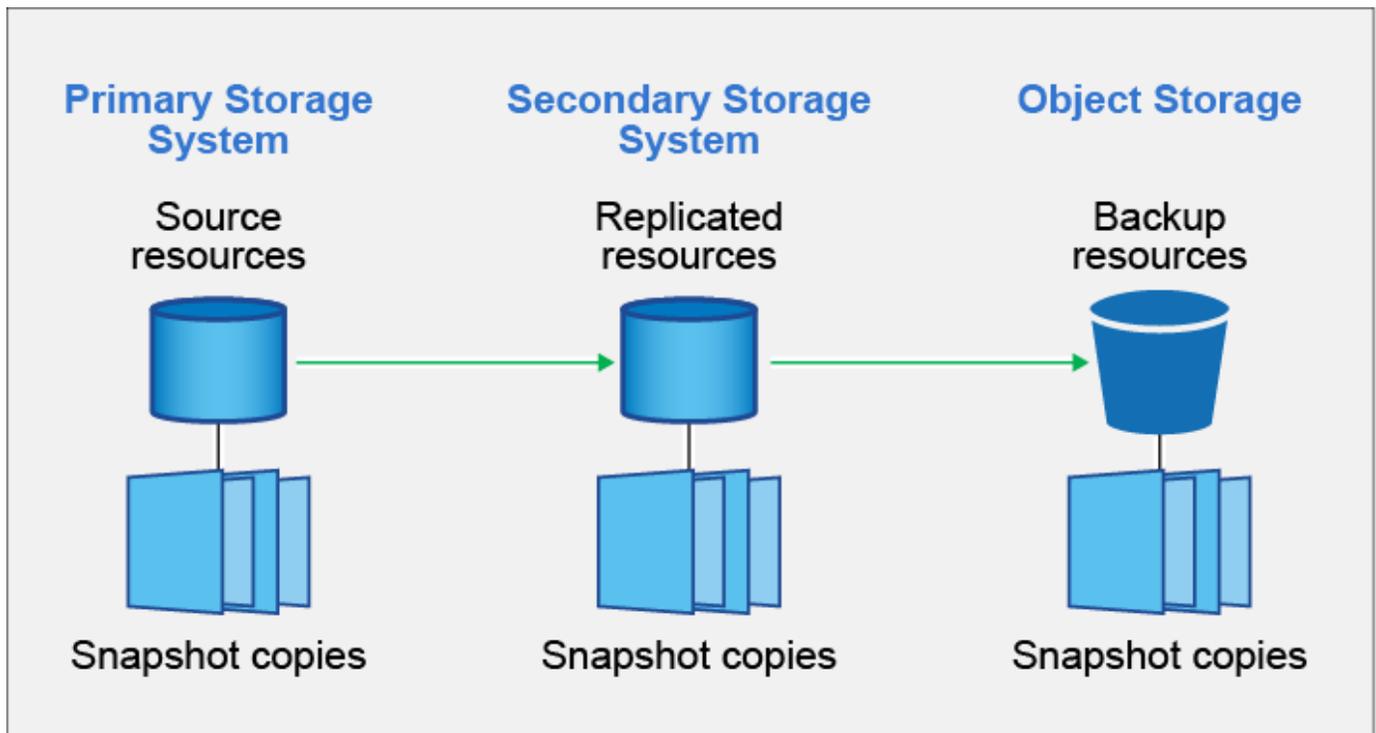
NetApp Backup and Recovery は、ONTAPボリュームデータの保護と長期アーカイブのためのバックアップおよび復元機能を提供します。3-2-1 戦略を実装して、ソースデータのコピーを2つの異なるストレージシステムに3つ、クラウドに1つ保存することができます。



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

アクティブ化後、バックアップとリカバリによって、ブロックレベルの永久増分バックアップが作成され、別のONTAPクラスターとクラウド内のオブジェクトストレージに保存されます。ソースボリュームに加えて、次のものも用意します。

- ソースシステム上のボリュームのスナップショット
- 別のストレージシステム上の複製ボリューム
- オブジェクトストレージ内のボリュームのバックアップ



NetApp Backup and Recovery は、NetApp のSnapMirrorデータ レプリケーション テクノロジーを活用して、スナップショットを作成し、それをバックアップの場所に転送することで、すべてのバックアップが完全に同期されるようにします。

3-2-1 アプローチの利点は次のとおりです。

- 複数のデータ コピーにより、内部および外部のサイバー セキュリティの脅威から保護されます。
- 異なるタイプのメディアを使用すると、1つのタイプに障害が発生した場合でも回復しやすくなります。
- オンサイト コピーから迅速に復元し、オンサイト コピーが侵害された場合はオフサイト コピーを使用できます。

必要に応じて、任意のバックアップ コピーから、ボリューム_全体、_フォルダ、または1つ以上の_ファイル_を同じシステムまたは別のシステムに復元できます。

機能

レプリケーション機能:

- バックアップと災害復旧をサポートするために、ONTAPストレージ システム間でデータを複製します。
- 高可用性により DR 環境の信頼性を確保します。
- 2つのシステム間の事前共有キー (PSK) を介して設定されたネイティブONTAPインフライト暗号化。
- コピーされたデータは、書き込み可能になって使用可能になるまで変更できません。
- 転送に失敗した場合、レプリケーションは自動的に修復されます。
- と比較すると ["NetApp Replication"](#)NetApp Backup and Recoveryのレプリケーションには、次の機能が含まれています。
 - 一度に複数のFlexVolボリュームをセカンダリ システムに複製します。
 - UI を使用して、複製されたボリュームをソース システムまたは別のシステムに復元します。

見る["ONTAPボリュームのレプリケーションの制限"](#)ONTAPボリュームのNetApp Backup and Recoveryで使用できないレプリケーション機能のリストについては、こちらをご覧ください。

オブジェクトへのバックアップ機能:

- 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します。
- 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、固有の復旧ポイント目標を持つ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。
- クラスタで今後作成されるすべてのボリュームに適用されるバックアップ ポリシーを作成します。
- 変更不可能なバックアップ ファイルを作成し、保持期間中はロックされて保護されるようにします。
- バックアップ ファイルをスキャンしてランサムウェア攻撃の可能性を検出し、感染したバックアップを自動的に削除/置き換えます。
- 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節約します。
- ボリュームのバックアップを保持しながら不要なソース ボリュームをアーカイブできるように、バックアップ関係を削除します。
- 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 クラウドまたはプライベート クラウドへバックアップします。
- バックアップ データは、保存時にはAES-256 ビット暗号化、実行時には TLS 1.2 HTTPS 接続によって保護されます。
- クラウド プロバイダーのデフォルトの暗号化キーを使用する代わりに、独自の顧客管理キーを使用してデータを暗号化します。

- 単一ボリュームの最大 4,000 件のバックアップをサポートします。

復元機能:

- ローカル スナップショット、複製されたボリューム、またはオブジェクト ストレージ内のバックアップされたボリュームから特定の時点のデータを復元します。
- ボリューム、フォルダー、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復元します。
- 別のサブスクリプション/アカウントを使用しているシステム、または別のリージョンにあるシステムにデータを復元します。
- クラウド ストレージからCloud Volumes ONTAPシステムまたはオンプレミス システムへのボリュームのクイック リストア を実行します。ボリュームへのアクセスをできるだけ早く提供する必要がある災害復旧の状況に最適です。
- 元の ACL を維持しながら、ブロック レベルでデータを復元し、指定した場所にデータを直接配置します。
- ファイル カタログを参照して検索し、個々のフォルダーとファイルを簡単に選択して単一ファイルの復元を行うことができます。

バックアップおよび復元操作でサポートされているシステム

NetApp Backup and Recovery は、ONTAPシステムとパブリックおよびプライベート クラウド プロバイダーをサポートします。

サポートされている地域

NetApp Backup and Recovery は、多くの Amazon Web Services、Microsoft Azure、Google Cloud リージョンでCloud Volumes ONTAPによってサポートされています。

["グローバル地域マップを使用して詳細を確認する"](#)

サポートされているバックアップ先

NetApp Backup and Recoveryと、次のソース システムから次のセカンダリ システムおよびパブリック クラウド プロバイダーとプライベート クラウド プロバイダーのオブジェクト ストレージにONTAPボリュームをバックアップできます。スナップショットはソース システムに存在します。

ソースシステム	セカンダリシステム (レプリケーション)	宛先オブジェクトストア (バックアップ)
AWS のCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	Amazon S3
Azure のCloud Volumes ONTAP	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure ブロブ
Google のCloud Volumes ONTAP	Google オンプレミスONTAPシステムのCloud Volumes ONTAP	Google Cloud Storage
オンプレミスのONTAPシステム	Cloud Volumes ONTAPオンプレミスONTAPシステム	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

サポートされている復元先

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから次のシステムにONTAPデータを復元できます。スナップショットはソース システムに存在し、同じシステムにのみ復元できます。

バックアップファイルの場所		宛先システム
オブジェクトストア (バックアップ)	セカンダリシステム (レプリケーション)	
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP
Azure ブログ	Azure のCloud Volumes ONTAP オンプレミスONTAPシステム	Azure のCloud Volumes ONTAP オンプレミスONTAPシステム
Google Cloud Storage	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
NetAppStorageGRID	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム
ONTAP S3	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム

「オンプレミスのONTAPシステム」への参照には、FAS、AFF、およびONTAP Selectシステムが含まれることに注意してください。

サポートされているボリューム

NetApp Backup and Recovery は、次のタイプのボリュームをサポートしています。

- FlexVol読み取り/書き込みボリューム
- FlexGroupボリューム (ONTAP 9.12.1以降が必要)
- SnapLock Enterpriseボリューム (ONTAP 9.11.1 以降が必要)
- オンプレミスボリュームのSnapLock Compliance (ONTAP 9.14 以降が必要)
- SnapMirrorデータ保護 (DP) 宛先ボリューム



NetApp Backup and Recovery は、FlexCacheボリュームのバックアップをサポートしていません。

以下のセクションを参照してください"[ONTAPボリュームのバックアップとリストアの制限](#)"追加の要件と制限については、こちらをご覧ください。

料金

ONTAPシステムでNetApp Backup and Recovery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。これら両方の料金は、サービスのオブジェクト部分へのバックアップに対して発生します。

スナップショットや複製ボリュームの作成には、スナップショットや複製ボリュームを保存するために必要な

ディスク容量以外は料金はかかりません。

リソース料金

オブジェクト ストレージ容量とクラウドへのバックアップ ファイルの書き込みと読み取りに対して、リソース料金がクラウド プロバイダーに支払われます。

- オブジェクト ストレージへのバックアップの場合、オブジェクト ストレージのコストをクラウド プロバイダーに支払います。

NetApp Backup and Recovery はソース ボリュームのストレージ効率を維持するため、ONTAP効率化後のデータ (重複排除と圧縮が適用された後の少量のデータ) に対してクラウド プロバイダーのオブジェクト ストレージ コストを支払います。

- 検索と復元を使用してデータを復元する場合、クラウド プロバイダーによって特定のリソースがプロビジョニングされ、検索要求によってスキャンされるデータの量に応じて TiB ごとにコストが発生します。(これらのリソースは参照と復元には必要ありません。)
 - AWSでは、"アマゾンアテナ"そして "AWS グループ"リソースは新しい S3 バケットにデプロイされません。
 - Azureでは、"Azure Synapse ワークスペース"そして "Azure データレイクストレージ"データを保存および分析するためにストレージ アカウントにプロビジョニングされます。
 - Googleでは新しいバケットがデプロイされ、"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。
- アーカイブ オブジェクト 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 データを復元する場合は、クラウド プロバイダーから追加の GiB あたりの取得料金とリクエストあたりの料金が発生します。
- ボリューム データの復元プロセス中にバックアップ ファイルをランサムウェアに対してスキャンする予定がある場合 (クラウド バックアップに対して DataLock と Ransomware Resilience を有効にしている場合)、クラウド プロバイダーから追加の送信コストも発生します。

サービス料

サービス料金はNetAppに支払われ、オブジェクト ストレージへのバックアップを 作成 するコストと、それらのバックアップからボリュームまたはファイルを 復元 するコストの両方をカバーします。オブジェクト ストレージにバックアップされるONTAPボリュームのソース論理使用容量 (ONTAP効率前) によって計算された、オブジェクト ストレージで保護するデータに対してのみ料金を支払います。この容量は、フロントエンド テラバイト (FETB) とも呼ばれます。

バックアップ サービスの支払い方法は 3 つあります。最初のオプションは、クラウド プロバイダーにサブスクライブすることです。これにより、月ごとに支払いが可能になります。2 番目のオプションは、年間契約を結ぶことです。3 番目のオプションは、NetAppから直接ライセンスを購入することです。

ライセンス

NetApp Backup and Recovery は、次の消費モデルで利用できます。

- **BYOL:** NetAppから購入したライセンスで、どのクラウド プロバイダーでも使用できます。
- **PAYGO:** クラウド プロバイダーのマーケットプレイスからの時間単位のサブスクリプション。
- **年間:** クラウド プロバイダーのマーケットプレイスからの年間契約。

バックアップ ライセンスは、オブジェクト ストレージからのバックアップと復元にのみ必要です。スナップショットおよび複製されたボリュームの作成にはライセンスは必要ありません。

自分のライセンスを持参する

BYOL は期間ベース (1 年、2 年、または 3 年) であり、1 TiB 単位で容量ベースになります。一定期間 (たとえば 1 年) および最大容量 (たとえば 10 TiB) のサービス使用料を NetApp に支払います。

サービスを有効にするために NetApp Console に入力するシリアル番号を受け取ります。どちらかの制限に達した場合は、ライセンスを更新する必要があります。バックアップ BYOL ライセンスは、NetApp Console 組織またはアカウントに関連付けられているすべてのソース システムに適用されます。

["BYOL ライセンスの管理方法を学ぶ"](#)。

従量課金制サブスクリプション

NetApp Backup and Recovery は、従量課金モデルで消費ベースのライセンスを提供します。クラウド プロバイダーのマーケットプレイスを通じてサブスクライブすると、バックアップされたデータに対して GiB ごとに料金が発生します。前払いはありません。クラウド プロバイダーから毎月の請求書を通じて請求されます。

["従量課金制サブスクリプションの設定方法を学ぶ"](#)。

PAYGO サブスクリプションに最初にサインアップすると、30 日間の無料トライアルが利用できることに注意してください。

年間契約

AWS を使用する場合、1 年、2 年、または 3 年の期間で 2 つの年間契約を利用できます。

- 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 NetApp Backup and Recovery をバンドルできる「CVO Professional」プラン。これには、このライセンスに対して課金される Cloud Volumes ONTAP ボリュームの無制限のバックアップが含まれます (バックアップ容量はライセンスに対してカウントされません)。

Azure を使用する場合、1 年、2 年、または 3 年の期間で 2 つの年間契約を利用できます。

- 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 NetApp Backup and Recovery をバンドルできる「CVO Professional」プラン。これには、このライセンスに対して課金される Cloud Volumes ONTAP ボリュームの無制限のバックアップが含まれます (バックアップ容量はライセンスに対してカウントされません)。

GCP を使用する場合、NetApp からプライベート オファーをリクエストし、NetApp Backup and Recovery のアクティベーション中に Google Cloud Marketplace からサブスクライブするときにプランを選択できます。

["年間契約の設定方法を学ぶ"](#)。

す。クラスター/システムごとに1つのオブジェクトストアがあり、コンソールではオブジェクトストアに「netapp-backup-clusteruid」という名前が付けられます。このオブジェクトストアを削除しないように注意してください。

- AWSでは、コンソールで ["Amazon S3 ブロックパブリックアクセス機能"](#) S3 バケット上。
- Azure では、コンソールは、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。コンソール ["BLOBデータへのパブリックアクセスをブロックします"](#) デフォルトです。
- GCP では、コンソールは Google Cloud Storage バケットのストレージ 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、コンソールは S3 バケットに既存のテナント アカウントを使用します。
- ONTAP S3 では、コンソールは S3 バケットに既存のユーザー アカウントを使用します。

将来的にクラスタの宛先オブジェクトストアを変更する場合は、["システムのNetApp Backup and Recoveryの登録を解除する"](#)、新しいクラウド プロバイダー情報を使用してNetApp Backup and Recoveryを有効にします。

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

システムに対してNetApp Backup and Recovery を有効にすると、最初に選択したすべてのボリュームが、選択したポリシーを使用してバックアップされます。スナップショット、複製されたボリューム、バックアップファイルごとに個別のポリシーを選択できます。異なるリカバリポイント目標 (RPO) を持つ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、そのクラスターに追加のポリシーを作成し、NetApp Backup and Recovery をアクティブ化した後でそれら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の毎時、毎日、毎週、毎月、毎年のバックアップの組み合わせを選択できます。オブジェクトへのバックアップでは、3 か月、1 年、7 年間のバックアップと保持を提供するシステム定義のポリシーのいずれかを選択することもできます。ONTAP System Manager またはONTAP CLI を使用してクラスタ上に作成したバックアップ保護ポリシーも選択肢として表示されます。これには、カスタムSnapMirrorラベルを使用して作成されたポリシーが含まれます。



ボリュームに適用されるスナップショット ポリシーには、レプリケーション ポリシーとオブジェクトへのバックアップ ポリシーで使用しているラベルのいずれかが必要です。一致するラベルが見つからない場合、バックアップ ファイルは作成されません。たとえば、「毎週」複製されたボリュームとバックアップ ファイルを作成する場合は、「毎週」スナップショットを作成するスナップショット ポリシーを使用する必要があります。

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、古いバックアップが削除されるため、常に最新のバックアップが保持されます (そのため、古いバックアップがスペースを占有し続けることはありません)。



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SnapMirror関係で定義されている期間と同じです。必要に応じて、API を使用してこれを変更できます。

バックアップファイルの保護設定

クラスターでONTAP 9.11.1 以降を使用している場合は、オブジェクト ストレージ内のバックアップを削除やランサムウェア攻撃から保護できます。各バックアップ ポリシーには、特定の期間 (保持期間) にわたってバックアップ ファイルに適用できる *DataLock* および *Ransomware Resilience* のセクションが用意されています。

- **DataLock** は、バックアップ ファイルが変更されたり削除されたりするのを防ぎます。
- **ランサムウェア保護** は、バックアップ ファイルの作成時とバックアップ ファイルからのデータの復元時に、バックアップ ファイルをスキャンしてランサムウェア攻撃の証拠を探します。

スケジュールされたランサムウェア保護スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は 7 日間です。スキャンは最新のスナップショットに対してのみ実行されます。コストを削減するために、スケジュールされたスキャンを無効にすることができます。「詳細設定」ページのオプションを使用して、最新のスナップショットでスケジュールされたランサムウェア スキャンを有効または無効にすることができます。有効にすると、デフォルトでスキャンが毎週実行されます。スケジュールを日単位や週単位に変更したり、無効にしたりしてコストを節約できます。

バックアップの保持期間は、バックアップ スケジュールの保持期間に最大 31 日間のバッファを加えた期間と同じです。たとえば、5 個のコピーが保持される 毎週 のバックアップでは、各バックアップ ファイルが 5 週間ロックされます。6 個のコピーが保持される 月次 バックアップでは、各バックアップ ファイルが 6 か月間ロックされます。

現在、バックアップ先が Amazon S3、Azure Blob、または NetApp StorageGRID の場合にサポートが利用できます。他のストレージ プロバイダーの宛先は、今後のリリースで追加される予定です。

詳細については、次の情報を参照してください。

- ["DataLockとランサムウェア保護の仕組み"](#)。
- ["詳細設定ページでランサムウェア保護オプションを更新する方法"](#)。



バックアップをアーカイブ ストレージに階層化している場合、DataLock を有効にすることはできません。

古いバックアップファイルのアーカイブストレージ

特定のクラウド ストレージを使用する場合、一定の日数後に古いバックアップ ファイルをより安価なストレージ クラス/アクセス ティアに移動できます。バックアップ ファイルを標準のクラウド ストレージに書き込まずに、すぐにアーカイブ ストレージに送信することも選択できます。DataLock を有効にしている場合はアーカイブ ストレージを使用できないことに注意してください。

- AWS では、バックアップは *Standard* ストレージ クラスで開始され、30 日後に *Standard-Infrequent Access* ストレージ クラスに移行します。

クラスターで ONTAP 9.10.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後に NetApp Backup and Recovery UI で古いバックアップを *S3 Glacier* または *S3 Glacier Deep Archive* ストレージに階層化することを選択できます。["AWS アーカイブストレージの詳細"](#)。

- Azure では、バックアップは *Cool* アクセス層に関連付けられています。

クラスターで ONTAP 9.10.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後に NetApp Backup and Recovery UI で古いバックアップを *Azure Archive* ストレージに階層化することを選択できます。["Azure アーカイブ ストレージの詳細"](#)。

- GCP では、バックアップは *Standard* ストレージ クラスに関連付けられています。

クラスターで ONTAP 9.12.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後に NetApp Backup and Recovery UI で古いバックアップをアーカイブ ストレージに階層化することを選択できます。["Google アーカイブ ストレージの詳細"](#)。

- StorageGRIDでは、バックアップは *Standard* ストレージ クラスに関連付けられます。

オンプレミスのクラスターでONTAP 9.12.1 以上を使用しており、StorageGRIDシステムで 11.4 以上を使用している場合は、一定の日数後に古いバックアップ ファイルをパブリック クラウド アーカイブ ストレージにアーカイブできます。現在サポートされているのは、AWS S3 Glacier/S3 Glacier Deep Archive または Azure Archive ストレージ層です。["StorageGRIDからのバックアップファイルのアーカイブについて詳しくは"](#)。

古いバックアップ ファイルのアーカイブの詳細については、[\[link:prev-ontap-policy-object-options.html\]](#) を参照してください。

FabricPool階層化ポリシーの考慮事項

バックアップするボリュームがFabricPoolアグリゲート上に存在し、それに割り当てられた階層化ポリシー以外のポリシーがある場合、注意すべき点がいくつかあります。 `none` :

- FabricPool階層化ボリュームの最初のバックアップでは、すべてのローカル データとすべての階層化データ (オブジェクト ストアから) を読み取る必要があります。バックアップ操作では、オブジェクト ストレージに階層化されたコールド データが「再加熱」されることはありません。

この操作により、クラウド プロバイダーからデータを読み取るためのコストが 1 回だけ増加する可能性があります。

- 後続のバックアップは増分バックアップであるため、この影響はありません。
- ボリュームが最初に作成されるときに階層化ポリシーが割り当てられている場合は、この問題は発生しません。
- 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 `all` ボリュームへの階層化ポリシー。データは即座に階層化されるため、NetApp Backup and Recovery はローカル層ではなくクラウド層からデータを読み取ります。同時バックアップ操作ではクラウド オブジェクト ストアへのネットワーク リンクが共有されるため、ネットワーク リソースが飽和状態になるとパフォーマンスが低下する可能性があります。この場合、このタイプのネットワーク飽和を減らすために、複数のネットワーク インターフェイス (LIF) を事前に構成する必要がある場合があります。

NetApp Backup and Recoveryで保護の旅を計画する

NetApp Backup and Recovery を使用すると、ソース ボリュームのコピーを最大 3 つ作成してデータを保護できます。ボリュームでバックアップと回復を有効にするときに選択できるオプションは多数あるため、準備ができるように選択内容を確認する必要があります。



NetApp Backup and Recoveryのワークロードを切り替えるには、["さまざまなNetApp Backup and Recoveryワークロードに切り替える"](#)。

以下のオプションについて説明します。

- どのような保護機能を使用しますか: スナップショット、複製ボリューム、クラウドへのバックアップ
- どのバックアップアーキテクチャを使用しますか: ボリュームのカスケードバックアップまたはファンアウトバックアップ

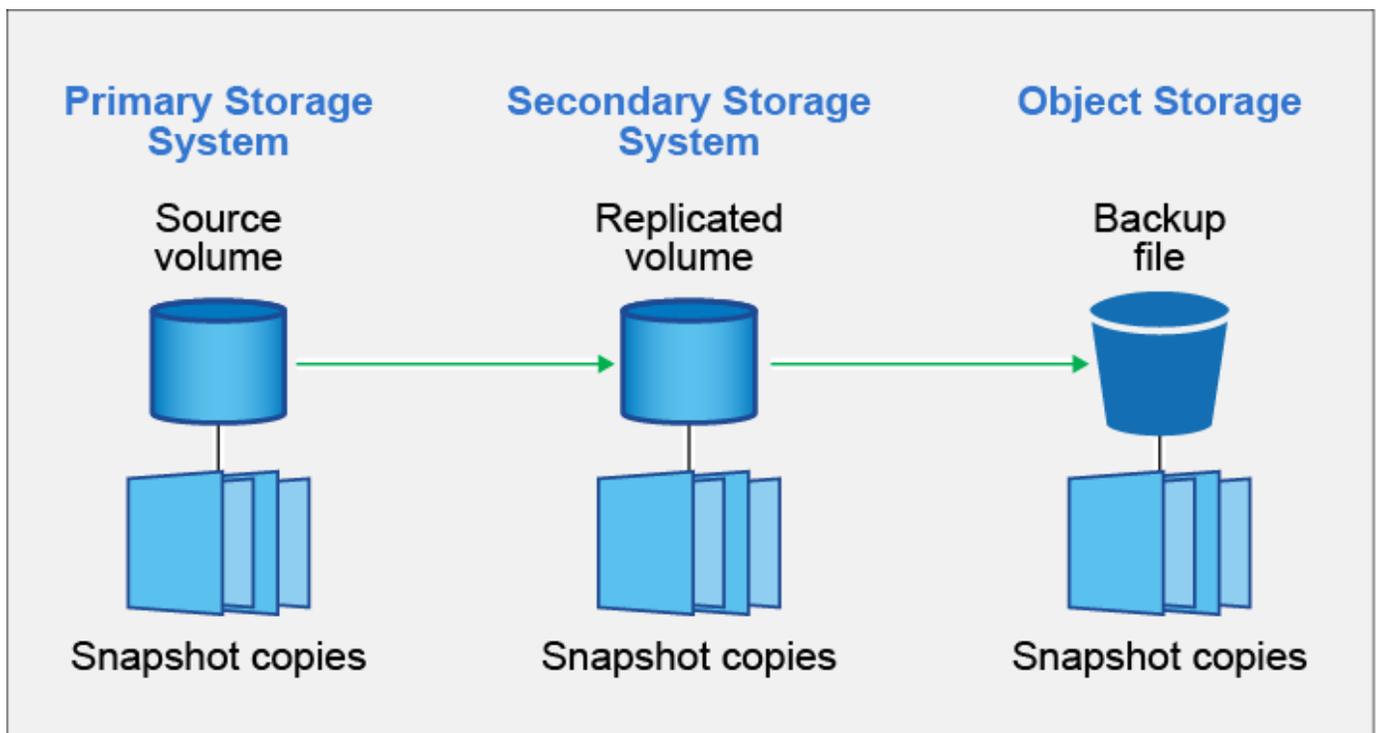
- デフォルトのバックアップポリシーを使用しますか、それともカスタムポリシーを作成する必要がありますか
- サービスにクラウドバケットを作成させたいですか、それとも始める前にオブジェクトストレージコンテナを作成したいですか？
- どのコンソール エージェント展開モードを使用していますか (標準、制限、またはプライベート モード)

どの保護機能を使用するか

使用する機能を選択する前に、各機能の機能と、提供される保護の種類について簡単に説明します。

バックアップ タイプ	説明
Snapshot	ソース ボリューム内のボリュームの読み取り専用の特定点のイメージをスナップショットとして作成します。スナップショットを使用して、個々のファイルを回復したり、ボリュームの内容全体を復元したりできます。
レプリケーション	別のONTAPストレージ システムにデータのセカンダリ コピーを作成し、セカンダリ データを継続的に更新します。データは最新の状態に保たれ、必要なときにいつでも利用できます。
クラウド バックアップ	保護と長期アーカイブの目的でクラウドにデータのバックアップを作成します。必要に応じて、ボリューム、フォルダー、または個々のファイルをバックアップから同じシステムまたは別のシステムに復元できます。

スナップショットはすべてのバックアップ方法の基礎であり、バックアップおよびリカバリ サービスを使用するために必要です。スナップショットは、ボリュームの読み取り専用の特定点のイメージです。イメージは、最後のスナップショットが作成されてからファイルに加えられた変更のみを記録するため、最小限のストレージスペースしか消費せず、パフォーマンスのオーバーヘッドもごくわずかです。ボリューム上に作成されたスナップショットは、図に示すように、複製されたボリュームとバックアップ ファイルをソース ボリュームに加えられた変更と同期させるために使用されます。



別のONTAPストレージシステムに複製されたボリュームを作成し、クラウドにファイルをバックアップすることもできます。または、複製されたボリュームまたはバックアップファイルのみを作成することもできます。それはあなたの選択です。

要約すると、ONTAPシステム内のボリュームに対して作成できる有効な保護フローは次のとおりです。

- ソースボリューム → スナップショット → 複製ボリューム → バックアップファイル
- ソースボリューム → スナップショット → バックアップファイル
- ソースボリューム → スナップショット → 複製ボリューム



複製されたボリュームまたはバックアップファイルの最初の作成には、ソースデータの完全なコピーが含まれます。これは、ベースライン転送と呼ばれます。後続の転送には、ソースデータの差分コピー (スナップショット) のみが含まれます。

さまざまなバックアップ方法の比較

次の表は、3つのバックアップ方法の一般的な比較を示しています。オブジェクトストレージスペースは通常、オンプレミスのディスクストレージよりも安価ですが、クラウドからデータを頻繁に復元する可能性があるとして予想される場合は、クラウドプロバイダーからの送信料金によって節約額がいくらか減る可能性があります。クラウド内のバックアップファイルからデータを復元する必要がある頻度を特定する必要があります。

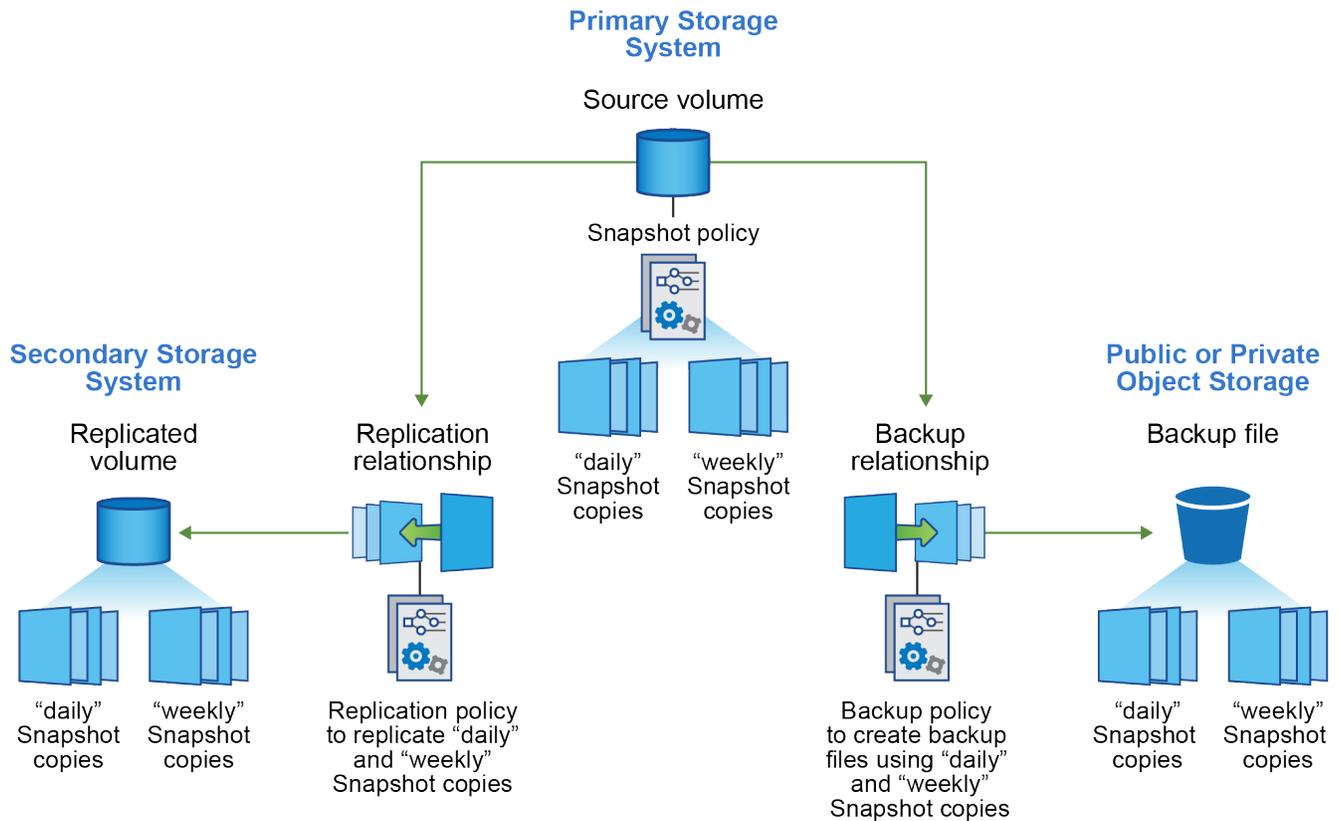
この基準に加えて、クラウドストレージでは、DataLock および Ransomware Resilience 機能を使用する場合、追加のセキュリティオプションが提供され、古いバックアップファイルにアーカイブストレージクラスを選択することで、さらにコストを節約できます。["DataLockとランサムウェア対策およびアーカイブストレージ設定の詳細"](#)。

バックアップタイプ	バックアップ速度	バックアップコスト	速度を回復する	復元コスト
スナップショット	高	低 (ディスク容量)	高	低
複製	中	中 (ディスク容量)	中	中規模 (ネットワーク)
クラウドバックアップ	低	低 (オブジェクト空間)	低	高額 (プロバイダー料金)

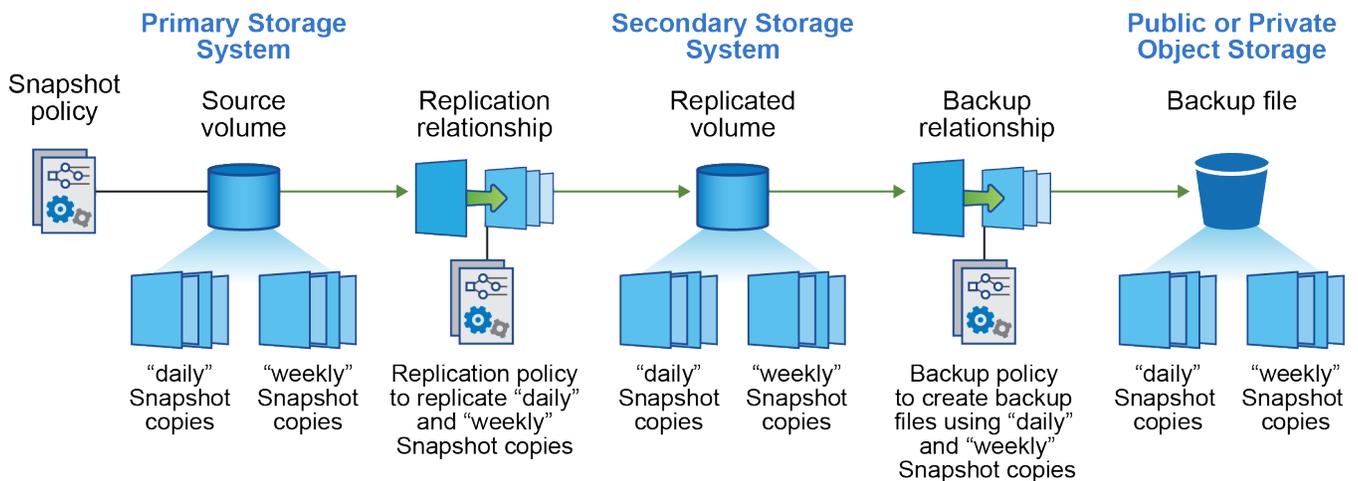
どのバックアップアーキテクチャを使用するか

複製されたボリュームとバックアップファイルの両方を作成する場合、ボリュームをバックアップするためにファンアウトアーキテクチャまたはカスケードアーキテクチャを選択できます。

ファンアウトアーキテクチャは、スナップショットを宛先ストレージシステムとクラウド内のバックアップオブジェクトの両方に独立して転送します。



カスケード アーキテクチャでは、まずスナップショットが宛先ストレージシステムに転送され、次にそのシステムがそのコピーをクラウド内のバックアップオブジェクトに転送します。



さまざまなアーキテクチャの選択肢の比較

この表は、ファンアウト アーキテクチャとカスケード アーキテクチャの比較を示します。

ファンアウト	カスケード
スナップショットを2つの異なるシステムに送信するため、ソースシステムのパフォーマンスへの影響はわずかです。	スナップショットを一度だけ送信するため、ソースストレージシステムのパフォーマンスへの影響が少なくなります。

ファンアウト	カスケード
すべてのポリシー、ネットワーク、ONTAP構成がソースシステム上で実行されるため、セットアップが簡単になります。	一部のネットワークとONTAP構成をセカンダリシステムからも実行する必要があります。

スナップショット、レプリケーション、バックアップのデフォルトポリシーを使用しますか？

NetAppが提供するデフォルトのポリシーを使用してバックアップを作成することも、カスタムポリシーを作成することもできます。アクティベーションウィザードを使用してボリュームのバックアップおよびリカバリサービスを有効にする場合、デフォルトのポリシーと、システム (Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム) にすでに存在するその他のポリシーから選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティベーションウィザードを開始する前または使用中にポリシーを作成できます。

- デフォルトのスナップショットポリシーでは、時間別、日次、週次スナップショットが作成され、時間別スナップショットが6つ、日次スナップショットが2つ、週次スナップショットが2つ保持されます。
- デフォルトのレプリケーションポリシーでは、毎日および毎週のスナップショットがレプリケートされ、7つの毎日のスナップショットと52の毎週のスナップショットが保持されます。
- デフォルトのバックアップポリシーでは、毎日および毎週のスナップショットが複製され、7つの毎日のスナップショットと52の毎週のスナップショットが保持されます。

レプリケーションまたはバックアップ用のカスタムポリシーを作成する場合、ポリシーラベル(「毎日」や「毎週」など)がスナップショットポリシーに存在するラベルと一致している必要があります。一致していないと、レプリケートされたボリュームとバックアップファイルが作成されません。

NetApp Backup and Recovery UIで、スナップショット、レプリケーション、およびオブジェクトストレージポリシーへのバックアップを作成できます。セクションを参照してください["新しいバックアップポリシーの追加"](#)詳細については。

NetApp Backup and Recoveryを使用してカスタムポリシーを作成するだけでなく、System Manager またはONTAPコマンドラインインターフェイス (CLI) を使用することもできます。

- ["System ManagerまたはONTAP CLIを使用してスナップショットポリシーを作成します"](#)
- ["System ManagerまたはONTAP CLIを使用してレプリケーションポリシーを作成します。"](#)

注意: System Manager を使用する場合は、レプリケーションポリシーのポリシータイプとして非同期を選択し、オブジェクトへのバックアップポリシーとして非同期とクラウドへのバックアップを選択します。

ここでは、カスタムポリシーを作成する場合に役立つ可能性のあるONTAP CLI コマンドのサンプルをいくつか示します。 `admin vserver` (ストレージVM) を `<vserver_name>` これらのコマンドでは。

ポリシーの説明	コマンド
シンプルなスナップショットポリシー	<code>snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly</code>

ポリシーの説明	コマンド
クラウドへのシンプルなバックアップ	<pre> snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>
DataLockとランサムウェア対策を備えたクラウドへのバックアップ	<pre> snapmirror policy create -policy CloudBackupService- Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name> snapmirror policy add-rule -policy CloudBackupService- Enterprise -retention-period 30days </pre>
アーカイブストレージクラスによるクラウドへのバックアップ	<pre> snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>
別のストレージシステムへのシンプルなレプリケーション	<pre> snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name> snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>



クラウド関係へのバックアップには、ボールド ポリシーのみを使用できます。

ポリシーはどこに保存されますか？

バックアップ ポリシーは、使用する予定のバックアップ アーキテクチャ (ファンアウトまたはカスケード) に応じて異なる場所に存在します。レプリケーションでは 2 つの ONTAP ストレージ システムがペアになり、オブジェクトへのバックアップではストレージ プロバイダーが宛先として使用されるため、レプリケーションポリシーとバックアップポリシーは同じ方法で設計されていません。

- スナップショット ポリシーは常にプライマリ ストレージ システムに存在します。
- レプリケーション ポリシーは常にセカンダリ ストレージ システムに存在します。
- オブジェクトへのバックアップ ポリシーは、ソース ボリュームが存在するシステム上に作成されます。これは、ファンアウト構成の場合はプライマリ クラスタ、カスケード構成の場合はセカンダリ クラスタです。

これらの違いは表に示されています。

アーキテクチャ	スナップショットポリシー	レプリケーションポリシー	バックアップ ポリシー
ファンアウト	プライマリ	セカンダリ	プライマリ
カスケード	プライマリ	セカンダリ	セカンダリ

したがって、カスケード アーキテクチャを使用するときカスタム ポリシーを作成する予定の場合は、複製

されたボリュームが作成されるセカンダリ システムでオブジェクト ポリシーへのレプリケーションとバックアップを作成する必要があります。ファンアウト アーキテクチャを使用するときにカスタム ポリシーを作成する予定の場合は、複製されたボリュームが作成されるセカンダリ システムにレプリケーション ポリシーを作成し、プライマリ システムにオブジェクト ポリシーへのバックアップを作成する必要があります。

すべてのONTAPシステムに存在するデフォルトのポリシーを使用している場合は、設定は完了です。

独自のオブジェクトストレージコンテナを作成しますか？

システムのオブジェクト ストレージにバックアップ ファイルを作成すると、デフォルトでは、バックアップ およびリカバリ サービスによって、構成したオブジェクト ストレージ アカウントにバックアップ ファイル用のコンテナ (バケットまたはストレージ アカウント) が作成されます。AWS または GCP バケットの名前は、デフォルトで「netapp-backup-<uuid>」になります。Azure Blob ストレージ アカウントの名前は「netappbackup<uuid>」です。

特定のプレフィックスを使用したり、特別なプロパティを割り当てたりしたい場合は、オブジェクト プロバイダー アカウントでコンテナを自分で作成できます。独自のコンテナを作成する場合は、アクティベーション ウィザードを開始する前にコンテナを作成する必要があります。NetApp Backup and Recovery、任意のバケットを使用したり、バケットを共有したりできます。バックアップ アクティベーション ウィザードは、選択したアカウントと資格情報に対してプロビジョニングされたコンテナを自動的に検出し、使用するコンテナを選択できるようにします。

バケットは、コンソールから、またはクラウド プロバイダーから作成できます。

- ["コンソールから Amazon S3 バケットを作成する"](#)
- ["コンソールから Azure Blob ストレージ アカウントを作成する"](#)
- ["コンソールから Google Cloud Storage バケットを作成する"](#)

「netapp-backup-xxxxxx」以外のバケットプレフィックスを使用する予定の場合は、コンソールエージェントの IAM ロールの S3 権限を変更する必要があります。

高度なバケット設定

古いバックアップ ファイルをアーカイブ ストレージに移動する場合、または DataLock と Ransomware 保護を有効にしてバックアップ ファイルをロックし、ランサムウェアの可能性をスキャンする場合は、特定の構成設定でコンテナを作成する必要があります。

- 現時点では、クラスターでONTAP 9.10.1 以降のソフトウェアを使用している場合、独自のバケット上のアーカイブ ストレージはAWS S3 ストレージでサポートされています。デフォルトでは、バックアップは S3 *Standard* ストレージ クラスから開始されます。適切なライフサイクル ルールを使用してバケットを作成してください。
 - 30 日後、バケットの全スコープ内のオブジェクトを S3 *Standard-IA* に移動します。
 - 「smc_push_to_archive: true」タグが付いたオブジェクトを `_Glacier Flexible Retrieval_` (旧S3 Glacier) に移動します。
- DataLock とランサムウェア保護は、クラスターでONTAP 9.11.1 以降のソフトウェアを使用している場合はAWS ストレージでサポートされ、ONTAP 9.12.1 以降のソフトウェアを使用している場合はAzure ストレージでサポートされます。
 - AWS の場合、30 日間の保持期間を使用してバケットでオブジェクト ロックを有効にする必要があります。

- Azure の場合、バージョンレベルの不変性をサポートするストレージ クラスを作成する必要があります。

どのコンソールエージェント展開モードを使用していますか

すでにコンソールを使用してストレージを管理している場合は、コンソール エージェントがすでにインストールされています。NetApp Backup and Recoveryと同じコンソール エージェントを使用する予定であれば、準備は完了です。別のコンソール エージェントを使用する必要がある場合は、バックアップとリカバリの実装を開始する前にそれをインストールする必要があります。

NetApp Consoleは、ビジネス要件とセキュリティ要件を満たす方法でコンソールを使用できるようにする複数の導入モードを提供します。標準モードでは、コンソール SaaS レイヤーを活用して完全な機能を提供しますが、制限モードとプライベートモードは接続制限のある組織で利用できます。

"NetApp Consoleの導入モードの詳細"。

完全なインターネット接続を備えたサイトのサポート

NetApp Backup and Recovery を完全なインターネット接続 (標準モード または SaaS モード と呼ばれます) を備えたサイトで使用する場合、コンソールによって管理されるオンプレミスのONTAPまたはCloud Volumes ONTAPシステムに複製されたボリュームを作成でき、サポートされているいずれかのクラウド プロバイダーのオブジェクト ストレージにバックアップ ファイルを作成できます。"[サポートされているバックアップ先の完全なリストを参照してください](#)"。

有効なコンソール エージェントの場所の一覧については、バックアップ ファイルを作成する予定のクラウド プロバイダーの次のいずれかのバックアップ手順を参照してください。コンソール エージェントを Linux マシンに手動でインストールするか、特定のクラウド プロバイダーに展開する必要があるという制限がいくつかあります。

- "[Cloud Volumes ONTAPデータを Amazon S3 にバックアップする](#)"
- "[Cloud Volumes ONTAPデータを Azure Blob にバックアップする](#)"
- "[Cloud Volumes ONTAPデータを Google Cloud にバックアップする](#)"
- "[オンプレミスのONTAPデータを Amazon S3 にバックアップする](#)"
- "[オンプレミスのONTAPデータを Azure Blob にバックアップする](#)"
- "[オンプレミスのONTAPデータを Google Cloud にバックアップする](#)"
- "[オンプレミスのONTAPデータをStorageGRIDにバックアップする](#)"
- "[オンプレミスのONTAPをONTAP S3 にバックアップする](#)"

インターネット接続が制限されているサイトのサポート

NetApp Backup and Recovery は、インターネット接続が制限されているサイト (制限モード と呼ばれます) でボリューム データをバックアップするために使用できます。この場合、宛先のクラウド リージョンにコンソール エージェントを展開する必要があります。

- オンプレミスのONTAPシステムまたはAWS 商用リージョンにインストールされたCloud Volumes ONTAPシステムから Amazon S3 にデータをバックアップできます。"[Cloud Volumes ONTAPデータを Amazon S3 にバックアップする](#)"。
- オンプレミスのONTAPシステムまたは Azure 商用リージョンにインストールされたCloud Volumes

ONTAPシステムから Azure Blob にデータをバックアップできます。"[Cloud Volumes ONTAPデータを Azure Blob にバックアップする](#)"。

インターネットに接続できないサイトのサポート

NetApp Backup and Recovery は、インターネット接続のないサイト (プライベート モード または ダーク サイトとも呼ばれます) でボリューム データをバックアップするために使用できます。この場合、同じサイト内の Linux ホストにコンソール エージェントを展開する必要があります。



BlueXPプライベート モード (レガシーBlueXPインターフェイス) は通常、インターネット接続がなく、AWS Secret Cloud、AWS Top Secret Cloud、Azure IL6 などの安全なクラウド領域があるオンプレミス環境で使用されます。NetApp は、従来のBlueXPインターフェイスを使用してこれらの環境を引き続きサポートします。従来のBlueXPインターフェイスのプライベートモードのドキュメントについては、"[BlueXPプライベートモードの PDF ドキュメント](#)"。

- ローカルのオンプレミスONTAPシステムからローカルのNetApp StorageGRIDシステムにデータをバックアップできます。"[オンプレミスのONTAPデータをStorageGRIDにバックアップする](#)"。
- ローカルのオンプレミスONTAPシステムから、ローカルのオンプレミスONTAPシステムまたは S3 オブジェクト ストレージ用に構成されたCloud Volumes ONTAPシステムにデータをバックアップできます。"[オンプレミスのONTAPデータをONTAP S3 にバックアップする](#)"。

NetApp Backup and Recoveryを使用してONTAPボリュームのバックアップポリシーを管理する

NetApp Backup and Recoveryでは、NetAppが提供する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を作成するか、カスタム ポリシーを作成します。ポリシーは、バックアップの頻度、バックアップの実行時間、保持されるバックアップ ファイルの数を制御します。



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

アクティベーション ウィザードを使用してボリュームのバックアップおよびリカバリ サービスを有効にする場合、デフォルトのポリシーと、システム (Cloud Volumes ONTAPまたはオンプレミスのONTAPシステム) にすでに存在するその他のポリシーから選択できます。既存のポリシーとは異なるポリシーを使用する場合は、アクティベーション ウィザードを使用する前または使用中にポリシーを作成できます。

提供されているデフォルトのバックアップポリシーの詳細については、以下を参照してください。"[保護の旅を計画する](#)"。

NetApp Backup and Recovery は、スナップショット、レプリケーション、オブジェクト ストレージへのバックアップという 3 種類のONTAPデータのバックアップを提供します。ポリシーは、使用するアーキテクチャとバックアップの種類に応じて異なる場所に存在します。

アーキテクチャ	スナップショットポリシーの保存場所	レプリケーションポリシーの保存場所	オブジェクトポリシーの保存場所へのバックアップ
ファンアウト	プライマリ	セカンダリ	プライマリ

アーキテクチャ	スナップショットポリシーの保存場所	レプリケーションポリシーの保存場所	オブジェクトポリシーの保存場所へのバックアップ
カスケード	プライマリ	セカンダリ	セカンダリ

環境、設定、保護の種類に応じて、次のツールを使用してバックアップ ポリシーを作成します。

- NetApp ConsoleUI
- システムマネージャーUI
- ONTAP CLI



System Manager を使用する場合は、レプリケーション ポリシーのポリシー タイプとして 非同期 を選択し、オブジェクトへのバックアップ ポリシーとして 非同期 とクラウドへのバックアップ を選択します。

システムのポリシーを表示する

1. コンソール UI で、ボリューム > バックアップ設定 を選択します。
2. バックアップ設定ページでシステムを選択し、*アクション*を選択します。... アイコンをクリックし、*ポリシー管理*を選択します。

ポリシー管理ページが表示されます。スナップショット ポリシーはデフォルトで表示されます。

3. システム内に存在する他のポリシーを表示するには、レプリケーション ポリシー または バックアップ ポリシー のいずれかを選択します。既存のポリシーをバックアップ プランに使用できる場合は、準備は完了です。異なる特性を持つポリシーが必要な場合は、このページから新しいポリシーを作成できます。

ポリシーを作成

オブジェクト ストレージへのスナップショット、レプリケーション、バックアップを管理するポリシーを作成できます。

- [\[スナップショットを開始する前にスナップショットポリシーを作成する\]](#)
- [\[レプリケーションを開始する前にレプリケーションポリシーを作成する\]](#)
- [\[バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成します。\]](#)

スナップショットを開始する前にスナップショットポリシーを作成する

3-2-1 戦略の一部として、プライマリ ストレージ システム上のボリュームのスナップショットを作成します。

ポリシー作成プロセスの一部として、スケジュールと保持を示すスナップショットとSnapMirrorラベルを識別することが含まれます。定義済みのラベルを使用することも、独自のラベルを作成することもできます。

手順

1. コンソール UI で、ボリューム > バックアップ設定 を選択します。
2. バックアップ設定ページでシステムを選択し、*アクション*を選択します。... アイコンをクリックし、*ポリシー管理*を選択します。

ポリシー管理ページが表示されます。

3. [ポリシー] ページで、[ポリシーの作成] > [スナップショット ポリシーの作成] を選択します。
4. ポリシー名を指定します。
5. スナップショット スケジュールを選択します。最大 5 つのラベルを設定できます。または、スケジュールを作成します。
6. スケジュールを作成する場合:
 - a. 時間ごと、日ごと、週ごと、月ごと、または年ごとの頻度を選択します。
 - b. スケジュールと保持期間を示すスナップショット ラベルを指定します。
 - c. スナップショットをいつ、どのくらいの頻度で取得するかを入力します。
 - d. 保持: 保持するスナップショットの数を入力します。
7. *作成*を選択します。

カスケードアーキテクチャを使用したスナップショットポリシーの例

この例では、2 つのクラスターを持つスナップショット ポリシーを作成します。

1. クラスター 1:
 - a. ポリシー ページでクラスター 1 を選択します。
 - b. レプリケーションおよびオブジェクトへのバックアップ ポリシー セクションは無視します。
 - c. スナップショット ポリシーを作成します。
2. クラスター 2:
 - a. ポリシー ページでクラスター 2 を選択します。
 - b. スナップショット ポリシー セクションは無視します。
 - c. オブジェクト ポリシーへのレプリケーションおよびバックアップを構成します。

レプリケーションを開始する前にレプリケーションポリシーを作成する

3-2-1 戦略には、別のストレージ システム上のボリュームの複製が含まれる場合があります。レプリケーション ポリシーは、セカンダリ ストレージ システム上に存在します。

手順

1. [ポリシー] ページで、[ポリシーの作成] > [レプリケーション ポリシーの作成] を選択します。
2. 「ポリシーの詳細」セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル (最大 5 個) を指定します。
4. 転送スケジュールを指定します。
5. *作成*を選択します。

バックアップを開始する前に、オブジェクトストレージへのバックアップポリシーを作成します。

3-2-1 戦略には、ボリュームをオブジェクト ストレージにバックアップすることが含まれる場合があります。

このストレージポリシーは、バックアップアーキテクチャに応じて異なるストレージシステムの場所に存在します。

- ファンアウト: プライマリストレージシステム
- カスケード: セカンダリストレージシステム

手順

1. ポリシー管理ページで、ポリシーの作成 > *バックアップポリシーの作成*を選択します。
2. 「ポリシーの詳細」セクションで、ポリシー名を指定します。
3. 各ラベルの保持期間を示すSnapMirrorラベル (最大 5 個) を指定します。
4. 転送スケジュールやバックアップをアーカイブするタイミングなどの設定を指定します。
5. (オプション) 一定の日数が経過した後に古いバックアップ ファイルを、より安価なストレージ クラスまたはアクセスティアに移動するには、[アーカイブ] オプションを選択し、データがアーカイブされるまでの経過日数を指定します。バックアップ ファイルをアーカイブ ストレージに直接送信するには、「Archive After Days」に **0** を入力します。

["アーカイブストレージ設定の詳細"](#)。

6. (オプション) バックアップが変更されたり削除されたりするのを防ぐには、**DataLock** とランサムウェア保護 オプションを選択します。

クラスターでONTAP 9.11.1 以降を使用している場合は、*DataLock* と *Ransomware protection* を構成することで、バックアップが削除されないように保護することができます。

["利用可能なDataLock設定の詳細"](#)。

7. *作成*を選択します。

ポリシーを編集する

カスタム スナップショット、レプリケーション、またはバックアップ ポリシーを編集できます。

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すべてのボリュームに影響します。

手順

1. ポリシー管理ページでポリシーを選択し、*アクション*を選択します。  アイコンをクリックし、[ポリシーの編集] を選択します。



プロセスはレプリケーション ポリシーとバックアップ ポリシーで同じです。

2. 「ポリシーの編集」 ページで変更を加えます。
3. *保存*を選択します。

ポリシーを削除する

どのボリュームにも関連付けられていないポリシーを削除できます。

ボリュームにポリシーが関連付けられており、そのポリシーを削除する場合は、まずボリュームからポリシー

を削除する必要があります。

手順

1. ポリシー管理ページでポリシーを選択し、*アクション*を選択します。  アイコンをクリックし、*スナップショットポリシーの削除*を選択します。
2. *削除*を選択します。

詳細情報の参照

System Manager またはONTAP CLI を使用してポリシーを作成する手順については、以下を参照してください。

["System Managerを使用してスナップショットポリシーを作成する"](#) ["ONTAP CLIを使用してスナップショットポリシーを作成する"](#) ["System Managerを使用してレプリケーションポリシーを作成する"](#) ["ONTAP CLIを使用してレプリケーションポリシーを作成する"](#) ["System Manager を使用してオブジェクト ストレージ ポリシーへのバックアップを作成する"](#) ["ONTAP CLIを使用してオブジェクトストレージポリシーへのバックアップを作成する"](#)

NetApp Backup and Recoveryのオブジェクトへのバックアップポリシー オプション

NetApp Backup and Recovery を使用すると、オンプレミスのONTAPおよびCloud Volumes ONTAPシステム用のさまざまな設定でバックアップ ポリシーを作成できます。



これらのポリシー設定は、オブジェクト ストレージへのバックアップにのみ関連します。これらの設定はいずれもスナップショットまたはレプリケーション ポリシーには影響しません。



NetApp Backup and Recoveryのワークロードを切り替えるには、["さまざまなNetApp Backup and Recoveryワークロードに切り替える"](#)。

バックアップスケジュールオプション

NetApp Backup and Recovery を使用すると、システム (クラスタ) ごとに固有のスケジュールを持つ複数のバックアップ ポリシーを作成できます。異なる復旧ポイント目標 (RPO) を持つボリュームに、異なるバックアップ ポリシーを割り当てることができます。

各バックアップ ポリシーには、バックアップ ファイルに適用できる「ラベルと保持」のセクションが用意されています。ボリュームに適用されるスナップショット ポリシーは、NetApp Backup and Recoveryによって認識されるポリシーのいずれかである必要があることに注意してください。そうでないと、バックアップ ファイルは作成されません。

スケジュールには、ラベルと保持値の 2 つの部分があります。

- ラベル は、ボリュームからバックアップ ファイルが作成 (または更新) される頻度を定義します。次の種類のラベルから選択できます。
 - 時間別、日別、週別、月別、*年別*の時間枠のいずれか、または組み合わせを選択できます。
 - 3 か月、1 年、または 7 年間のバックアップと保持を提供するシステム定義のポリシーのいずれかを

選択できます。

- ONTAP System Manager または ONTAP CLI を使用してクラスタ上にカスタム バックアップ保護ポリシーを作成した場合は、それらのポリシーのいずれかを選択できます。
- 保持 値は、各ラベル (期間) に保持されるバックアップ ファイルの数を定義します。カテゴリまたは間隔内のバックアップの最大数に達すると、古いバックアップが削除されるため、常に最新のバックアップが保持されます。また、古いバックアップがクラウド内のスペースを占有し続けることがなくなるため、ストレージ コストも節約できます。

たとえば、7 つの 週次 バックアップと 12 つの 月次 バックアップを作成するバックアップ ポリシーを作成するとします。

- 毎週、毎月、ボリュームのバックアップファイルが作成されます
- 8週目には、最初の週次バックアップが削除され、8週目の新しい週次バックアップが追加されます (最大7つの週次バックアップが保持されます)
- 13 か月目に、最初の月次バックアップが削除され、13 か月目の新しい月次バックアップが追加されます (最大 12 の月次バックアップが保持されます)

年間バックアップは、オブジェクト ストレージに転送された後、ソース システムから自動的に削除されます。このデフォルトの動作は、システムの「詳細設定」ページで変更できます。

DataLockとランサムウェア保護オプション

NetApp Backup and Recovery は、ボリューム バックアップに対する DataLock およびランサムウェア保護のサポートを提供します。これらの機能を使用すると、バックアップ ファイルをロックしてスキャンし、バックアップ ファイル上のランサムウェアの可能性を検出できます。これは、クラスターのボリューム バックアップをさらに保護したい場合に、バックアップ ポリシーで定義できるオプションの設定です。

これら 2 つの機能はバックアップ ファイルを保護するため、バックアップに対してランサムウェア攻撃が試みられた場合でも、常に有効なバックアップ ファイルがあり、そこからデータを回復することができます。また、バックアップをロックして一定期間保持する必要がある特定の規制要件を満たすのにも役立ちます。DataLock および Ransomware Resilience オプションを有効にすると、NetApp Backup and Recovery アクティベーションの一部としてプロビジョニングされるクラウド バケットで、オブジェクトのロックとオブジェクトのバージョン管理が有効になります。

この機能はソース ボリュームを保護するものではなく、ソース ボリュームのバックアップのみを保護します。いくつかの ["ONTAPが提供するランサムウェア対策"](#)ソースボリュームを保護します。



- DataLock とランサムウェア保護を使用する予定の場合は、最初のバックアップ ポリシーを作成し、そのクラスターに対してNetApp Backup and Recovery をアクティブ化するときに、これを有効にできます。後で、NetApp Backup and Recovery の詳細設定を使用して、ランサムウェア スキャンを有効または無効にすることができます。
- ボリューム データを復元するときにコンソールがバックアップ ファイルでランサムウェアをスキャンすると、バックアップ ファイルの内容にアクセスするためにクラウド プロバイダーから追加の送信コストが発生します。

DataLockとは

この機能を使用すると、SnapMirror経由でクラウドに複製されたクラウド スナップショットをロックできるほか、ランサムウェア攻撃を検出してオブジェクト ストア上のスナップショットの一貫したコピーを回復する機能も有効になります。この機能は、AWS、Azure、Google Cloud Platform、StorageGRIDでサポートさ

れています。

DataLock は、バックアップ ファイルが一定期間変更または削除されるのを防ぎます。これは、不変ストレージとも呼ばれます。この機能は、オブジェクト ストレージ プロバイダーの「オブジェクト ロック」テクノロジーを使用します。

クラウド プロバイダーは、スナップショットの保持期間に基づいて計算される保持期限 (RUD) を使用します。スナップショットの保持期間は、ラベルとバックアップ ポリシーで定義された保持数に基づいて計算されます。

スナップショットの最小保存期間は 30 日です。これがどのように機能するか、いくつかの例を見てみましょう。

- 保持回数 20 で 毎日 ラベルを選択した場合、スナップショットの保持期間は 20 日となり、デフォルトで最小の 30 日になります。
- 保持回数 4 で **Weekly** ラベルを選択した場合、スナップショットの保持期間は 28 日となり、デフォルトで最小の 30 日になります。
- 保持回数 3 で 月次 ラベルを選択した場合、スナップショットの保持期間は 90 日になります。
- 保持回数 1 で **Yearly** ラベルを選択した場合、スナップショットの保持期間は 365 日になります。

保持期限 (RUD) とは何ですか？ また、それはどのように計算されますか？

保持期限 (RUD) は、スナップショットの保持期間に基づいて決定されます。保存期間は、スナップショットの保存期間とバッファを合計して計算されます。

- バッファは、転送時間のバッファ (3 日) + コスト最適化のバッファ (28 日) で、合計 31 日になります。
- 最小保持期間は 30 日 + 31 日のバッファ = 61 日です。

以下に例をいくつか挙げます。

- 12 回の保持期間を持つ月次バックアップ スケジュールを作成した場合、バックアップは 12 か月間 (プラス 31 日間) ロックされた後、削除され (次のバックアップ ファイルに置き換えられます) ます。
- 毎日 30 回、毎週 7 回、毎月 12 回のバックアップを作成するバックアップ ポリシーを作成する場合、ロックされた保持期間は 3 つあります。
 - 「30日ごと」のバックアップは61日間 (30日間+31日間のバッファ) 保持されます。
 - 「7週間ごと」のバックアップは11週間 (7週間+31日) 保持され、
 - 「12 か月ごと」のバックアップは 12 か月間 (プラス 31 日間) 保持されます。
- 24 の保持期間を持つ 1 時間ごとのバックアップ スケジュールを作成すると、バックアップが 24 時間ロックされると思われるかもしれませんが、ただし、これは最小期間の 30 日未満であるため、各バックアップは 61 日間 (30 日 + 31 日のバッファ) ロックされ、保持されます。



古いバックアップは、バックアップ ポリシーの保持期間後ではなく、DataLock の保持期間が終了した後に削除されます。

DataLock の保持設定は、バックアップ ポリシーのポリシー保持設定よりも優先されます。バックアップ ファイルがオブジェクト ストアに長期間保存されるため、ストレージ コストに影響する可能性があります。

DataLockとランサムウェア保護を有効にする

ポリシーを作成するときに、DataLock とランサムウェア保護を有効にできます。ポリシーの作成後は、これを有効化、変更、無効化することはできません。

1. ポリシーを作成するときは、**DataLock** および **Ransomware Resilience** セクションを展開します。
2. 次のいずれかを選択します。
 - なし: DataLock 保護とランサムウェア耐性は無効になっています。
 - ロック解除: DataLock 保護とランサムウェア耐性が有効になっています。特定の権限を持つユーザーは、保持期間中に保護されたバックアップ ファイルを上書きまたは削除できます。
 - ロック済み: DataLock 保護とランサムウェア耐性が有効になっています。保持期間中、ユーザーは保護されたバックアップ ファイルを上書きまたは削除することはできません。これにより、完全な規制遵守が実現します。

参照"[詳細設定ページでランサムウェア保護オプションを更新する方法](#)".

ランサムウェア対策とは

ランサムウェア保護は、バックアップ ファイルをスキャンして、ランサムウェア攻撃の証拠を探します。ランサムウェア攻撃の検出は、チェックサムと比較を使用して実行されます。新しいバックアップ ファイルと以前のバックアップ ファイルで潜在的なランサムウェアが特定された場合、その新しいバックアップ ファイルは、ランサムウェア攻撃の兆候が見られない最新のバックアップ ファイルに置き換えられます。(ランサムウェア攻撃を受けたと判断されたファイルは、置き換えられてから 1 日後に削除されます。)

スキャンは次の状況で発生します:

- クラウド バックアップ オブジェクトのスキャンは、クラウド オブジェクト ストレージに転送されるとすぐに開始されます。バックアップ ファイルが最初にクラウド ストレージに書き込まれるときにスキャンが実行されず、次のバックアップ ファイルが書き込まれるときにスキャンが実行されます。
- 復元プロセスのためにバックアップを選択すると、ランサムウェア スキャンを開始できます。
- スキャンはいつでもオンデマンドで実行できます。

回復プロセスはどのように機能しますか?

ランサムウェア攻撃が検出されると、サービスは Active Data Console エージェントの Integrity Checker REST API を使用して回復プロセスを開始します。データ オブジェクトの最も古いバージョンが真実のソースであり、回復プロセスの一環として現在のバージョンに作成されます。

これがどのように機能するか見てみましょう:

- ランサムウェア攻撃が発生した場合、サービスはバケット内のオブジェクトを上書きまたは削除しようとします。
- クラウド ストレージはバージョン管理が有効になっているため、バックアップ オブジェクトの新しいバージョンが自動的に作成されます。バージョン管理がオンの状態でオブジェクトを削除すると、そのオブジェクトは削除済みとしてマークされますが、引き続き取得可能です。オブジェクトが上書きされた場合、以前のバージョンが保存され、マークされます。
- ランサムウェア スキャンが開始されると、両方のオブジェクト バージョンのチェックサムが検証され、比較されます。チェックサムが矛盾している場合、潜在的なランサムウェアが検出されています。

- 回復プロセスでは、最後に正常だったコピーに戻す作業が行われます。

サポートされているシステムとオブジェクトストレージプロバイダー

次のパブリックおよびプライベート クラウド プロバイダーのオブジェクト ストレージを使用する場合、次のシステムのONTAPボリュームで DataLock およびランサムウェア保護を有効にできます。

ソースシステム	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 ブロブ
Google Cloud のCloud Volumes ONTAP	Google Cloud
オンプレミスのONTAPシステム	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

要件

- AWS の場合:
 - クラスタはONTAP 9.11.1以降を実行している必要があります
 - コンソールエージェントはクラウドまたはオンプレミスに導入できます
 - 次の S3 権限は、コンソール エージェントに権限を提供する IAM ロールの一部である必要があります。これらは、リソース「arn:aws:s3:::netapp-backup-*」の「backupS3Policy」セクションにあります。

AWS S3 の権限

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:オブジェクトのタグ付け
- s3:オブジェクトの削除
- s3:オブジェクトのタグ付けを削除
- s3:GetObjectRetention
- s3:オブジェクトバージョンタグ付けの削除
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:オブジェクトバージョンの削除
- s3:バケットバージョンのリスト
- s3:リストバケット
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketバージョン管理
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:バイパスガバナンス保持
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

"必要な権限をコピーして貼り付けることができるポリシーの完全なJSON形式を表示します。"。

- Azureの場合:
 - クラスタはONTAP 9.12.1以降を実行している必要があります
 - コンソールエージェントはクラウドまたはオンプレミスに導入できます
- Google Cloud の場合:
 - クラスタはONTAP 9.17.1以降を実行している必要があります
 - コンソールエージェントはクラウドまたはオンプレミスに導入できます

- StorageGRIDの場合:
 - クラスタはONTAP 9.11.1以降を実行している必要があります
 - StorageGRIDシステムは11.6.0.3以降を実行している必要があります
 - コンソール エージェントは、オンプレミスで展開する必要があります (インターネット アクセスの有無にかかわらずサイトにインストールできます)
 - 次の S3 権限は、コンソール エージェントに権限を提供する IAM ロールの一部である必要があります。

StorageGRID S3 権限

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:オブジェクトのタグ付け
- s3:オブジェクトの削除
- s3:オブジェクトのタグ付けを削除
- s3:GetObjectRetention
- s3:オブジェクトバージョンタグ付けの削除
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:オブジェクトバージョンの削除
- s3:バケットバージョンのリスト
- s3:リストバケット
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketバージョン管理
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

制限事項

- バックアップ ポリシーでアーカイブ ストレージを構成している場合、DataLock およびランサムウェア保護機能は使用できません。
- NetApp Backup and Recoveryをアクティブ化するときに選択した DataLock オプションは、そのクラスタのすべてのバックアップ ポリシーに使用する必要があります。
- 単一のクラスタで複数の DataLock モードを使用することはできません。
- DataLock を有効にすると、すべてのボリュームのバックアップがロックされます。1つのクラスタにロックされたボリューム バックアップとロックされていないボリューム バックアップを混在させることはできません。
- DataLock およびランサムウェア保護は、DataLock およびランサムウェア保護が有効になっているバックアップ ポリシーを使用した新しいボリューム バックアップに適用されます。後で「詳細設定」オプションを使用してこれらの機能を有効または無効にすることができます。
- FlexGroupボリュームは、ONTAP 9.13.1 以降を使用している場合にのみ、DataLock およびランサムウェア保護を使用できます。

DataLockのコストを軽減するヒント

DataLock 機能をアクティブにしたまま、ランサムウェア スキャン機能を有効または無効にすることができます。追加料金を回避するには、スケジュールされたランサムウェア スキャンを無効にすることができます。これにより、セキュリティ設定をカスタマイズし、クラウド プロバイダーからのコストの発生を回避できます。

スケジュールされたランサムウェア スキャンが無効になっている場合でも、必要に応じてオンデマンド スキャンを実行できます。

さまざまなレベルの保護を選択できます。

- ランサムウェア スキャンなしの **DataLock**: ガバナンス モードまたはコンプライアンス モードのいずれかの宛先ストレージ内のバックアップ データを保護します。
 - ガバナンス モード: 管理者が保護されたデータを上書きまたは削除する柔軟性を提供します。
 - コンプライアンス モード: 保持期間が終了するまで完全に消去不可能な状態を保ちます。これにより、規制の厳しい環境における最も厳しいデータ セキュリティ要件を満たすことができます。データはライフサイクル中に上書きまたは変更できないため、バックアップ コピーに対して最強レベルの保護が提供されます。



代わりに、Microsoft Azure ではロックおよびロック解除モードが使用されます。

- ランサムウェア スキャン機能を備えた **DataLock**: データのセキュリティをさらに強化します。この機能は、バックアップ コピーを変更しようとする試みを検出するのに役立ちます。何らかの試みが行われた場合、データの新しいバージョンが慎重に作成されます。スキャン頻度は1、2、3、4、5、6、または7日に変更できます。スキャンを7日ごとに設定すると、コストが大幅に削減されます。

DataLockのコストを軽減するためのヒントについては、以下を参照してください。
<https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475>

さらに、DataLockに関連する費用の見積もりは、"[NetApp Backup and Recoveryの総所有コスト \(TCO\) 計算ツール](#)"。

アーカイブ保存オプション

AWS、Azure、または Google クラウド ストレージを使用する場合、一定の日数が経過すると、古いバックアップ ファイルをより安価なアーカイブ ストレージ クラスまたはアクセス層に移動できます。バックアップ ファイルを標準のクラウド ストレージに書き込まずに、すぐにアーカイブ ストレージに送信することも選択できます。バックアップ ファイルをアーカイブ ストレージに直接送信するには、「Archive After Days」に **0** と入力するだけです。これは、クラウド バックアップのデータにアクセスする必要がほとんどないユーザーや、テープ ソリューションへのバックアップを置き換えるユーザーにとって特に役立ちます。

アーカイブ層のデータは必要なときにすぐにアクセスできず、取得コストが高くなります。そのため、バックアップ ファイルをアーカイブするかどうかを決定する前に、バックアップ ファイルからデータを復元する必要がある頻度を考慮する必要があります。



- すべてのデータ ブロックをアーカイブ クラウド ストレージに送信するために「0」を選択した場合でも、メタデータ ブロックは常に標準のクラウド ストレージに書き込まれます。
- DataLock を有効にしている場合は、アーカイブ ストレージは使用できません。
- **0** 日 (すぐにアーカイブ) を選択した後は、アーカイブ ポリシーを変更することはできません。

各バックアップ ポリシーには、バックアップ ファイルに適用できる「アーカイブ ポリシー」のセクションが用意されています。

- AWS では、バックアップは *Standard* ストレージ クラスで開始され、30 日後に *Standard-Infrequent Access* ストレージ クラスに移行します。

クラスターで 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* または *S3 Glacier Deep Archive* ストレージに階層化できます。["AWSアーカイブストレージの詳細"](#)。

- NetApp Backup and Recovery をアクティブ化するときに最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合、将来のポリシーでは *S3 Glacier* が唯一のアーカイブ オプションになります。
 - 最初のバックアップ ポリシーで *S3 Glacier* を選択した場合は、そのクラスターの将来のバックアップ ポリシーを *S3 Glacier Deep Archive* 層に変更できます。
 - 最初のバックアップ ポリシーで *S3 Glacier Deep Archive* を選択した場合、その層はそのクラスターの将来のバックアップ ポリシーで使用できる唯一のアーカイブ層になります。
- Azure では、バックアップは *Cool* アクセス層に関連付けられています。

クラスターで 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 *Azure Archive* ストレージに階層化できます。["Azure アーカイブ ストレージの詳細"](#)。

- GCP では、バックアップは *Standard* ストレージ クラスに関連付けられています。

オンプレミスのクラスターで ONTAP 9.12.1 以降を使用している場合は、コストをさらに最適化するために、一定の日数後に NetApp Backup and Recovery UI で古いバックアップをアーカイブ ストレージに階層化することを選択できます。["Google アーカイブ ストレージの詳細"](#)。

- StorageGRID では、バックアップは *Standard* ストレージ クラスに関連付けられます。

オンプレミスのクラスターで ONTAP 9.12.1 以上を使用しており、StorageGRID システムで 11.4 以上を使用している場合は、古いバックアップ ファイルをパブリック クラウド アーカイブ ストレージにアーカイブできます。

- AWS の場合、AWS 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できます。["AWSアーカイブストレージの詳細"](#)。
- Azure の場合、古いバックアップを Azure Archive ストレージに階層化できます。["Azure アーカイブストレージの詳細"](#)。

NetApp Backup and Recoveryの詳細設定でオブジェクトストレージへのバックアップ オプションを管理する

[詳細設定] ページを使用して、各ONTAPシステムに対してNetApp Backup and Recoveryをアクティブ化するとき設定した、クラスターレベルのオブジェクトへのバックアップストレージ設定を変更できます。「デフォルト」のバックアップ設定として適用されているいくつかの設定を変更することもできます。これには、オブジェクトストレージへのバックアップの転送速度の変更、履歴スナップショットをバックアップファイルとしてエクスポートするかどうか、システムのランサムウェア スキャンの有効化または無効化などが含まれます。



これらの設定は、オブジェクトストレージへのバックアップでのみ使用できます。これらの設定はいずれもスナップショットまたはレプリケーションの設定には影響しません。



NetApp Backup and Recoveryのワークロードを切り替えるには、["さまざまなNetApp Backup and Recoveryワークロードに切り替える"](#)。

詳細設定ページで次のオプションを変更できます。

- ONTAPシステムにオブジェクトストレージへのアクセス権限を与えるストレージキーを変更する
- オブジェクトストレージに接続されているONTAP IPspaceを変更する
- 最大転送速度オプションを使用して、オブジェクトストレージにバックアップをアップロードするために割り当てられたネットワーク帯域幅を変更する
- 履歴スナップショットをバックアップファイルとしてエクスポートし、将来のボリュームの初期ベースラインバックアップファイルに含めるかどうかを変更する
- 「年次」スナップショットをソースシステムから削除するかどうかを変更する
- スケジュールされたスキャンを含む、システムのランサムウェアスキャンを有効または無効にする

クラスターレベルのバックアップ設定を表示する

各システムのクラスターレベルのシステム設定とプロバイダー設定を表示できます。

手順

1. コンソール メニューから、保護 > バックアップとリカバリ を選択します。
2. *ボリューム*タブから*バックアップ設定*を選択します。
3. バックアップ設定ページ から、... システムについては、「詳細設定の構成 > システム設定」を選択してシステム設定を表示し、「詳細設定の構成 > プロバイダー設定」を選択してプロバイダー設定を表示します。

表示されるページには、そのシステムの現在の設定が表示されます。プロバイダー設定を表示する場合、表示されるプロバイダー設定は、ページの上で選択したバケットに関連します。

ソース クラスタ上のONTAPのバージョンと、バックアップが存在するクラウド プロバイダの宛先によっては、一部のオプションが使用できないことに注意してください。

オブジェクトストレージにバックアップをアップロードするために利用できるネットワーク帯域幅を変更する

システムに対してNetApp Backup and Recoveryを有効にすると、デフォルトでは、ONTAPは無制限の帯域幅を使用して、システム内のボリュームからオブジェクト ストレージにバックアップ データを転送できます。バックアップトラフィックが通常のユーザー ワークロードに影響を与えていることに気付いた場合は、[詳細設定] ページの [最大転送速度] オプションを使用して、転送中に使用されるネットワーク帯域幅の量を調整できます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定ページ から、... システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[最大転送速度] セクションを展開します。
4. 最大転送速度として 1 ~ 1,000 Mbps の間の値を選択します。
5. *制限*ラジオ ボタンを選択し、使用できる最大帯域幅を入力するか、*無制限*を選択して制限がないことを示します。
6. *適用*を選択します。

この設定は、システム内のボリュームに対して構成されている可能性のある他のレプリケーション関係に割り当てられる帯域幅には影響しません。

履歴スナップショットをバックアップファイルとしてエクスポートするかどうかを変更する

このシステムで使用しているバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致するボリュームのローカル スナップショットがある場合は、それらの履歴スナップショットをバックアップ ファイルとしてオブジェクト ストレージにエクスポートできます。これにより、古いスナップショットをベースラインバックアップ コピーに移動して、クラウド内のバックアップを初期化できるようになります。

このオプションは、新しい読み取り/書き込みボリュームの新しいバックアップ ファイルにのみ適用され、データ保護 (DP) ボリュームではサポートされないことに注意してください。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定ページ から、... システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[既存のスナップショットのコピーをエクスポート] セクションを展開します。
4. 既存のスナップショットをエクスポートするかどうかを選択します。
5. *適用*を選択します。

「年次」スナップショットをソースシステムから削除するかどうかを変更する

いずれかのボリュームのバックアップポリシーに「年間」バックアップラベルを選択すると、作成されるスナップショットが非常に大きくなります。デフォルトでは、これらの年次スナップショットは、オブジェクトストレージに転送された後、ソースシステムから自動的に削除されます。このデフォルトの動作は、年間スナップショットの削除セクションから変更できます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定ページから、... システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. [詳細設定] ページで、[年次スナップショットの削除] セクションを展開します。
4. ソースシステムに年次スナップショットを保持するには、[無効] を選択します。
5. *適用*を選択します。

ランサムウェアスキャンを有効または無効にする

ランサムウェア保護スキャンはデフォルトで有効になっています。スキャン頻度のデフォルト設定は7日間です。スキャンは最新のスナップショットに対してのみ実行されます。

DataLockとランサムウェア耐性オプションの詳細については、以下を参照してください。"[DataLockとランサムウェア耐性オプション](#)"。

スケジュールを日単位や週単位に変更したり、無効にしたりしてコストを節約できます。



ランサムウェアスキャンを有効にすると、クラウドプロバイダーに応じて追加料金が発生します。

スケジュールされたランサムウェアスキャンが無効になっている場合でも、オンデマンドスキャンを実行することはでき、復元操作中にスキャンが実行されます。

参照"[ポリシーの管理](#)"ランサムウェア検出を実装するポリシーの管理の詳細については、こちらをご覧ください。

システムのランサムウェアスキャンを有効または無効にする

クラスターのランサムウェアスキャンを有効または無効にすることができます。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定ページから、... システムの場合は、[詳細設定の構成 > システム設定] を選択します。
3. 表示されたページで、ランサムウェアスキャンセクションを展開します。
4. *ランサムウェアスキャン*を有効または無効にします。
5. *スケジュールされたランサムウェアスキャン*を選択します。
6. 必要に応じて、毎週のデフォルトスキャンを日ごとまたは週ごとに変更します。

7. スキャンを実行する頻度を日数または週数で設定します。

8. *適用*を選択します。

プロバイダーのランサムウェアスキャンを有効または無効にする

プロバイダー設定ページを使用して、プロバイダー レベルでランサムウェア スキャンを有効または無効にすることができます。このページの設定は、ページの上で選択したバケットに関連しています。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定ページ から、... システムの場合は、[詳細設定の構成] > [プロバイダー設定] を選択します。
3. 表示されたページの上で、設定を変更する必要があるバケットを選択します。
4. *ランサムウェアスキャン*セクションを展開します。
5. *ランサムウェアスキャン*を有効または無効にします。
6. *スケジュールされたランサムウェアスキャン*を選択します。
7. 必要に応じて、毎週のデフォルトスキャンを日ごとまたは週ごとに変更します。
8. スキャンを実行する頻度を日数または週数で設定します。
9. *適用*を選択します。

NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Amazon S3 にバックアップする

Cloud Volumes ONTAPシステムから Amazon S3 へのボリューム データのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を完了します。



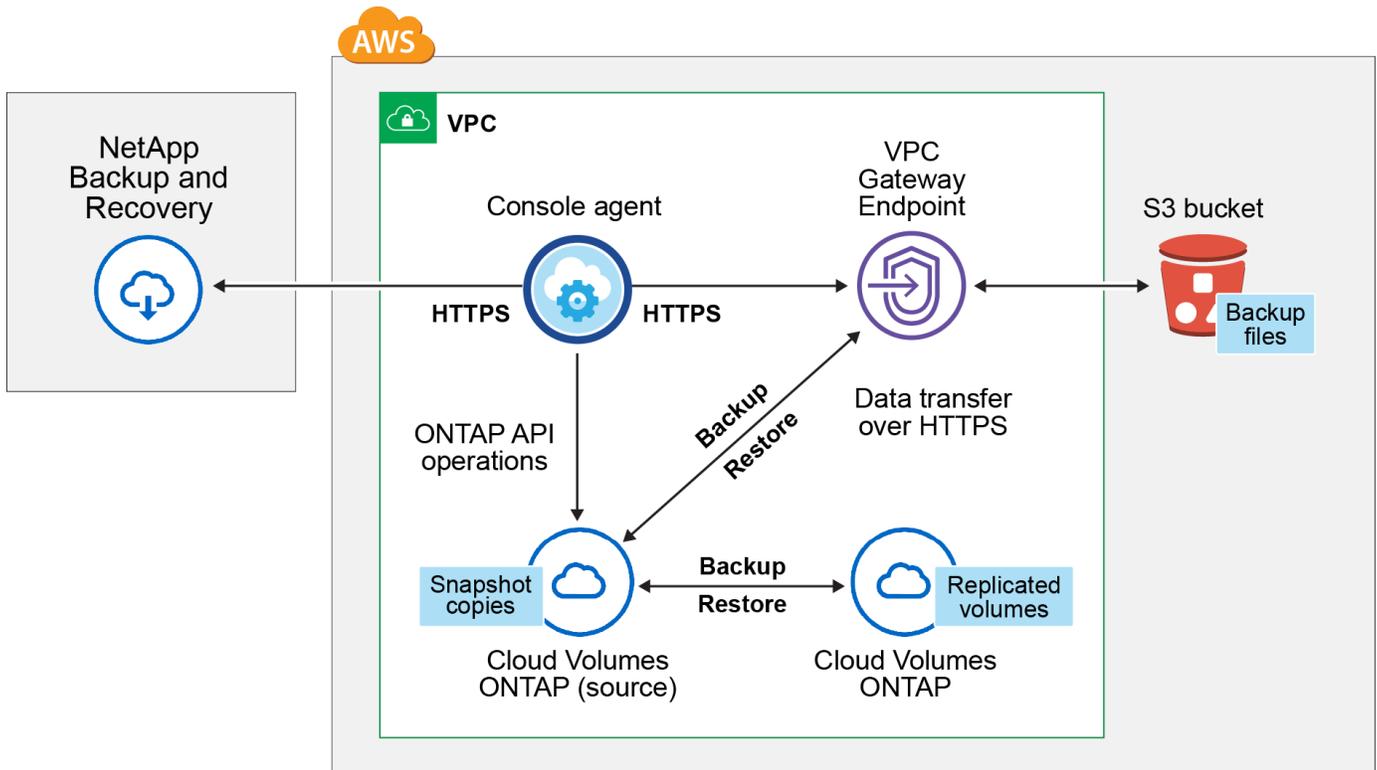
NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

構成のサポートを確認する

ボリュームを S3 にバックアップする前に、次の要件を読んで、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れらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。



VPC ゲートウェイ エンドポイントがすでに VPC 内に存在している必要があります。"[ゲートウェイエンドポイントの詳細](#)"。

サポートされるONTAPバージョン

最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。

データ暗号化に顧客管理キーを使用するために必要な情報

アクティベーションウィザードでは、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マー管理キーを選択できます。この場合、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確認する](#)"。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、Cloud Volumes ONTAPとNetApp Backup and Recoveryの導入を可能にするコンソールサブスクリプションが AWS Marketplace で利用できます。必要がある "[このNetApp Consoleサブスクリプションを購読する](#)"NetApp Backup and Recoveryを有効にする前に、NetApp Backup and Recoveryの課金は、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、"[AWSマーケットプレイスページ](#)"その後 "[サブスクリプションをAWS認証情報に関連付ける](#)"。

Cloud Volumes ONTAPとNetApp Backup and Recoveryをバンドルできる年間契約の場合は、Cloud Volumes ONTAPシステムを作成するとき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。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"[BYOLライセンスの管理方法を学ぶ](#)"。コンソールエージェントとCloud Volumes ONTAPシステムをダーク サイトに展開する場合は、BYOL ライセンスを使用する必要があります。

また、バックアップを保存するストレージスペース用の AWS アカウントも必要です。

コンソールエージェントを準備する

コンソールエージェントは、完全なインターネットアクセスまたは制限されたインターネットアクセス（「標準」または「制限」モード）を備えた AWS リージョンにインストールする必要があります。"[詳細については、NetApp Consoleの展開モードを参照してください。](#)"。

- "[コンソールエージェントについて学ぶ](#)"
- "[AWS にコンソールエージェントを標準モード（フルインターネットアクセス）でデプロイする](#)"
- "[制限モード（送信アクセスが制限される）でコンソール エージェントをインストールする](#)"

コンソールエージェントへの権限を確認または追加する

コンソールに権限を与える IAM ロールには、最新の S3 権限が含まれている必要があります。"[コンソールポリシー](#)"。ポリシーにこれらの権限がすべて含まれていない場合は、"[AWSドキュメント: IAMポリシーの編集](#)"。

ポリシーからの具体的な権限は次のとおりです。

```

{
  "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:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "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-*"
]
}
```



AWS中国リージョンでバックアップを作成する場合、IAMポリシーのすべての `_Resource_` セクションのAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります。例：
`arn:aws-cn:s3:::netapp-backup-*`。

必要なAWS Cloud Volumes ONTAP権限

Cloud Volumes ONTAPシステムがONTAP 9.12.1以降のソフトウェアを実行している場合、そのシステムに権限を提供するIAMロールには、最新のNetApp Backup and Recovery専用の新しいS3権限セットが含まれている必要があります。"[Cloud Volumes ONTAPポリシー](#)"。

コンソールバージョン 3.9.23 以降を使用してCloud Volumes ONTAPシステムを作成した場合、これらの権限はすでにIAMロールの一部になっているはずですが、それ以外の場合は、不足している権限を追加する必要があります。

サポートされているAWSリージョン

NetApp Backup and Recovery は、AWS GovCloud リージョンを含むすべてのAWSリージョンでサポートされています。

別のAWSアカウントでバックアップを作成するために必要な設定

デフォルトでは、バックアップはCloud Volumes ONTAPシステムに使用されているアカウントと同じアカウントを使用して作成されます。バックアップに別のAWSアカウントを使用する場合は、次の手順を実行する必要があります。

- 権限「s3:PutBucketPolicy」と「s3:PutBucketOwnershipControls」が、コンソールエージェントに権限を提供するIAMロールの一部であることを確認します。
- コンソールで宛先AWSアカウントの認証情報を追加します。"[やり方を見る](#)"。
- 2番目のアカウントのユーザー資格情報に次の権限を追加します。

```
"athena:StartQueryExecution",  
"athena:GetQueryResults",  
"athena:GetQueryExecution",  
"glue:GetDatabase",  
"glue:GetTable",  
"glue:CreateTable",  
"glue:CreateDatabase",  
"glue:GetPartitions",  
"glue:BatchCreatePartition",  
"glue:BatchDeletePartition"
```

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

["独自のバケットの作成について詳しくは"](#)。

ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソースシステムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスのONTAPネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスターは、追加のサブネット、ポート、ファイアウォール、およびクラスターの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 ["ONTAPドキュメントでクラスターピアリングの前提条件を確認する"](#)。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする

NetApp Backup and Recoveryを有効にするのは簡単です。既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって、手順が若干異なります。

新しいシステムでNetApp Backup and Recoveryを有効にする

NetApp Backup and Recovery は、システム ウィザードで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。

見る ["AWS でCloud Volumes ONTAP を起動"](#) Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
2. クラウド プロバイダーとして **Amazon Web Services** を選択し、単一ノードまたは 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] を選択します。
5. ウィザードのページを完了してシステムを展開します。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、NetApp Backup and Recoveryを起動し、["保護したいボリュームごとにバックアップを有効化します"](#)。

既存のシステムでNetApp Backup and Recoveryを有効にする

コンソールからいつでも既存のシステムでNetApp Backup and Recoveryを有効にできます。

手順

1. コンソールの システム ページでクラスターを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 を選択します。

バックアップの Amazon S3 保存先が システム ページにクラスターとして存在する場合は、クラスターを Amazon S3 システムにドラッグしてセットアップ ウィザードを開始できます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

バックアップの AWS 保存先がコンソールの [システム] ページにシステムとして存在する場合は、ONTAPクラスターを AWS オブジェクト ストレージにドラッグできます。

- バックアップとリカバリ バーで ボリューム を選択します。ボリュームタブから*アクション*を選択します  アイコン オプションをクリックし、単一ボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていないボリューム) に対して **3-2-1 保護のアクティブ化** を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
 - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

。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をオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは3つすべてが選択されています。
 - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。既存のバケットを選択するか、新しいバケットを構成する場合、クラスターごとに最大6つのバケットにボリュームをバックアップできます。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
 - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。



スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- a. ポリシーの名前を入力します。

b. 通常は異なる頻度のスケジュールを最大 5 つ選択します。

c. *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。

- レプリケーション ターゲット: 宛先システムとストレージ VM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
- レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- i. ポリシーの名前を入力します。
- ii. 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- iii. *作成*を選択します。

5. バックアップ: 次のオプションを設定します。

- プロバイダー: **Amazon Web Services** を選択します。
- プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

バックアップを保存するために使用する AWS アカウントを入力します。これは、Cloud Volumes ONTAPシステムが存在するアカウントとは異なるアカウントにすることができます。

バックアップに別の AWS アカウントを使用する場合は、コンソールでバックアップ先の AWS アカウントの認証情報を追加し、コンソールに権限を付与する IAM ロールに「s3:PutBucketPolicy」および「s3:PutBucketOwnershipControls」権限を追加する必要があります。

バックアップを保存するリージョンを選択します。これは、Cloud Volumes ONTAPシステムが存在するリージョンとは異なるリージョンにすることができます。

新しいバケットを作成するか、既存のバケットを選択します。

- 暗号化: 新しいバケットを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの AWS 暗号化キーを使用するか、AWS アカウントから独自のカスタマー管理キーを選択するかを選択します。 ("[独自の暗号化キーの使用方法を確認する](#)")。

独自のカスタマー管理キーを使用する場合は、キー コンテナとキー情報を入力します。



既存のバケットを選択した場合は、暗号化情報がすでに利用可能であるため、ここで入力する必要はありません。

- ネットワーク: このプロバイダーのネットワーク オプションを構成します。
- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- i. ポリシーの名前を入力します。
- ii. 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- iii. オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLockとランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。
- iv. *作成*を選択します。

◦ 既存のスナップショットをエクスポート: このシステム内のボリュームに、このシステムに対して選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) と一致するローカル スナップショットがある場合、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、ローカル スナップショット、レプリケーション、およびバックアップの不一致なラベルを自動的に修正する チェックボックスをオンにします。これにより、スナップショット、レプリケーション、およびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行

する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用して、Cloud Volumes ONTAPデータを Azure Blob ストレージにバックアップします。

Cloud Volumes ONTAPシステムから Azure Blob ストレージへのボリュームデータのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を実行します。



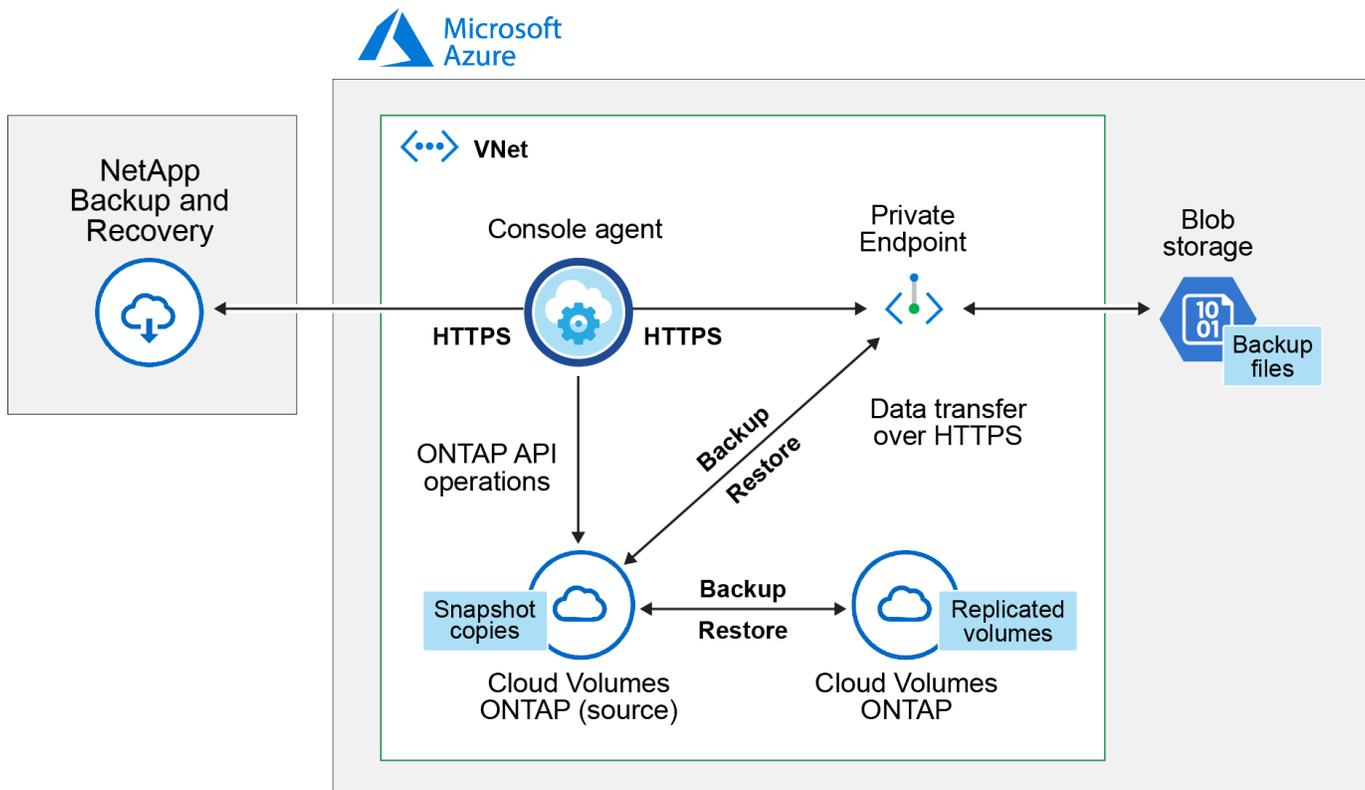
NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

構成のサポートを確認する

ボリュームを Azure Blob ストレージにバックアップする前に、次の要件を読んで、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れらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。



サポートされるONTAPバージョン

最低でもONTAP 9.8、ONTAP 9.8P13以降が推奨されます。

サポートされているAzureリージョン

NetApp Backup and Recovery は、Azure Government リージョンを含むすべての Azure リージョンでサポートされています。

デフォルトでは、NetApp Backup and Recovery はコストの最適化のためにローカル冗長性 (LRS) を使用して BLOB コンテナをプロビジョニングします。異なるゾーン間でデータが確実に複製されるようにしたい場合は、NetApp Backup and Recovery をアクティブ化した後、この設定をゾーン冗長 (ZRS) に変更できます。Microsoftの指示を参照してください "[ストレージアカウントの複製方法を変更する](#)"。

別の Azure サブスクリプションにバックアップを作成するために必要な設定

デフォルトでは、バックアップはCloud Volumes ONTAPシステムに使用されているものと同じサブスクリプションを使用して作成されます。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、NetApp Backup and Recoveryを有効にする前に、Azure Marketplace 経由のサブスクリプションが必要です。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。"[システムウィザードの詳細と資格情報ページからサブスクライブできます](#)"。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"[BYOLライセンスの管理方法を学ぶ](#)"。コンソールエージェントとCloud Volumes ONTAPシステムをダーク サイト (「プライベート モード」) に展開する場合は、BYOL ライセンスを使用する必要があります。

また、バックアップを保存するストレージ スペース用の Microsoft Azure サブスクリプションが必要です。

コンソールエージェントを準備する

コンソール エージェントは、完全なインターネット アクセスまたは制限されたインターネット アクセス (「標準」または「制限」モード) を備えた Azure リージョンにインストールできます。"[詳細については、NetApp Consoleの展開モードを参照してください](#)。"。

- "[コンソールエージェントについて学ぶ](#)"
- "[Azure にコンソール エージェントを標準モード \(完全なインターネット アクセス\) でデプロイする](#)"
- "[制限モード \(送信アクセスが制限される\) でコンソール エージェントをインストールする](#)"

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の検索と復元機能を使用するには、Azure Synapse ワークスペースと Data Lake ストレージ アカウントにアクセスできるように、コンソール エージェントのロールに特定のアクセス許可が必要です。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ってください。

開始する前に

- Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。"[このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください](#)"。リソース プロバイダーを登録するには、サブスクリプションの所有者または投稿者 であ

る必要があります。

- コンソール エージェントと Azure Synapse SQL サービス間の通信には、ポート 1433 が開いている必要があります。

手順

1. コンソール エージェント仮想マシンに割り当てられたロールを識別します。
 - a. Azure ポータルで、仮想マシン サービスを開きます。
 - b. コンソール エージェント仮想マシンを選択します。
 - c. [設定] で、[ID] を選択します。
 - d. *Azure ロールの割り当て*を選択します。
 - e. コンソール エージェント仮想マシンに割り当てられたカスタム ロールをメモします。
2. カスタム ロールを更新します。
 - a. Azure ポータルで、Azure サブスクリプションを開きます。
 - b. *アクセス制御 (IAM) > ロール*を選択します。
 - c. カスタム ロールの省略記号 (...) を選択し、[編集] を選択します。
 - d. **JSON** を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全なJSON形式を表示する"

- e. *確認+更新*を選択し、*更新*を選択します。

データ暗号化に顧客管理キーを使用するために必要な情報

アクティベーション ウィザードでは、既定の Microsoft 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータの暗号化に使用できます。この場合、Azure サブスクリプション、Key Vault 名、およびキーが必要になります。"[独自のキーの使用方法を確認する](#)"。

NetApp Backup and Recoveryは、Azureアクセスポリシー、Azureロールベースアクセス制御 (Azure RBAC) 権限モデル、および_マネージドハードウェアセキュリティモデル_ (HSM) をサポートしています ("[Azure Key Vault Managed HSM とは何ですか?](#)")。

Azure Blob ストレージ アカウントを作成する

デフォルトでは、サービスによってストレージ アカウントが作成されます。独自のストレージ アカウントを使用する場合は、バックアップ アクティベーションウィザードを開始する前にストレージ アカウントを作成し、ウィザードでそれらのストレージ アカウントを選択できます。

"[独自のストレージアカウントの作成について詳しくは、こちらをご覧ください。](#)"。

ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスのONTAPネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスターは、追加のサブネット、ポート、ファイアウォール、およびクラスターの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。"[ONTAPドキュメントでクラスターピアリングの前提条件を確認する](#)"。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする

NetApp Backup and Recoveryを有効にするのは簡単です。既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって、手順が若干異なります。

新しいシステムでNetApp Backup and Recoveryを有効にする

NetApp Backup and Recovery は、システム ウィザードで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。

見る ["Azure でCloud Volumes ONTAP を起動する"](#) Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。



リソース グループの名前を選択する場合は、Cloud Volumes ONTAPをデプロイするときにNetApp Backup and Recovery を無効にします。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
2. クラウド プロバイダーとして **Microsoft Azure** を選択し、単一ノードまたは HA システムを選択します。
3. [Azure 資格情報の定義] ページで、資格情報の名前、クライアント ID、クライアント シークレット、ディレクトリ ID を入力し、[続行] を選択します。
4. [詳細と資格情報] ページに入力し、Azure Marketplace サブスクリプションが設定されていることを確認して、[続行] を選択します。
5. [サービス] ページで、サービスを有効のままにして、[続行] を選択します。
6. ウィザードのページを完了してシステムを展開します。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、NetApp Backup and Recoveryを起動し、["保護したいボリュームごとにバックアップを有効化します"](#)。

既存のシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recoveryをいつでもシステムから直接有効にできます。

手順

1. コンソールの システム ページでシステムを選択し、右側のパネルの [バックアップとリカバリ] の横にある **有効** を選択します。

バックアップの Azure Blob 保存先がコンソールの システム ページにシステムとして存在する場合は、クラスターを Azure Blob システムにドラッグしてセットアップ ウィザードを開始できます。
2. ウィザードのページを完了して、NetApp Backup and Recoveryを展開します。
3. バックアップを開始する場合は、[ONTAPボリューム上のバックアップをアクティブ化する](#)。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップア

クティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。

バックアップの Azure 保存先が **Systems** ページにシステムとして存在する場合は、ONTAP クラスタを Azure Blob オブジェクト ストレージにドラッグできます。

- バックアップとリカバリ バーで ボリューム を選択します。ボリュームタブから*アクション*を選択します **...** アイコンをクリックし、単一ボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない) の [バックアップのアクティブ化]* を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーのうち 1 つ以上を持つボリュームです。

FlexVol または FlexGroup ボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVol または FlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つの FlexGroup ボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じ SnapLock 設定が必要です。すべてのボリュームで SnapLock Enterprise を有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
 - 最初のボリュームを選択したら、すべての FlexVol ボリュームを選択できます。(FlexGroup ボリュームは一度に 1 つだけ選択できます。) 既存の FlexVol ボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

◦ 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をオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてが必要な場合
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは3つすべてが選択されています。
 - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
 - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいスナップショットポリシーを作成します。



スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。

- *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。

- レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
- レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。



レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: **Microsoft Azure** を選択します。
- プロバイダー設定: プロバイダーの詳細を入力します。

バックアップを保存するリージョンを入力します。これは、Cloud Volumes ONTAPシステムが存在するリージョンとは異なるリージョンにすることができます。

新しいストレージ アカウントを作成するか、既存のストレージ アカウントを選択します。

バックアップを保存するために使用する Azure サブスクリプションを入力します。これは、Cloud Volumes ONTAPシステムが存在するサブスクリプションとは異なるサブスクリプションにすることができます。

Blob コンテナを管理する独自のリソース グループを作成するか、リソース グループの種類とグループを選択します。



バックアップ ファイルが変更されたり削除されたりするのを防ぐには、30 日間の保持期間を使用して不変ストレージが有効になっているストレージ アカウントが作成されていることを確認してください。

- 暗号化キー: 新しい Azure ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、既定の Azure 暗号化キーを使用するか、Azure アカウントから独自のカスタマー管理キーを選択するかを選択します。

独自のカスタマー管理キーを使用する場合は、キー コンテナとキー情報を入力します。"[独自のキーの使い方を学ぶ](#)"。



既存の Microsoft ストレージ アカウントを選択した場合は、暗号化情報が既に用意されているため、ここで入力する必要はありません。

- ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。

プライベート エンドポイントはデフォルトで無効になっています。

- i. バックアップするボリュームが存在する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 インターネット アクセスが必要です。
 - ii. 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。"[Azure プライベート エンドポイントの使用について学習します](#)"。
- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLockとランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - *作成*を選択します。
- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。
6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ボリュームと同期されます。

入力したリソース グループに BLOB ストレージ コンテナが作成され、そこにバックアップ ファイルが保存されます。

デフォルトでは、NetApp Backup and Recovery はコストの最適化のためにローカル冗長性 (LRS) を使用して BLOB コンテナをプロビジョニングします。異なるゾーン間でデータが複製されるようにしたい場合は、この設定をゾーン冗長性 (ZRS) に変更できます。Microsoftの指示を参照してください ["ストレージアカウントの複製方法を変更する"](#)。

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。

バックアップと復元ジョブのステータスを監視することもできます。 ["ジョブ監視ページ"](#)。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

次の手順

- あなたはできる ["バックアップファイルとバックアップポリシーを管理する"](#)。これには、バックアップの開始と停止、バックアップの削除、バックアップ スケジュールの追加と変更などが含まれます。
- あなたはできる ["クラスタレベルのバックアップ設定を管理する"](#)。これには、ONTAPがクラウドストレージにアクセスするために使用するストレージ キーの変更、オブジェクトストレージへのバックアップのアップロードに使用できるネットワーク帯域幅の変更、将来のボリュームの自動バックアップ設定の変更などが含まれます。
- また、 ["バックアップ ファイルからボリューム、フォルダ、または個々のファイルを復元する"](#) AWS のCloud Volumes ONTAPシステム、またはオンプレミスのONTAPシステムに接続します。

NetApp Backup and Recoveryを使用してCloud Volumes ONTAPデータを Google Cloud Storage にバックアップする

Cloud Volumes ONTAPシステムから Google Cloud Storage へのボリューム データのバックアップを開始するには、NetApp Backup and Recoveryでいくつかの手順を完了します。



NetApp Backup and Recoveryのワークロードを切り替えるには、 ["さまざまなNetApp Backup and Recoveryワークロードに切り替える"](#)。

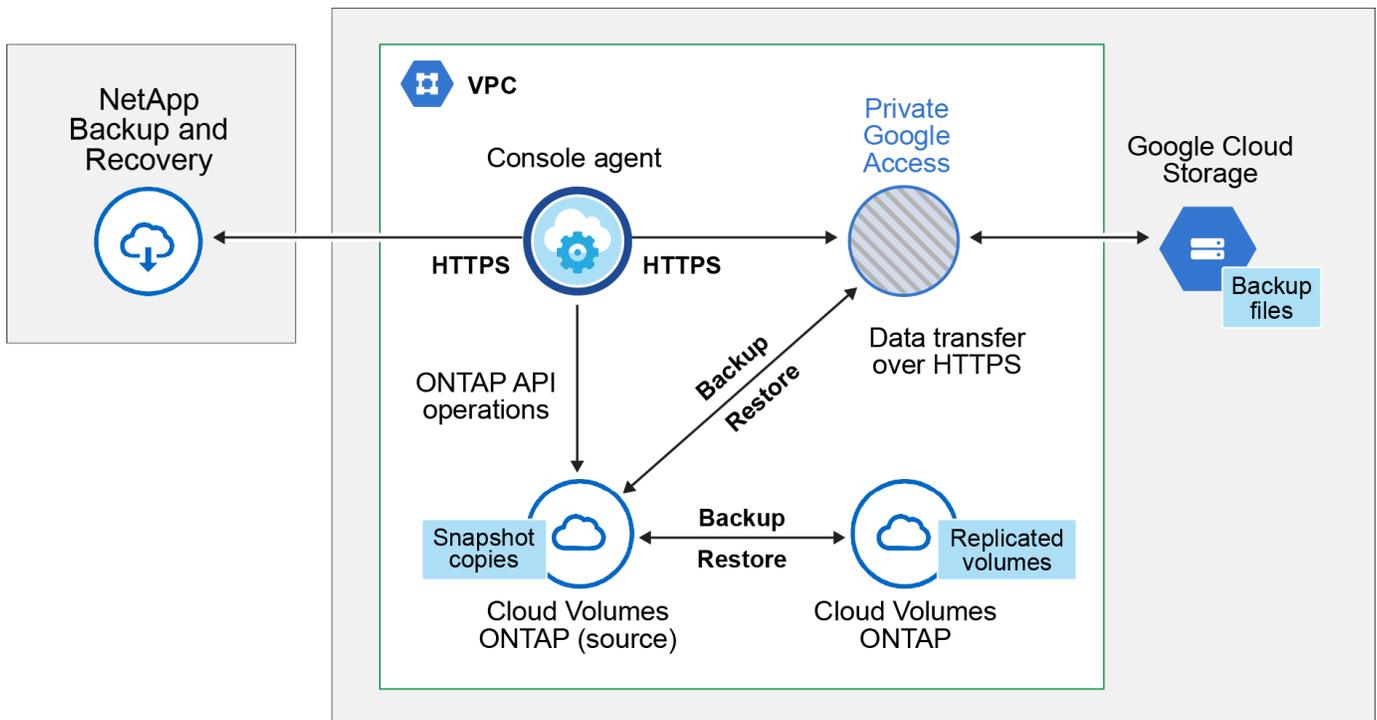
構成のサポートを確認する

Google Cloud Storage へのボリュームのバックアップを開始する前に、次の要件を読んで、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れらの間で準備する必要がある接続を示しています。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダ

りONTAPシステムに接続することもできます。



サポートされるONTAPバージョン

最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。

サポートされているGCPリージョン

NetApp Backup and Recoveryは、すべてのGCPリージョンでサポートされています。

GCP サービス アカウント

Google Cloud プロジェクトにカスタムロールを持つサービス アカウントが必要です。"[サービスアカウントの作成方法を学ぶ](#)"。



NetApp Backup and Recovery がGoogle Cloud Storage バケットにアクセスできるようにするサービス アカウントには、ストレージ管理者のロールは不要になりました。

ライセンス要件を確認する

NetApp Backup and Recovery PAYGO ライセンスの場合、Cloud Volumes ONTAPとNetApp Backup and Recoveryの導入を可能にするコンソール サブスクリプションが Google Marketplace で利用できます。必要がある "[このコンソールサブスクリプションを購読する](#)"NetApp Backup and Recoveryを有効にする前に。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。"[システムウィザードの詳細と資格情報ページからサブスクライブできます](#)"。

NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要です。"[BYOLライセンスの管理方法を学ぶ](#)"。

また、バックアップを保存する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。

コンソールエージェントを準備する

コンソール エージェントは、インターネットにアクセスできる Google リージョンにインストールする必要があります。

- ["コンソールエージェントについて学ぶ"](#)
- ["Google Cloud にコンソール エージェントをデプロイする"](#)

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の「検索と復元」機能を使用するには、Google Cloud BigQuery サービスにアクセスできるように、コンソール エージェントのロールに特定の権限が必要です。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ってください。

手順

1. の中で ["Google Cloud コンソール"](#)、*役割*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 ロールを選択します。
4. ロールの権限を更新するには、「ロールの編集」を選択します。
5. 次の新しい権限をロールに追加するには、「権限の追加」を選択します。

```
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. 編集したロールを保存するには、[更新] を選択します。

顧客管理暗号鍵 (CMEK) の使用に必要な情報

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。"[顧客管理暗号化キーの詳細](#)"。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認する必要があります。参照 ["Google Cloud ドキュメント: API の有効化"](#) 詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

["独自のバケットの作成について詳しくは"](#)。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスタがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 ["ONTAPドキュメントでクラスタピアリングの前提条件を確認する"](#)。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。
- 異なるサブネットにある 2 つのCloud Volumes ONTAPシステム間でデータを複製するには、サブネットを一緒にルーティングする必要があります (これがデフォルト設定です)。

Cloud Volumes ONTAPでNetApp Backup and Recoveryを有効にする

NetApp Backup and Recoveryを有効にする手順は、既存のCloud Volumes ONTAPシステムがあるか、新しいシステムがあるかによって若干異なります。

新しいシステムでNetApp Backup and Recoveryを有効にする

システム ウィザードを完了して新しいCloud Volumes ONTAPシステムを作成すると、NetApp Backup and Recovery を有効にできます。

サービス アカウントがすでに構成されている必要があります。Cloud Volumes ONTAPシステムを作成するときにサービス アカウントを選択しない場合は、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。

見る "[GCP でCloud Volumes ONTAP を起動](#)"Cloud Volumes ONTAPシステムを作成するための要件と詳細については、こちらをご覧ください。

手順

1. コンソールの システム ページで、システムの追加 を選択し、クラウド プロバイダーを選択して、新規追加 を選択します。 * Cloud Volumes ONTAPの作成*を選択します。
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高可用性) を選択します。
4. 詳細と資格情報: 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 (コンソール エージェントが存在するプロジェクト) と異なる場合は、[プロジェクトの編集] 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. 資格情報を指定します。

GCP Marketplace サブスクリプションが設定されていることを確認します。

5. サービス: NetApp Backup and Recovery を有効のままにして、[続行] をクリックします。
6. ウィザードのページを完了して、説明に従ってシステムを展開します。 "[GCP でCloud Volumes ONTAP を起動](#)"。

結果

システムでNetApp Backup and Recovery が有効になっています。これらのCloud Volumes ONTAPシステムでボリュームを作成したら、NetApp Backup and Recoveryを起動し、"[保護したいボリュームごとにバックアップを有効化します](#)"。

既存のシステムで**NetApp Backup and Recovery**を有効にする

NetApp Backup and Recovery は、いつでもシステムから直接有効にすることができます。

手順

1. コンソールの システム ページでシステムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効 を選択します。

バックアップの Google Cloud Storage 保存先がコンソールの [システム] ページにシステムとして存在する場合は、クラスタを Google Cloud Storage システムにドラッグしてセットアップ ウィザードを開始できます。

Google Cloud Storage をバックアップ先として準備する

Google Cloud Storage をバックアップ ターゲットとして準備するには、次の手順を実行します。

- 権限を設定します。
- (オプション) 独自のバケットを作成します。(必要に応じて、サービスによってバケットが作成されません。)
- (オプション) データ暗号化用の顧客管理キーを設定する

権限を設定する

カスタム ロールを使用して特定の権限を持つサービス アカウントにストレージ アクセス キーを提供する必要があります。サービス アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用される Cloud Storage バケットを認証してアクセスできるようになります。Google Cloud Storage が誰がリクエストを行っているかを認識するために、キーが必要になります。

手順

1. の中で ["Google Cloud コンソール"](#)、[*役割*](#)ページに移動します。
2. ["新しいロールの作成"](#)以下の権限を持ちます:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloudコンソールでは、["サービスアカウントページに移動します"](#)。

4. Cloud プロジェクトを選択します。
5. サービス アカウントの作成 を選択し、必要な情報を入力します。
 - a. サービス アカウントの詳細: 名前と説明を入力します。
 - b. このサービス アカウントにプロジェクトへのアクセスを許可する: 先ほど作成したカスタム ロールを選択します。
 - c. *完了*を選択します。
6. へ移動 ["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、*相互運用性*を選択します。まだ行っていない場合は、[相互運用性アクセスを有効にする]を選択します。
 - b. サービス アカウントのアクセス キー の下で、サービス アカウントのキーの作成 を選択し、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。

後でバックアップ サービスを構成するときに、NetApp Backup and Recoveryにキーを入力する必要があります。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

["独自のバケットの作成について詳しくは"](#)。

データ暗号化用の顧客管理暗号鍵 (CMEK) を設定する

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。

独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。 ["顧客管理暗号化キーの詳細"](#)。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認

する必要があります。参照 ["Google Cloud ドキュメント: API の有効化"](#)詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。

- コンソールの [システム ページ*](#) からシステムを選択し、右側のパネルの [\[バックアップとリカバリ\]](#) の横にある [有効化 > バックアップ ボリューム](#) を選択します。

バックアップの GCP 保存先がコンソールの [システム ページ](#)にシステムとして存在する場合は、ONTAPクラスターを GCP オブジェクト ストレージにドラッグできます。

- [バックアップとリカバリ](#) バーで [ボリューム](#) を選択します。ボリュームタブから[*アクション*](#)を選択します [***](#) アイコンをクリックし、単一ボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない) の [\[バックアップのアクティブ化\]*](#) を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。 [*次へ*](#) を選択してください。
- コンソール エージェントがまだない場合は、[\[コンソール エージェントの追加\]](#) オプションが表示されます。参照 [\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」 ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
 - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
 - 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をオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。

- ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
- カスケード: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてセカンダリ ストレージ システムからオブジェクト ストレージへ流れます。
 - ファンアウト: 情報はプライマリ ストレージ システムからセカンダリ ストレージ システムへ、そしてプライマリ ストレージ システムからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいスナップショット ポリシーを作成します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - オブジェクトへのバックアップ ポリシーの場合は、Datalock と Ransomware Resilience を構成します。データロックとランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。
 - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
- レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
 - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。



レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - *作成*を選択します。
5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。
- プロバイダー: **Google Cloud** を選択します。

- プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

新しいバケットを作成するか、既存のバケットを選択します。

- 暗号化キー: 新しい Google バケットを作成した場合は、プロバイダから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Google Cloud 暗号化キーを使用するか、Google アカウントから独自の顧客管理キーを選択するかを選択します。

独自のカスタマー管理キーを使用する場合は、キー コンテナとキー情報を入力します。



既存の Google Cloud バケットを選択した場合は、暗号化情報がすでに利用可能であるため、今すぐ入力する必要はありません。

- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。
- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリストレージシステムボリュームと同期されます。

入力した Google アクセスキーとシークレットキーで示されるサービス アカウントに Google Cloud Storage バケットが作成され、そこにバックアップ ファイルが保存されます。

デフォルトでは、バックアップは *Standard* ストレージ クラスに関連付けられます。低コストの *Nearline*、*Coldline*、または *Archive* ストレージ クラスを使用できます。ただし、ストレージ クラスは、NetApp Backup and Recovery UI ではなく、Google を通じて構成します。Google トピックを見る "[バケットのデフォルトのストレージ クラスを変更する](#)" 詳細については。

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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

API コマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

次の手順

- あなたはできる"[バックアップファイルとバックアップポリシーを管理する](#)"。これには、バックアップの開始と停止、バックアップの削除、バックアップ スケジュールの追加と変更などが含まれます。
- あなたはできる"[クラスタレベルのバックアップ設定を管理する](#)"。これには、ONTAPがクラウドストレージにアクセスするために使用するストレージ キーの変更、オブジェクトストレージへのバックアップのアップロードに使用できるネットワーク帯域幅の変更、将来のボリュームの自動バックアップ設定の変更などが含まれます。
- また、"[バックアップファイルからボリューム、フォルダ、または個々のファイルを復元する](#)" AWS の Cloud Volumes ONTAP システム、またはオンプレミスの ONTAP システムに接続します。

NetApp Backup and Recovery を使用してオンプレミスの ONTAP データを Amazon S3 にバックアップする

NetApp Backup and Recovery でいくつかの手順を完了して、オンプレミスの ONTAP システムからセカンダリ ストレージ システムと Amazon S3 クラウド ストレージへのボリューム データのバックアップを開始します。



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



NetApp Backup and Recovery のワークロードを切り替えるには、"[さまざまな NetApp Backup and Recovery ワークロードに切り替える](#)"。

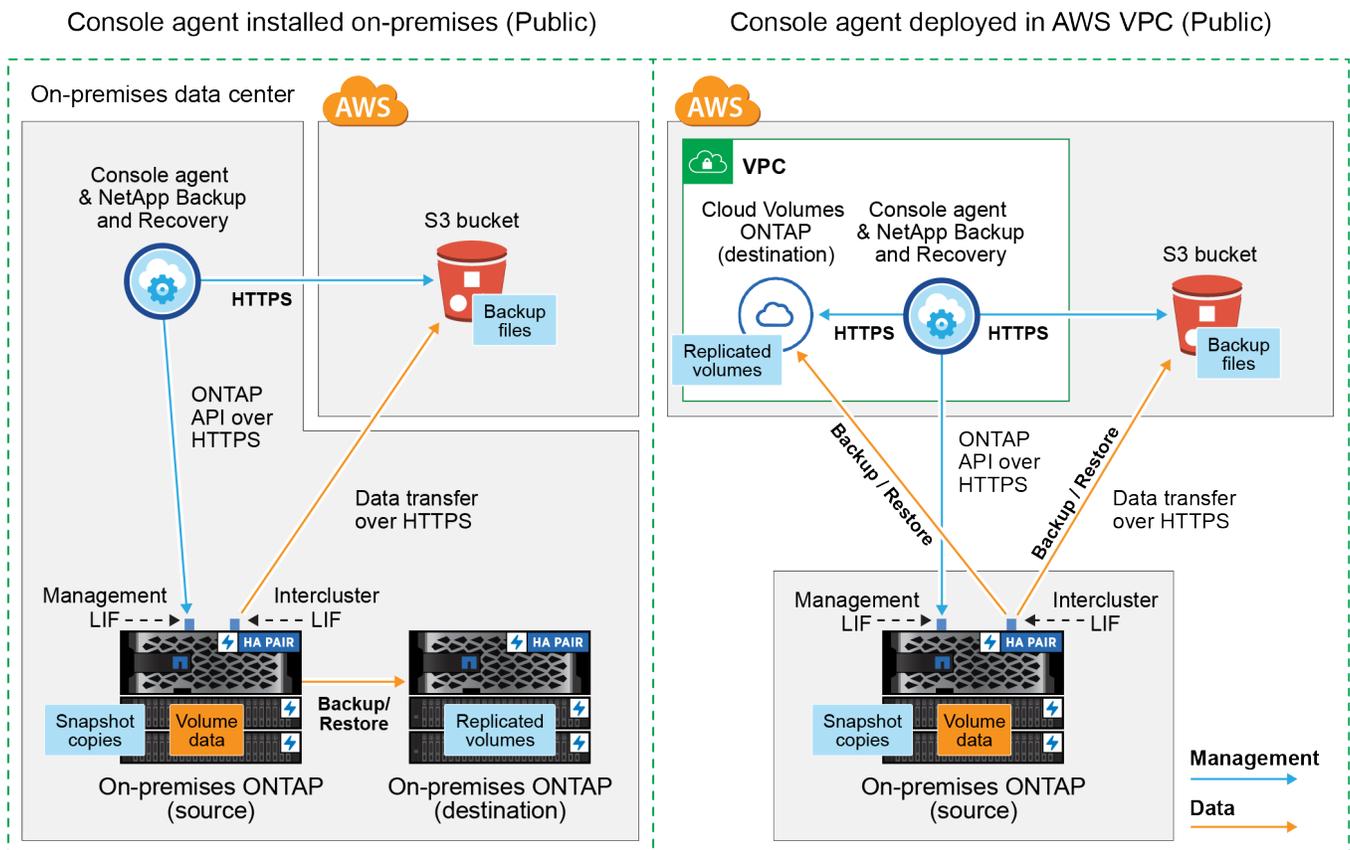
接続方法を特定する

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構成するとき使用する 2 つの接続方法のうちどちらを選択します。

- 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、プライベート IP アドレスを使用する VPC エンドポイント インターフェイスを介してトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリ ONTAPシステムに接続することもできます。

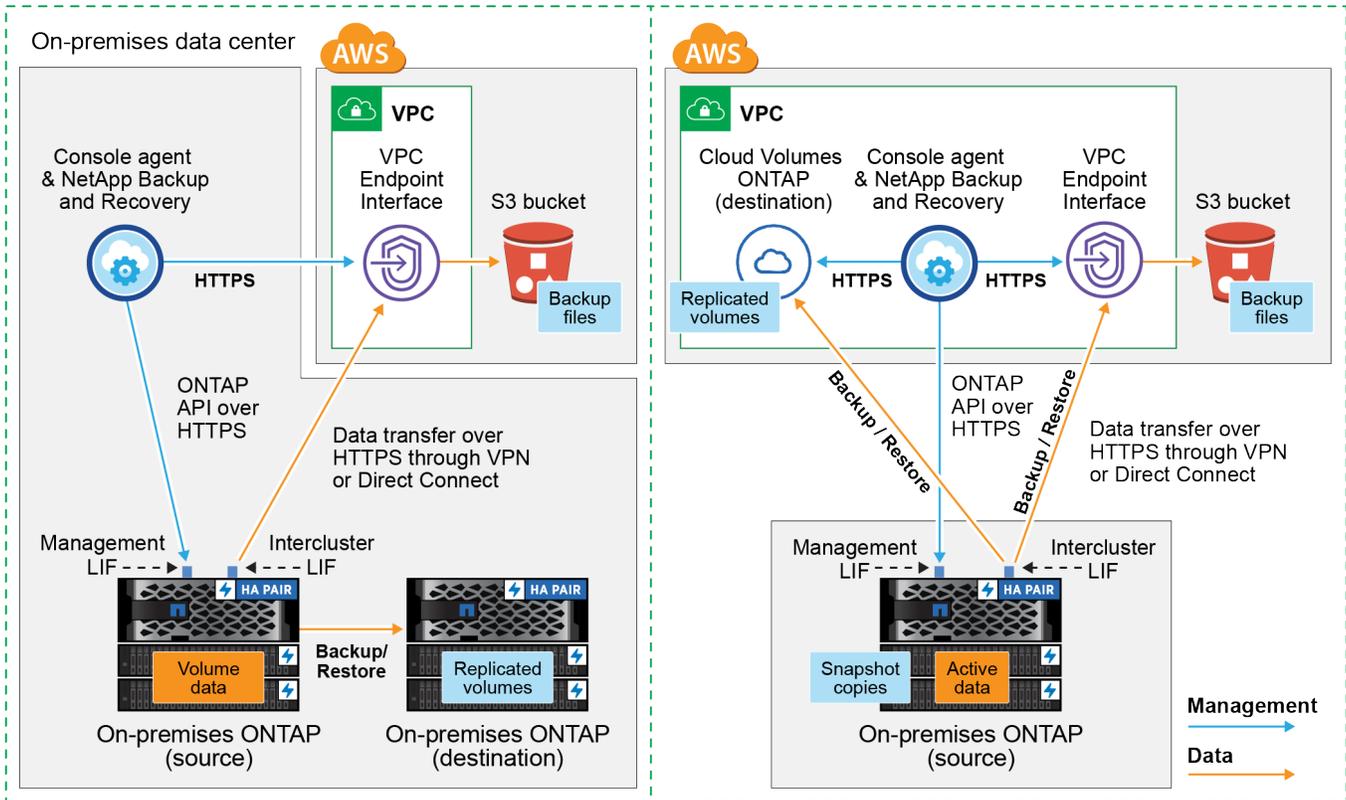
次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソールエージェント、または AWS VPC にデプロイしたコンソールエージェントを使用できます。



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソールエージェント、または AWS VPC にデプロイしたコンソールエージェントを使用できます。

Console agent installed on-premises (Private)

Console agent deployed in AWS VPC (Private)



コンソールエージェントを準備する

コンソール エージェントは、NetApp Console機能のメインソフトウェアです。ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

AWS VPC またはオンプレミスにコンソールエージェントがすでにデプロイされている場合は、準備は完了です。

そうでない場合は、ONTAPデータをAWS S3ストレージにバックアップするために、これらの場所のいずれかにコンソールエージェントを作成する必要があります。別のクラウドプロバイダーにデプロイされたコンソール エージェントは使用できません。

- ["コンソールエージェントについて学ぶ"](#)
- ["AWSにコンソールエージェントをインストールする"](#)
- ["オンプレミスにコンソールエージェントをインストールする"](#)
- ["AWS GovCloud リージョンにコンソールエージェントをインストールする"](#)

NetApp Backup and Recovery は、コンソール エージェントがオンプレミスでインストールされている場合ではなく、クラウドに展開されている場合に、GovCloud リージョンでサポートされます。さらに、AWS Marketplace からコンソールエージェントをデプロイする必要があります。NetApp Console SaaS Web サイトからコンソール エージェントを政府地域に展開することはできません。

コンソールエージェントのネットワーク要件を準備する

次のネットワーク要件が満たされていることを確認してください。

- コンソール エージェントがインストールさ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経由のNetApp Backup and Recovery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見る"](#))
 - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
 - AWS および AWS GovCloud のデプロイメントには、追加の受信および送信セキュリティ グループ ルールが必要です。見る ["AWS のコンソールエージェントのルール"](#)詳細については。
- ONTAPクラスタから VPC への Direct Connect または VPN 接続があり、コンソール エージェントと S3 間の通信を AWS 内部ネットワーク (プライベート接続) 内に維持したい場合は、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 インターフェイスを使用してシステムをプライベート接続用に設定する](#)。

ライセンス要件を確認する

AWS とNetApp Consoleの両方のライセンス要件を確認する必要があります。

- クラスタでNetApp Backup and Recoveryを有効にする前に、AWS の従量課金制 (PAYGO) NetApp Console Marketplace オファリングに登録するか、NetAppからNetApp Backup and Recovery BYOL ライセンスを購入して有効にする必要があります。これらのライセンスはあなたのアカウント用であり、複数のシステムで使用できません。
 - NetApp Backup and Recovery PAYGOライセンスの場合は、["AWS Marketplace からのNetApp Consoleの提供"](#)。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
 - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要になります。
- バックアップが保存されるオブジェクト 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。

サポート対象地域

AWS GovCloud リージョンを含む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。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。 <https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["クラスターの検出方法を学ぶ"]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ "[クラスターライセンスを管理する](#)"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "[クラスター時間を設定する](#)"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

"[SnapMirror関係に互換性のあるONTAPバージョンを表示する](#)"。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- クラスタでは、コンソール エージェントからクラスタ管理 LIF への受信 HTTPS 接続が必要です。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。これらのクラスタ間 LIF はオブジェクト ストアにアクセスできる必要があります。

クラスターは、バックアップおよび復元操作のために、クラスター間 LIF から Amazon S3 ストレージへのポート 443 経由の送信 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 ストレージは開始することなく、応答するだけです。

- クラスタ間 LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。 "[IPspacesについて詳しくはこちら](#)"。

NetApp Backup and Recoveryをセットアップするときに、使用する *IPspace* の入力を求められます。これらの LIF が関連付けられている *IPspace* を選択する必要があります。これは、「デフォルト」の *IPspace* の場合もあれば、作成したカスタム *IPspace* の場合もあります。

「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 ストレージにアクセスするために静的ルートを作成する必要がある場合があります。

IPspace 内のすべてのクラスタ間 LIF はオブジェクト ストアにアクセスできる必要があります。現在の IPspace に対してこれを構成できない場合は、すべてのクラスタ間 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ストレージ VM に対して DNS サーバーが設定されている必要があります。方法を見る ["SVMのDNSサービスを構成する"](#)。
- 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NetApp Backup and Recovery接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。
- S3 接続に AWS のプライベート 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 インターフェイスを使用してシステムをプライベート接続用に設定する](#)。
- ONTAPクラスターに S3 バケットにアクセスする権限があることを確認します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスタがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 ["ONTAPドキュメントでクラスタピアリングの前提条件を確認する"](#)。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Amazon S3をバックアップターゲットとして準備する

Amazon S3 をバックアップターゲットとして準備するには、次の手順を実行します。

- S3 権限を設定します。
- (オプション) 独自の S3 バケットを作成します。 (必要に応じて、サービスによってバケットが作成されません。)
- (オプション) データ暗号化用にカスタマー管理の AWS キーを設定します。
- (オプション) VPC エンドポイント インターフェイスを使用して、システムをプライベート接続用に設定します。

S3の権限を設定する

次の2セットの権限を構成する必要があります。

- コンソール エージェントが S3 バケットを作成および管理するための権限。
- オンプレミスのONTAPクラスターが S3 バケットのデータの読み取りと書き込みを行えるようにするための権限。

手順

1. コンソール エージェントに必要な権限があることを確認します。詳細については、"[NetApp Consoleポリシー権限](#)"。



AWS中国リージョンでバックアップを作成する場合、IAMポリシーのすべての `_Resource_` セクションのAWSリソース名「arn」を「aws」から「aws-cn」に変更する必要があります。例： `arn:aws-cn:s3:::netapp-backup-*`。

2. サービスをアクティブ化すると、バックアップ ウィザードによってアクセス キーとシークレット キーの入力が求められます。これらの認証情報はONTAPクラスターに渡され、ONTAP はS3 バケットにデータをバックアップおよび復元できるようになります。そのためには、次の権限を持つ IAM ユーザーを作成する必要があります。

参照 "[AWS ドキュメント: IAM ユーザーに権限を委任するロールの作成](#)"。

```

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

```

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

"独自のバケットの作成について詳しくは"。

独自のバケットを作成する場合は、「netapp-backup」というバケット名を使用する必要があります。カスタム名を使用する必要がある場合は、`ontapcloud-instance-policy-netapp-backup` 既存のCVOのIAMRoleを作成し、次のJSONブロックをS3権限に追加します。`Statement` 配列。含める必要がある `"Resource": "arn:aws:s3:::*"` バケットに関連付ける必要のあるすべての必要な権限を割り当てます。

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

データ暗号化用の顧客管理 **AWS** キーを設定する

デフォルトの Amazon S3 暗号化キーを使用してオンプレミスのクラスターと S3 バケット間で渡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、すべて準備完了です。

代わりに、デフォルトのキーではなく、独自の顧客管理キーを使用してデータを暗号化する場合は、NetApp Backup and Recoveryウィザードを開始する前に、暗号化管理キーを事前に設定しておく必要があります。

"Cloud Volumes ONTAPで独自のAmazon暗号化キーを使用する方法を参照してください。"。

"NetApp Backup and Recoveryで独自のAmazon暗号化キーを使用する方法を参照してください。"。

VPC エンドポイント インターフェースを使用してシステムをプライベート接続用に設定する

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、すべての権限がコンソール エージェントによって設定されるため、他に何もする必要はありません。

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経由のより安全な接続を確立したい場合は、バックアップアクティベーションウィザードで AWS PrivateLink 接続を選択するオプションがあります。プライベート IP アドレスを使用する VPC エンドポイント インターフェースを介してオンプレミス システムに接続するために VPN または AWS Direct Connect を使用する予定の場合は、これが必要です。

手順

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。"[Amazon S3 の AWS PrivateLink の使用に関する詳細については、こちらをご覧ください。](#)"。
2. コンソール エージェントに関連付けられているセキュリティ グループ構成を変更します。ポリシーを「カスタム」（「フルアクセス」から）に変更し、[バックアップポリシーからS3権限を追加する先に示したとおり](#)です。

プライベート エンドポイントへの通信にポート 80 (HTTP) を使用している場合は、設定は完了です。これで、クラスター上でNetApp Backup and Recoveryを有効にできるようになりました。

プライベート エンドポイントへの通信にポート 443 (HTTPS) を使用している場合は、次の 4 つの手順に示すように、VPC S3 エンドポイントから証明書をコピーし、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。これを実行するには"[コンソールエージェントをホストするVMにログインする](#)"次のコマンドを実行します。エンドポイントの DNS 名を入力するときは、先頭に「*」を置き換えて「bucket」を追加します。

```
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、そ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 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 (独自のストレージ VM 名に置き換えます)。

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

ONTAP ボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[API コマンドを表示する](#) レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [\[バックアップとリカバリ\]](#) の横にある [有効化 > バックアップ ボリューム](#) を選択します。

バックアップの Amazon S3 保存先がコンソールの システム ページにシステムとして存在する場合は、ONTAP クラスタを Amazon S3 オブジェクトストレージにドラッグできます。
 - バックアップとリカバリバーで [*ボリューム*](#) を選択します。ボリュームタブから [*アクション*](#) を選択します [...](#) アイコンをクリックし、単一ボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない) の [\[バックアップのアクティブ化\]*](#) を選択します。
- ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの

保護オプションが表示されます。この手順で2番目のオプションを実行した場合、ボリュームが1つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの1つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に1つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」 ページで、保護するボリュームを選択します。

- 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
- 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に1つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず1つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
- 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をオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてが必要な場合
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
 - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージシステムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: 情報はプライマリからセカンダリ、オブジェクト ストレージへ、そしてセカンダリからオブジェクト ストレージへと流れます。
 - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、ポリシーを作成します。



スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

4. ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。
 - ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLockとランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。
 - *作成*を選択します。
5. レプリケーション: 次のオプションを設定します。
 - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
 - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、ポリシーを作成します。



レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

6. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: **Amazon Web Services** を選択します。
- プロバイダー設定: プロバイダーの詳細と、バックアップを保存する AWS リージョンを入力します。

アクセス キーとシークレット キーは、ONTAP クラスターに S3 バケットへのアクセス権を付与するために作成した IAM ユーザー用です。

- バケット: 既存の S3 バケットを選択するか、新しいバケットを作成します。参照 ["S3バケットを追加する"](#)。
- 暗号化キー: 新しい S3 バケットを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Amazon S3 暗号化キーを使用するか、AWS アカウントから独自のカスタマー管理キーを選択するかを選択します。



既存のバケットを選択した場合は、暗号化情報がすでに利用可能であるため、ここで入力する必要はありません。

- ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。プライベート エンドポイントはデフォルトで無効になっています。
 - i. バックアップするボリュームが存在するONTAPクラスター内の IPspace。この IPspace のクラスター間 LIF には、アウトバウンド インターネット アクセスが必要です。
 - ii. 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。 ["Amazon S3 の AWS PrivateLink の使用に関する詳細をご覧ください"](#)。
- バックアップ ポリシー: 既存のバックアップ ポリシーを選択するか、ポリシーを作成します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、["ポリシーを作成します。"](#)。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。
- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。

7. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Azure Blob ストレージにバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのONTAPシステムからセカンダリ ストレージ システムおよび Azure Blob ストレージへのボリューム データのバックアップを開始します。



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



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

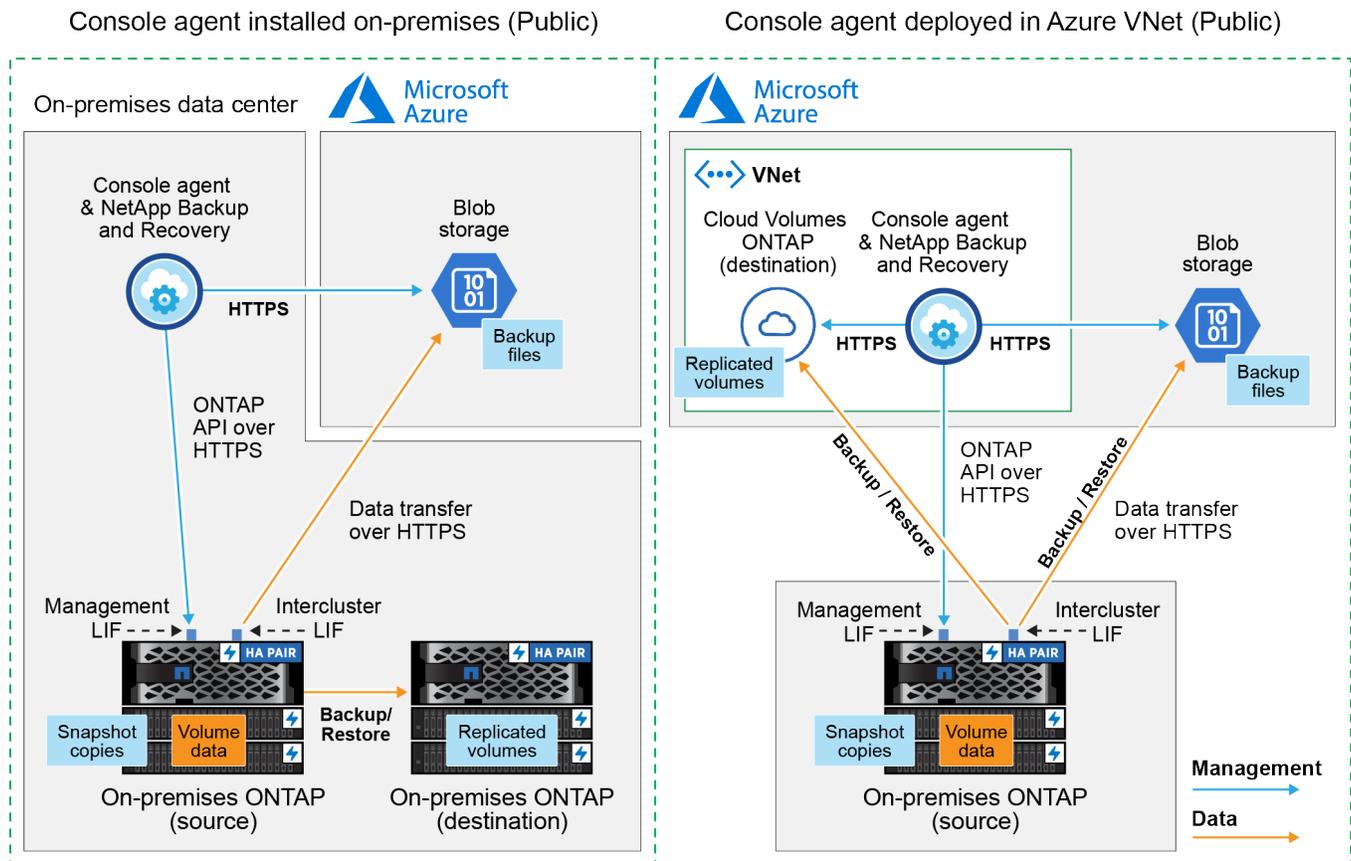
接続方法を特定する

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構成するとき使用する 2 つの接続方法のうちどちらを選択します。

- 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 プライベート エンドポイント経由でトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。

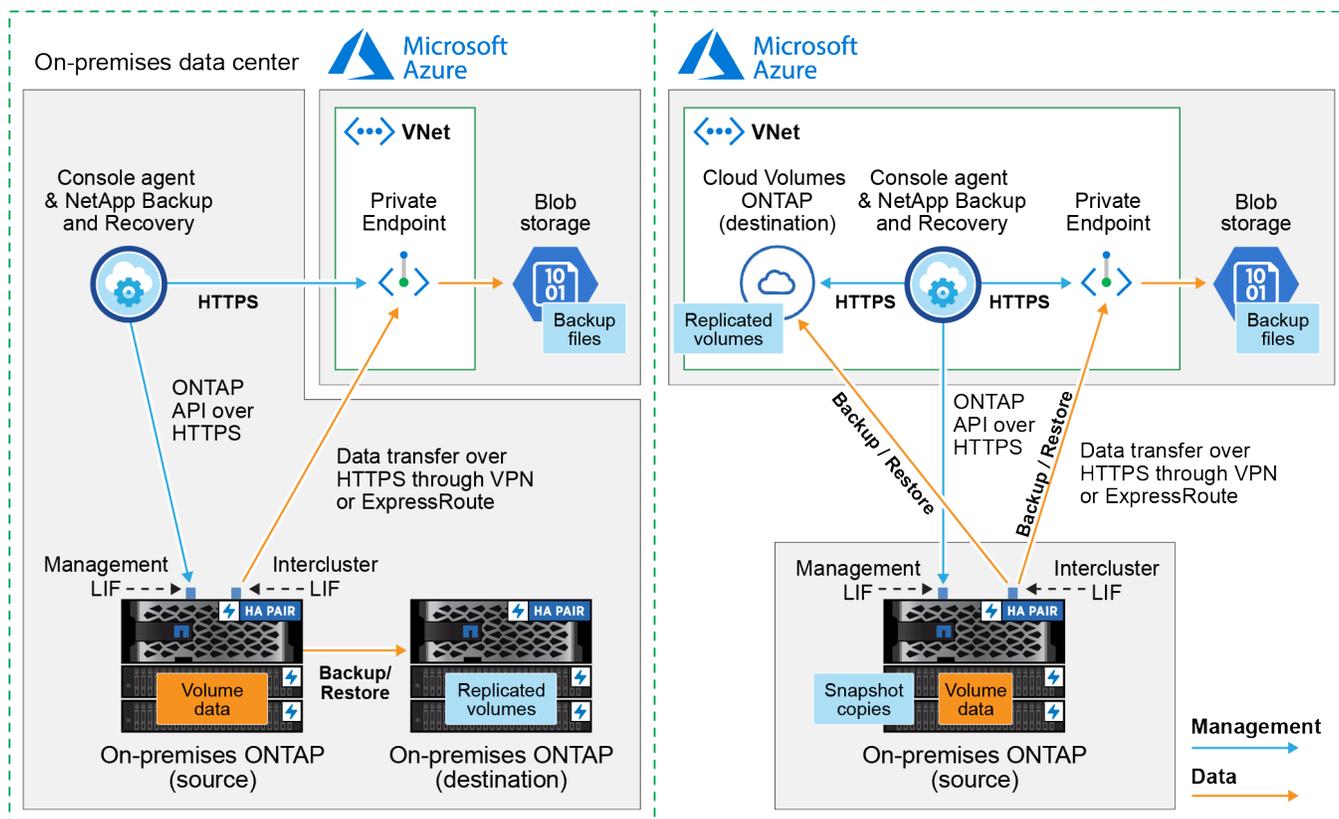
次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソール エージェント、または Azure VNet にデプロイしたコンソール エージェントを使用できます。



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。オンプレミスにインストールしたコンソール エージェント、または Azure VNet にデプロイしたコンソール エージェントを使用できます。

Console agent installed on-premises (Private)

Console agent deployed in Azure VNet (Private)



コンソールエージェントを準備する

コンソール エージェントは、NetApp Console機能のメイン ソフトウェアです。ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

Azure VNet またはオンプレミスにコンソール エージェントが既にデプロイされている場合は、準備は完了です。

そうでない場合は、いずれかの場所にコンソール エージェントを作成し、ONTAPデータを Azure Blob ストレージにバックアップする必要があります。別のクラウド プロバイダーにデプロイされたコンソール エージェントは使用できません。

- ["コンソールエージェントについて学ぶ"](#)
- ["Azureにコンソールエージェントをインストールする"](#)
- ["オンプレミスにコンソールエージェントをインストールする"](#)
- ["Azure Government リージョンにコンソール エージェントをインストールする"](#)

NetApp Backup and Recovery は、コンソール エージェントがオンプレミスでインストールされている場合ではなく、クラウドに展開されている場合に、Azure Government リージョンでサポートされます。さらに、Azure Marketplace からコンソール エージェントを展開する必要があります。コンソール SaaS Web サイトからコンソール エージェントを政府地域に展開することはできません。

コンソールエージェントのネットワークを準備する

コンソール エージェント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. コンソール エージェントがインストールさ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。
 - NetApp Backup and RecoveryおよびBlobオブジェクトストレージへのポート443経由のHTTPS接続(["エンドポイントのリストを見る"](#))
 - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
 - NetApp Backup and Recoveryの検索と復元機能が動作するには、コンソール エージェントと Azure Synapse SQL サービス間の通信用にポート 1433 が開いている必要があります。
 - Azure および Azure Government の展開には、追加の受信セキュリティ グループ ルールが必要です。見る ["Azure のコンソール エージェントのルール"](#)詳細については。
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にします。これは、ONTAPクラスターから VNet への ExpressRoute または VPN 接続があり、コンソール エージェントと 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 (プライベート接続) 内に維持する場合に必要です。

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の検索と復元機能を使用するには、Azure Synapse ワークスペースと Data Lake ストレージ アカウントにアクセスできるように、コンソール エージェントのロールに特定のアクセス許可が必要です。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ってください。

開始する前に

Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。 ["このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください"](#)。リソース プロバイダーに登録するには、サブスクリプションの所有者 または 投稿者 である必要があります。

手順

1. コンソール エージェント仮想マシンに割り当てられたロールを識別します。
 - a. Azure ポータルで、仮想マシン サービスを開きます。
 - b. コンソール エージェント仮想マシンを選択します。
 - c. *設定*の下で*ID*を選択します。
 - d. *Azure ロールの割り当て*を選択します。
 - e. コンソール エージェント仮想マシンに割り当てられたカスタム ロールをメモします。
2. カスタム ロールを更新します。
 - a. Azure ポータルで、Azure サブスクリプションを開きます。
 - b. *アクセス制御 (IAM) > ロール*を選択します。
 - c. カスタム ロールの省略記号 (...) を選択し、[編集] を選択します。
 - d. **JSON** を選択し、次の権限を追加します。

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"ポリシーの完全なJSON形式を表示する"

- e. *確認+更新*を選択し、*更新*を選択します。

ライセンス要件を確認する

Azure とコンソールの両方のライセンス要件を確認する必要があります。

- クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、Azure の従量課金制 (PAYGO) コンソール マーケットプレイス オファリングをサブスクライブするか、NetAppからNetApp Backup and Recovery 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あなたのアカウント用であり、複数のシステムで使用できます。
 - NetApp Backup and Recovery PAYGOライセンスの場合は、"[Azure Marketplace からのNetApp Consoleの提供](#)"。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
 - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービ​​スを使用できるようにするNetAppからのシリアル番号が必要になります。"[BYOLライセンスの管理方法を学ぶ](#)"。
- バックアップが保存されるオブジェクト 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。

サポート対象地域

Azure Government リージョンを含むすべてのリージョンで、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。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["クラスターの検出方法を学ぶ"]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ "[クラスターライセンスを管理する](#)".

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "[クラスター時間を設定する](#)".
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

"[SnapMirror関係に互換性のあるONTAPバージョンを表示する](#)".

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよび復元操作のために、クラスタ間 LIF から Azure Blob ストレージへのポート 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 ストレージは開始することではなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは Azure VNet に配置できます。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。["IPspacesについて詳しくはこちら"](#)。

NetApp Backup and Recoveryをセットアップするときに、使用する *IPspace* の入力を求められます。各 LIF が関連付けられている *IPspace* を選択する必要があります。これは、「デフォルト」の *IPspace* の場合もあれば、作成したカスタム *IPspace* の場合もあります。

- ノードおよびクラスタ間 LIF はオブジェクト ストアにアクセスできます。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る "[SVMのDNSサービスを構成する](#)".
- 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 ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 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NetApp Backup and Recoveryサービス接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。

ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスのONTAPネットワーク要件

- クラスタがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。"[ONTAPドキュメントでクラスタピアリングの前提条件を確認する](#)"。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Azure Blob をバックアップ先として準備する

1. アクティベーション ウィザードでは、既定の Microsoft 管理の暗号化キーを使用する代わりに、独自のカスタム管理キーを使用してデータを暗号化することができます。この場合、Azure サブスクリプション、Key Vault 名、およびキーが必要になります。"[独自のキーの使い方を学ぶ](#)"。

バックアップとリカバリでは、アクセス許可モデルとして Azure アクセス ポリシー がサポートされていることに注意してください。Azure ロールベースのアクセス制御 (Azure RBAC) アクセス許可モデルは現在サポートされていません。

2. オンプレミスのデータセンターから VNet へのパブリック インターネット経由のより安全な接続を確立したい場合は、アクティベーション ウィザードで Azure プライベート エンドポイントを構成するオプションがあります。この場合、この接続の VNet とサブネットを知っ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に関する詳細を参照してください](#)"。

Azure Blob ストレージ アカウントを作成する

デフォルトでは、サービスによってストレージ アカウントが作成されます。独自のストレージ アカウントを使用する場合は、バックアップ アクティブ化ウィザードを開始する前にストレージ アカウントを作成し、ウィザードでそれらのストレージ アカウントを選択できます。

"[独自のストレージアカウントの作成について詳しくは、こちらをご覧ください](#)。"

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップア

クティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。

- コンソールの システム ページで、システムを選択し、右側のパネルのバックアップとリカバリ サービスの横にある 有効化 > バックアップ ボリューム を選択します。

コンソールの [システム] ページにバックアップの Azure 保存先が存在する場合は、ONTAP クラスタを Azure Blob オブジェクト ストレージにドラッグできます。

- バックアップとリカバリバーで*ボリューム*を選択します。ボリュームタブから*アクション*を選択します **...** アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVol または FlexGroup ボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVol または FlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つの FlexGroup ボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じ SnapLock 設定が必要です。すべてのボリュームで SnapLock Enterprise を有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。

- 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
- 最初のボリュームを選択したら、すべての FlexVol ボリュームを選択できます (FlexGroup ボリュームは一度に 1 つだけ選択できます)。既存の FlexVol ボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。

◦ 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をオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは3つすべてが選択されています。

- ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
- レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
- バックアップ: ボリュームをオブジェクト ストレージにバックアップします。

2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。

- カスケード: 情報はプライマリからセカンダリへ、そしてセカンダリからオブジェクト ストレージへ流れます。
- ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。



スナップショットをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。

- *作成*を選択します。

4. レプリケーション: 次のオプションを設定します。

- レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
- レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。



レプリケーションをアクティブ化する前にカスタムポリシーを作成するには、"**ポリシーを作成します。**"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: **Microsoft Azure** を選択します。
- プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

新しいストレージ アカウントを作成するか、既存のストレージ アカウントを選択します。

Blob コンテナを管理する独自のリソース グループを作成するか、リソース グループの種類とグループを選択します。



バックアップ ファイルが変更されたり削除されたりするのを防ぐには、30 日間の保持期間を使用して不変ストレージが有効になっているストレージ アカウントが作成されていることを確認してください。



さらにコストを最適化するために古いバックアップ ファイルを Azure Archive Storage に階層化する場合は、ストレージ アカウントに適切なライフサイクル ルールがあることを確認してください。

- 暗号化キー: 新しい Azure ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、既定の Azure 暗号化キーを使用するか、Azure アカウントから独自のカスタマー管理キーを選択するかを選択します。

独自のカスタマー管理キーを使用する場合は、キー コンテナとキー情報を入力します。



既存の Microsoft ストレージ アカウントを選択した場合は、暗号化情報が既に用意されているため、ここで入力する必要はありません。

- ネットワーク: IPspace を選択し、プライベート エンドポイントを使用するかどうかを選択します。プライベート エンドポイントはデフォルトで無効になっています。
 - バックアップするボリュームが存在する 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 インターネット アクセスが必要です。

- ii. 必要に応じて、以前に構成した Azure プライベート エンドポイントを使用するかどうかを選択します。"[Azure プライベート エンドポイントの使用について学習します](#)"。
- バックアップ ポリシー: 既存のオブジェクト ストレージ ポリシーへのバックアップを選択するか、新しいポリシーを作成します。



バックアップをアクティブ化する前にカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLock とランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。
 - *作成*を選択します。
- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。
6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ボリュームと同期されます。

入力したリソース グループに BLOB ストレージ アカウントが作成され、そこにバックアップ ファイルが保存されます。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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータを Google Cloud Storage にバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからセカンダリストレージシステムと Google Cloud Storage へのボリュームデータのバックアップを開始します。



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



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

接続方法を特定する

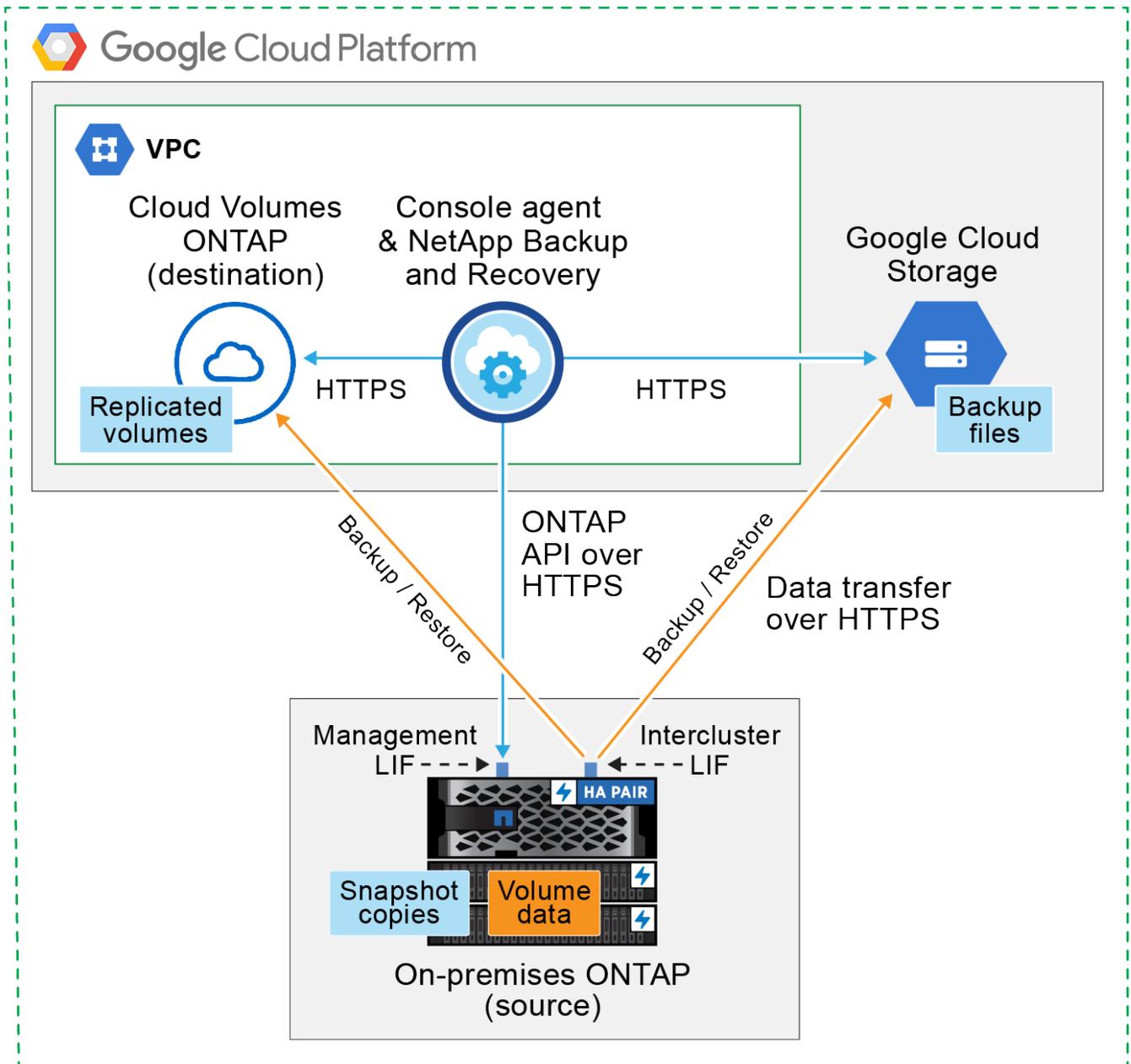
オンプレミスのONTAPシステムから Google Cloud Storage へのバックアップを構成するときに使用する2つの接続方法のうちどちらを選択します。

- 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 Google Cloud Interconnect 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 インターフェース経由でトラフィックをルーティングします。

オプションとして、パブリック接続またはプライベート接続を使用して、複製されたボリュームのセカンダリONTAPシステムに接続することもできます。

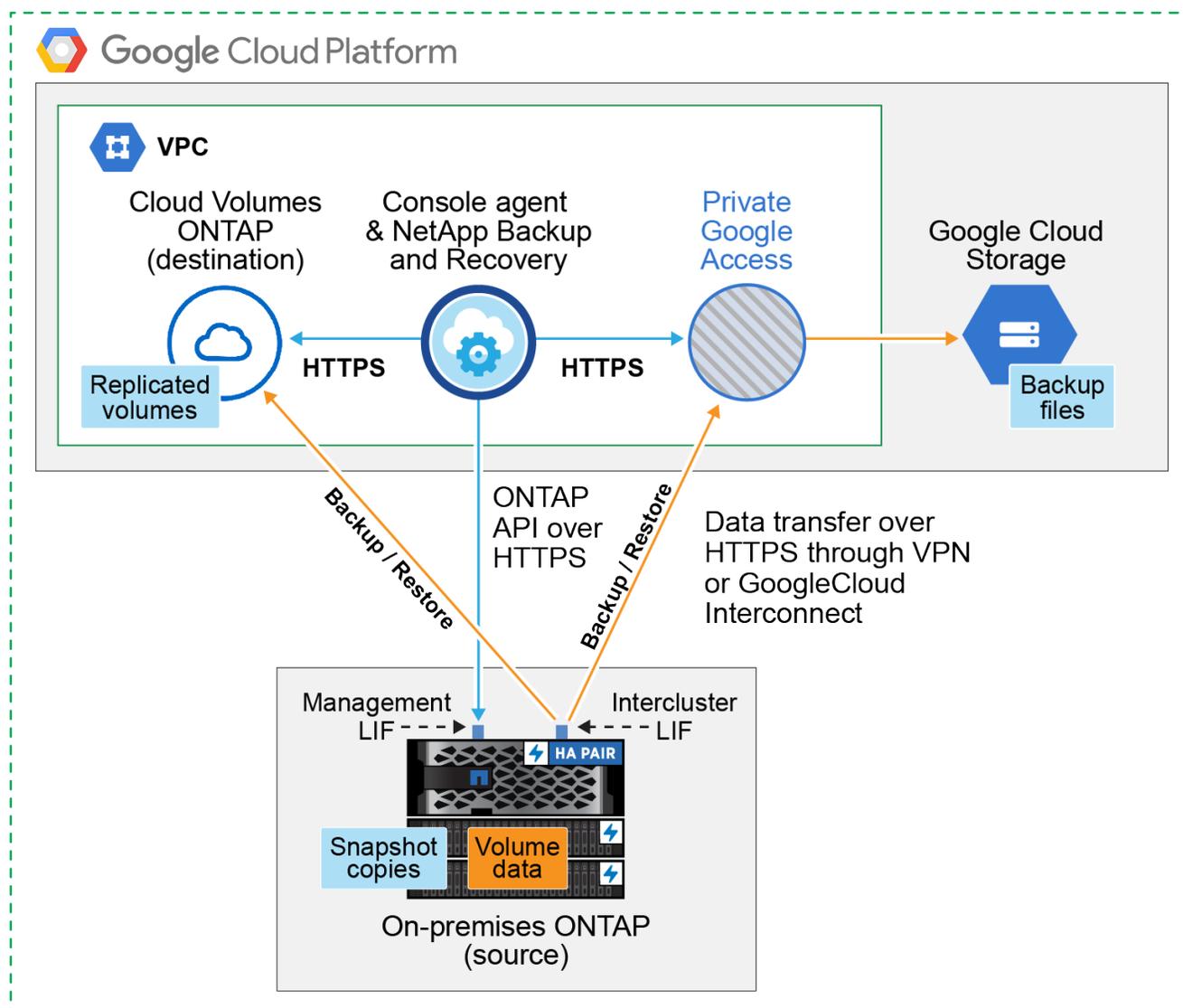
次の図は、*パブリック接続*方式と、コンポーネント間で準備する必要がある接続を示しています。コンソールエージェントは、Google Cloud Platform VPC にデプロイする必要があります。

Console agent deployed in Google Cloud VPC (Public)



次の図は、*プライベート接続*方式と、コンポーネント間で準備する必要がある接続を示しています。コンソールエージェントは、Google Cloud Platform VPC にデプロイする必要があります。

Console agent deployed in Google Cloud VPC (Private)



コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

Google Cloud Platform VPC にコンソール エージェントがすでにデプロイされている場合は、準備は完了です。

そうでない場合は、その場所にコンソール エージェントを作成して、ONTAPデータを Google Cloud Storage にバックアップする必要があります。別のクラウド プロバイダーまたはオンプレミスにデプロイされたコンソール エージェントは使用できません。

- ["コンソールエージェントについて学ぶ"](#)
- ["GCP にコンソール エージェントをインストールする"](#)

コンソールエージェントのネットワークを準備する

コンソール エージェント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. コンソール エージェントがインストールさ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。
 - NetApp Backup and RecoveryとGoogle Cloudストレージへのポート443経由のHTTPS接続(["エンドポイントのリストを見る"](#))
 - ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
2. コンソール エージェントをデプロイする予定のサブネットで、プライベート Google アクセス (またはプライベート サービス接続) を有効にします。"[プライベートGoogleアクセス](#)"または"[プライベートサービスコネク](#)ト"ONTAPクラスタから VPC への直接接続があり、コンソール エージェントと Google Cloud Storage 間の通信を仮想プライベート ネットワーク (プライベート接続) 内に維持する必要がある場合に必要です。

これらのプライベート アクセス オプションを設定するには、Google の指示に従ってください。DNSサーバーが次のように設定されていることを確認してください。`www.googleapis.com`そして`storage.googleapis.com`正しい内部 (プライベート) IP アドレスに設定します。

コンソールエージェントへの権限を確認または追加する

NetApp Backup and Recovery の「検索と復元」機能を使用するには、Google Cloud BigQuery サービスにアクセスできるように、コンソール エージェントのロールに特定の権限が必要です。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ってください。

手順

1. の中で "[Google Cloud コンソール](#)"、*役割*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 ロールを選択します。
4. ロールの権限を更新するには、「ロールの編集」を選択します。
5. 次の新しい権限をロールに追加するには、「権限の追加」を選択します。

```
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. 編集したルールを保存するには、[更新] を選択します。

ライセンス要件を確認する

- クラスタでNetApp Backup and Recoveryを有効にするには、Google の従量課金制 (PAYGO) コンソールマーケットプレイス サービスに登録するか、NetAppからNetApp Backup and Recovery BYOL ライセンスを購入して有効にする必要があります。これらのライセンスはあなたのアカウント用であり、複数のシステムで使用できます。
 - NetApp Backup and Recovery PAYGOライセンスの場合は、"[Google Marketplace のNetApp Console の提供](#)"。NetApp Backup and Recoveryの課金は、このサブスクリプションを通じて行われます。
 - NetApp Backup and Recovery BYOL ライセンスの場合、ライセンスの有効期間と容量にわたってサービスを使用できるようにするNetAppからのシリアル番号が必要になります。"[BYOLライセンスの管理方法を学ぶ](#)"。
- バックアップを保存するオブジェクト 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。

サポート対象地域

すべてのリージョンでオンプレミス システムから Google Cloud Storage へのバックアップを作成できます。サービスを設定するときに、バックアップを保存するリージョンを指定します。

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["クラスターの検出方法を学ぶ"]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ ["クラスターライセンスを管理する"](#)。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ ["クラスター時間を設定する"](#)。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

["SnapMirror関係に互換性のあるONTAPバージョンを表示する"](#)。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャの場合は、プライマリ システムで次の設定を構成します。
- カスケード バックアップ アーキテクチャの場合は、セカンダリ システムで次の設定を構成します。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよび復元操作のために、クラスタ間 LIF から Google Cloud 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 ストレージは開始することではなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは、Google Cloud Platform VPC に配置できます。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。LIF は、ONTAP がオブジェクト ストレージに接続するために使用する IPspace に関連付ける必要があります。["IPspacesについて詳しくはこちら"](#)。

NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る ["SVMのDNSサービスを構成する"](#)。

プライベートGoogleアクセスまたはプライベートサービス接続を使用している場合は、DNSサーバーが次のように設定されていることを確認してください。`storage.googleapis.com`正しい内部 (プライベート) IP アドレスに設定します。

- 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 ストレージにアクセスするために静的ルートを作成する必要があることに注意してください。
- 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NetApp Backup and Recovery接続と、ストレージ VM から DNS サーバーへのポート 53 (TCP/UDP) 経由の名前解決トラフィックを許可します。

ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソースシステムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスのONTAPネットワーク要件

- クラスターがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスターは、追加のサブネット、ポート、ファイアウォール、およびクラスターの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。"[ONTAPドキュメントでクラスターピアリングの前提条件を確認する](#)"。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

Google Cloud Storage をバックアップ先として準備する

Google Cloud Storage をバックアップ ターゲットとして準備するには、次の手順を実行します。

- 権限を設定します。
- (オプション) 独自のバケットを作成します。(必要に応じて、サービスによってバケットが作成されません。)
- (オプション) データ暗号化用の顧客管理キーを設定する

権限を設定する

カスタム ロールを使用して特定の権限を持つサービス アカウントにストレージ アクセス キーを提供する必要があります。サービス アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用される Cloud Storage バケットを認証してアクセスできるようになります。Google Cloud Storage が誰がリクエストを行っているかを認識するために、キーが必要になります。

手順

1. の中で "[Google Cloud コンソール](#)"、*役割*ページに移動します。
2. "[新しいロールの作成](#)"以下の権限を持ちます:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloudコンソールでは、"[サービスアカウントページに移動します](#)"。
4. Cloud プロジェクトを選択します。
5. サービス アカウントの作成 を選択し、必要な情報を入力します。
 - a. サービス アカウントの詳細: 名前と説明を入力します。
 - b. このサービス アカウントにプロジェクトへのアクセスを許可する: 先ほど作成したカスタム ロールを選択します。
 - c. *完了*を選択します。
6. [へ移動](#) "[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、*相互運用性*を選択します。まだ行っていない場合は、[相互運用性アクセスを有効にする]を選択します。
 - b. サービス アカウントのアクセス キー の下で、サービス アカウントのキーの作成 を選択し、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。

後でバックアップ サービスを構成するときに、NetApp Backup and Recoveryにキーを入力する必要があります。

独自のバケットを作成する

デフォルトでは、サービスによってバケットが作成されます。または、独自のバケットを使用する場合は、バックアップ アクティベーション ウィザードを開始する前にバケットを作成し、ウィザードでそれらのバケットを選択できます。

["独自のバケットの作成について詳しくは"](#)。

データ暗号化用の顧客管理暗号鍵 (CMEK) を設定する

デフォルトの Google 管理の暗号化キーを使用する代わりに、独自の顧客管理キーをデータ暗号化に使用できます。クロスリージョン キーとクロスプロジェクト キーの両方がサポートされているため、CMEK キーのプロジェクトとは異なるバケットのプロジェクトを選択できます。

独自の顧客管理キーを使用する予定の場合:

- アクティベーション ウィザードでこの情報を追加するには、キー リングとキー名が必要です。"[顧客管理暗号化キーの詳細](#)"。
- コンソール エージェントのロールに次の必要な権限が含まれていることを確認する必要があります。

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- プロジェクトで Google の「Cloud Key Management Service (KMS)」API が有効になっていることを確認する必要があります。参照 "[Google Cloud ドキュメント: API の有効化](#)" 詳細については。

CMEKの考慮事項:

- HSM (ハードウェア バックアップ) キーとソフトウェア生成キーの両方がサポートされています。
- 新しく作成された Cloud KMS キーとインポートされた Cloud KMS キーの両方がサポートされます。
- 地域キーのみがサポートされ、グローバル キーはサポートされません。
- 現在、「対称暗号化/復号化」目的のみがサポートされています。
- ストレージ アカウントに関連付けられたサービス エージェントには、NetApp Backup and Recoveryによって「CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)」IAM ロールが割り当てられます。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [\[バックアップとリカバリ\]](#) の横にある [有効化 > バックアップ ボリューム](#) を選択します。

コンソールの [システム] ページにバックアップの Google Cloud Storage 保存先が存在する場合は、ONTAPクラスターを Google Cloud オブジェクト ストレージにドラッグできます。

- バックアップとリカバリバーで*ボリューム*を選択します。ボリュームタブから*アクション*を選択します... アイコンをクリックし、単一ボリューム（オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない）の [バックアップのアクティブ化]* を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
 - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
 - 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をオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてが必要な場合

- アーキテクチャ
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは 3 つすべてが選択されています。
 - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップを選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: 情報はプライマリからセカンダリへ、そしてセカンダリからオブジェクト ストレージへ流れます。
 - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大 5 つ選択します。
 - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
 - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
 - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: **Google Cloud** を選択します。
- プロバイダー設定: プロバイダーの詳細とバックアップを保存するリージョンを入力します。

新しいバケットを作成するか、すでに作成したバケットを選択します。



さらにコストを最適化するために古いバックアップ ファイルを Google Cloud Archive ストレージに階層化する場合は、バケットに適切なライフサイクル ルールがあることを確認してください。

Google Cloud アクセスキーとシークレットキーを入力します。

- 暗号化キー: 新しい Google Cloud ストレージ アカウントを作成した場合は、プロバイダーから提供された暗号化キー情報を入力します。データの暗号化を管理するために、デフォルトの Google Cloud 暗号化キーを使用するか、Google Cloud アカウントから独自の顧客管理キーを選択するかを選択します。



既存の Google Cloud ストレージ アカウントを選択した場合は、暗号化情報がすでに用意されているため、ここで入力する必要はありません。

独自の顧客管理キーを使用する場合は、キーリングとキー名を入力します。 ["顧客管理暗号化キーの詳細"](#)。

- ネットワーク: IPspace を選択します。

バックアップするボリュームが存在する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 インターネット アクセスが必要です。

- バックアップ ポリシー: 既存のオブジェクト ストレージ ポリシーへのバックアップを選択するか、新しいポリシーを作成します。



カスタムポリシーを作成するには、 ["ポリシーを作成します。"](#)。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイル

としてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーション およびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、プライマリ ストレージ システム データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ システム データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、ソース ボリュームと同期されます。

入力した Google アクセスキーとシークレットキーで示されるサービス アカウントに Google Cloud Storage バケットが自動的に作成され、そこにバックアップ ファイルが保存されます。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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータをONTAP S3 にバックアップする

NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからボリューム データのバックアップを開始します。バックアップは、セカンダリONTAPストレージ システム (複製されたボリューム)、S3 サーバーとして設定されたONTAPシステム上のバケット (バックアップ ファイル)、またはその両方に送信できます。

プライマリオンプレミスONTAPシステムには、FAS、AFF、またはONTAP Selectシステムを使用できません。セカンダリONTAPシステムは、オンプレミスのONTAPまたはCloud Volumes ONTAPシステムになります。オブジェクトストレージは、オンプレミスのONTAPシステム、または Simple Storage Service (S3) オブジェクトストレージサーバーを有効にしたCloud Volumes ONTAPシステム上に配置できます。



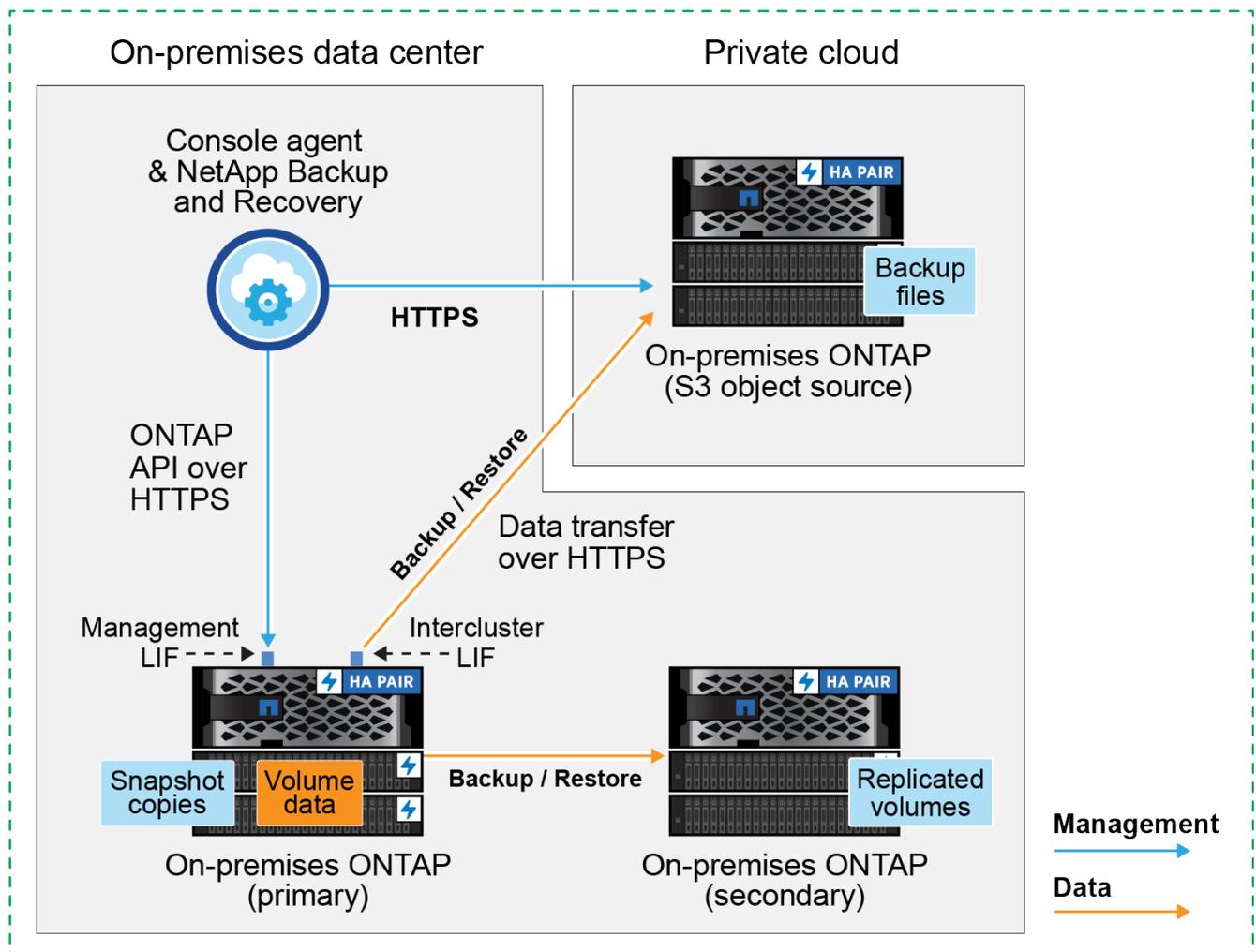
NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

接続方法を特定する

ONTAPシステム上の S3 バケットにバックアップを作成できる構成は多数あります。以下に 2 つのシナリオを示します。

次の図は、プライマリオンプレミスONTAPシステムを S3 用に設定されたオンプレミスONTAPシステムにバックアップする場合の各コンポーネントと、それらの間で準備する必要がある接続を示しています。また、ボリュームをレプリケートするために、同じオンプレミスの場所にあるセカンダリONTAPシステムへの接続も示します。

Console agent installed on premises (Public)

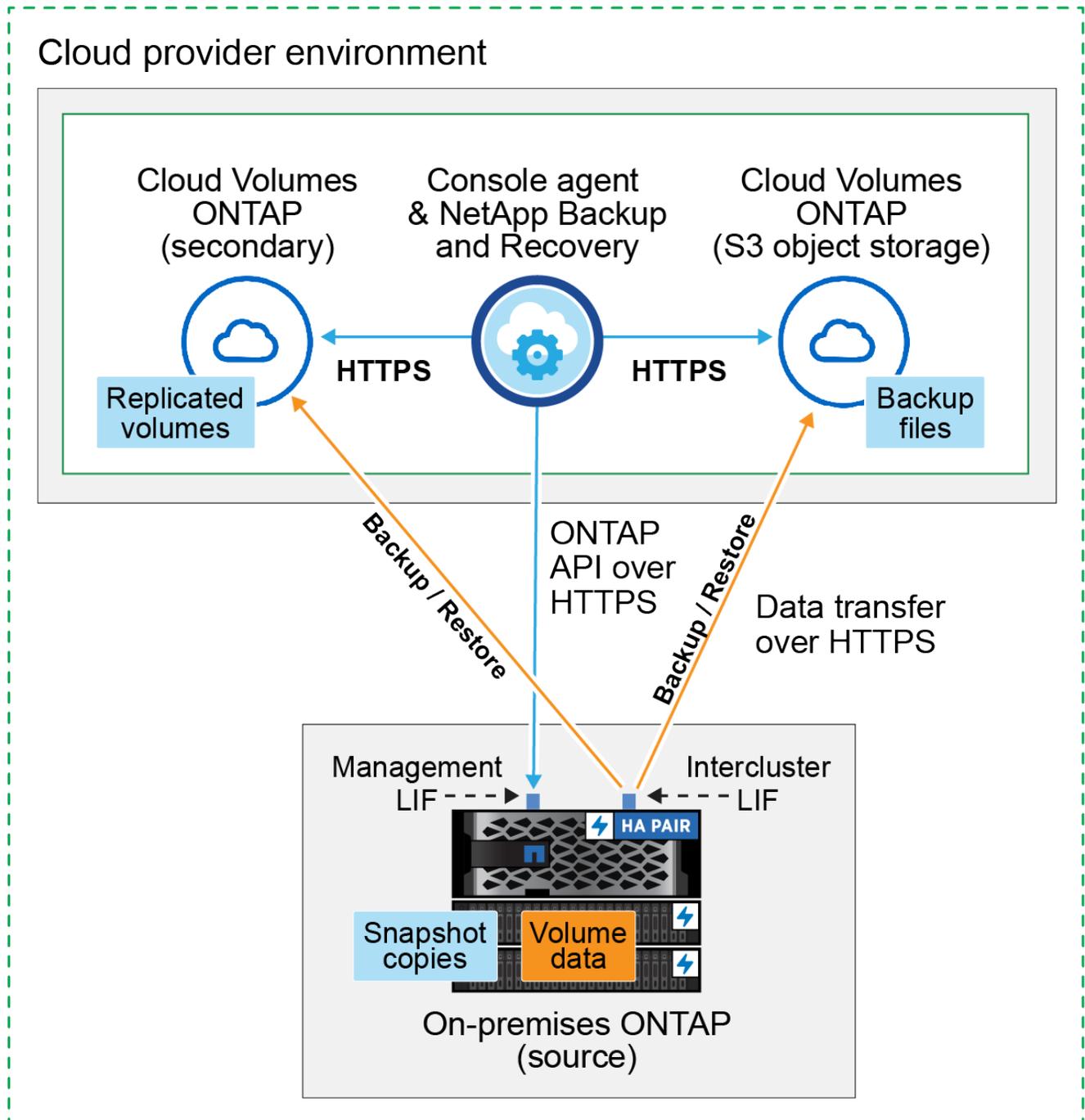


コンソール エージェントとプライマリ オンプレミスONTAPシステムがインターネット アクセスのないオンプレミスの場所にインストールされている場合 (「プライベート」モードの展開)、ONTAP S3 システムは同

じオンプレミス データセンターに配置する必要があります。

次の画像は、プライマリオンプレミスONTAPシステムを S3 用に構成されたCloud Volumes ONTAPシステムにバックアップする場合の各コンポーネントと、それらの間で準備する必要がある接続を示しています。また、ボリュームを複製するために、同じクラウド プロバイダー環境内のセカンダリCloud Volumes ONTAPシステムへの接続も示します。

Console agent deployed in cloud (Public)



このシナリオでは、コンソール エージェントは、Cloud Volumes ONTAPシステムが展開されているのと同じクラウド プロバイダー環境に展開する必要があります。

コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。 ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

ONTAP S3 にデータをバックアップする場合、オンプレミスまたはクラウドでコンソール エージェントが使用可能である必要があります。新しいコンソール エージェントをインストールするか、現在選択されているコンソール エージェントがこれらの場所のいずれかに存在することを確認する必要があります。オンプレミスのコンソール エージェントは、インターネット アクセスの有無にかかわらずサイトにインストールできます。

- ["コンソールエージェントについて学ぶ"](#)
- ["クラウド環境にコンソールエージェントをインストールする"](#)
- ["インターネットにアクセスできる Linux ホストにコンソール エージェントをインストールする"](#)
- ["インターネットにアクセスできない Linux ホストにコンソール エージェントをインストールする"](#)
- ["コンソールエージェント間の切り替え"](#)

コンソールエージェントのネットワーク要件を準備する

コンソール エージェントがインストールさ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経由のONTAP S3サーバへのHTTPS接続
- ソースONTAPクラスタ管理 LIF へのポート 443 経由の HTTPS 接続
- NetApp Backup and Recoveryへのポート 443 経由のアウトバウンド インターネット接続 (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)

プライベートモード (ダークサイト) の考慮事項

NetApp Backup and Recovery機能は、コンソール エージェントに組み込まれています。プライベート モードでインストールされている場合、新しい機能にアクセスするには、コンソール エージェント ソフトウェアを定期的に更新する必要があります。チェックしてください["NetApp Backup and Recoveryの新機能"](#)NetApp Backup and Recovery の各リリースの新機能を確認してください。新しい機能を使用する場合は、次の手順に従ってください。 ["コンソールエージェントソフトウェアをアップグレードする"](#)。

標準の SaaS 環境でNetApp Backup and Recoveryを使用すると、 NetApp Backup and Recovery の構成データがクラウドにバックアップされます。インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合、 NetApp Backup and Recovery の構成データは、バックアップが保存されているONTAP S3 バケットにバックアップされます。

ライセンス要件を確認する

クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、 NetAppからNetApp Backup and Recovery 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。このライセンスはオブジェクトストレージへのバックアップと復元用です。スナップショットや複製されたボリュームを作成するのにライセンスは必要ありません。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。

ライセンスの有効期間と容量にわたってサービスを使用するには、NetAppからのシリアル番号が必要になります。["BYOLライセンスの管理方法を学ぶ"](#)。



ONTAP S3 にファイルをバックアップする場合、PAYGO ライセンスはサポートされません。

ONTAP クラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAP クラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、NetApp Consoleの*システム* ページで利用できる必要があります。

クラスタを追加するには、クラスタ管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["クラスタの検出方法を学ぶ"]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ ["クラスタライセンスを管理する"](#)。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ ["クラスタ時間を設定する"](#)。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

["SnapMirror関係に互換性のあるONTAPバージョンを表示する"](#)。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件が満たされていることを確認する必要があります。



- ファンアウト バックアップ アーキテクチャを使用する場合は、プライマリ ストレージ システムで設定を構成する必要があります。
- カスケード バックアップ アーキテクチャを使用する場合は、セカンダリ ストレージ システムで設定を構成する必要があります。

["バックアップアーキテクチャの種類について詳しく学ぶ"](#)。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよびリストア操作のために、クラスタ間 LIF からONTAP S3 サーバへのユーザ指定ポートを介して HTTPS 接続を開始します。ポートはバックアップのセットアップ中に構成可能です。

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 ストレージは開始することではなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。LIF は、ONTAP がオブジェクト ストレージに接続するために使用する *IPspace* に関連付ける必要があります。["IPspacesについて詳しくはこちら"](#)。

NetApp Backup and Recoveryをセットアップするときに、使用する *IPspace* の入力を求められます。各 LIF が関連付けられている *IPspace* を選択する必要があります。これは、「デフォルト」の *IPspace* の場合もあれば、作成したカスタム *IPspace* の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る ["SVMのDNSサービスを構成する"](#)。
- 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 ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 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) を介してONTAPからオブジェクト ストレージへのNetApp Backup and Recoveryサービス接続と、ポート 53 (TCP/UDP) を介してストレージ VM から DNS サーバーへの名前解決トラフィックを許可します。

ボリュームを複製するための**ONTAP**ネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスの**ONTAP**ネットワーク要件

- クラスタがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAPシステムのピアリング要件を確認してください。 ["ONTAPドキュメントでクラスタピアリングの前提条件を](#)

確認する"。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

ONTAP S3をバックアップターゲットとして準備する

オブジェクト ストレージ バックアップに使用する予定のONTAPクラスタで、Simple Storage Service (S3) オブジェクト ストレージ サーバを有効にする必要があります。参照 ["ONTAP S3 ドキュメント"](#)詳細については。

注意: このクラスタをコンソールの システム ページに追加することはできますが、S3 オブジェクト ストレージ サーバとして識別されず、ソース システムをこの S3 システムにドラッグ アンド ドロップしてバックアップのアクティブ化を開始することはできません。

このONTAPシステムは次の要件を満たしている必要があります。

サポートされるONTAPバージョン

オンプレミスのONTAPシステムにはONTAP 9.8 以降が必要です。 Cloud Volumes ONTAPシステムにはONTAP 9.9.1 以降が必要です。

S3 認証情報

ONTAP S3 ストレージへのアクセスを制御するには、S3 ユーザーを作成する必要があります。 ["詳細については、ONTAP S3 のドキュメントを参照してください。"](#)

ONTAP S3 へのバックアップを設定すると、バックアップ ウィザードによって、ユーザー アカウントの S3 アクセス キーとシークレット キーの入力が求められます。ユーザー アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用されるONTAP S3 バケットを認証してアクセスできるようにします。キーは、ONTAP S3 が誰がリクエストを行っているかを認識するために必要です。

これらのアクセス キーは、次の権限を持つユーザー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",
"s3:GetBucketLocation"
```

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- バックアップしたいボリュームを選択します
- バックアップ戦略とポリシーを定義する
- 選択内容を確認する

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある 有効化 > バックアップ ボリューム を選択します。
 - バックアップとリカバリバーで*ボリューム*を選択します。 [ボリューム] タブで、アクション (...) オプションを選択し、単一のボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていない) に対して バックアップのアクティブ化 を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。
 - コンソールエージェントがすでにある場合は、設定は完了です。 *次へ* を選択してください。
 - コンソール エージェントがない場合は、[コンソール エージェントの追加] オプションが表示されま
す。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにすでにスナップショットまたはレプリケーション ポリシーが適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされることに注意してください。

1. 「ボリュームの選択」 ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。

- 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に1つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず1つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
- 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をオンにします。

2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを構成する必要があります。

- 保護オプション: ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションの1つまたはすべてを実装するかどうか
- アーキテクチャ: ファンアウトまたはカスケードバックアップアーキテクチャを使用するかどうか
- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー
- オブジェクトストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは3つすべてが選択されています。
 - ローカル スナップショット: ローカル スナップショットを作成します。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: S3 用に設定されたONTAPシステム上のバケットにボリュームをバックアップします。
2. アーキテクチャ: レプリケーションとバックアップの両方を選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: バックアップ データはプライマリ システムからセカンダリ システムへ流れ、次にセカンダリ システムからオブジェクト ストレージへ流れます。
 - ファンアウト: バックアップ データはプライマリ システムからセカンダリ システムへ、そしてプライマリ システムからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。

3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。



スナップショットをアクティブ化する前にカスタムポリシーを作成する場合は、System ManagerまたはONTAP CLIを使用できます。`snapmirror policy create` 指示。参照。



バックアップとリカバリを使用してカスタムポリシーを作成するには、"[ポリシーを作成します](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。

- 通常は異なる頻度のスケジュールを最大 5 つ選択します。

- *作成*を選択します。

4. レプリケーション: レプリケーション を選択した場合は、次のオプションを設定します。

- レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、宛先アグリゲート (FlexGroupボリュームの場合はアグリゲート) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。

- レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいポリシーを作成します。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: * ONTAP S3* を選択します。

- プロバイダー設定: S3 サーバーの FQDN の詳細、ポート、ユーザーのアクセス キーとシークレット キーを入力します。

アクセス キーとシークレット キーは、作成したユーザーがONTAPクラスターに S3 バケットへのアクセス権を付与するためのものです。

- ネットワーク: バックアップするボリュームが存在するソースONTAPクラスター内の IPspace を選択します。この IPspace のクラスター間 LIF には、アウトバウンド インターネット アクセスが必要です (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。



正しい IPspace を選択すると、NetApp Backup and Recovery がONTAPからONTAP S3 オブジェクト ストレージへの接続を確立できるようになります。

- バックアップ ポリシー: 既存のバックアップ ポリシーを選択するか、新しいバックアップ ポリシーを作成します。



System Manager またはONTAP CLI を使用してポリシーを作成できます。ONTAP CLI を使用してカスタムポリシーを作成するには `snapmirror policy create` コマンドについては、。



バックアップとリカバリを使用してカスタムポリシーを作成するには、"**ポリシーを作成します。**"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLockとランサムウェア耐性の詳細については、以下を参照してください。"**オブ**

ジェクトへのバックアップポリシー設定"。

- ***作成***を選択します。
- 既存のスナップショットをバックアップ ファイルとしてオブジェクト ストレージにエクスポートする: このシステム内のボリュームに、選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致するローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの最も完全な保護が確保されます。

6. ***次へ***を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。ポリシーが一致しない場合、バックアップは作成されません。
3. ***バックアップの有効化***を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、ソース データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、***API リクエストの表示***を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and Recoveryを使用してオンプレミスのONTAPデータをStorageGRIDにバックアップします。

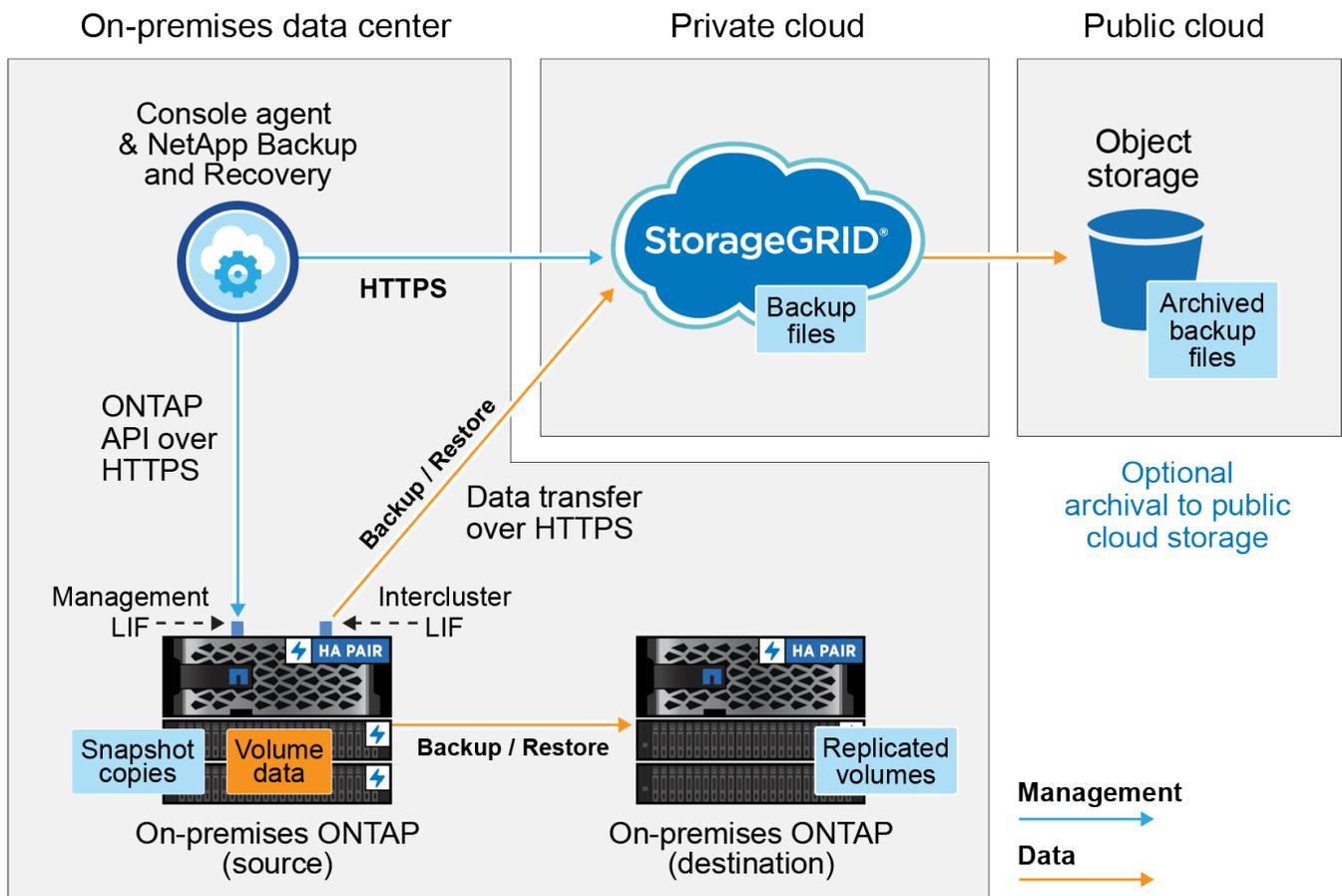
NetApp Backup and Recoveryでいくつかの手順を完了して、オンプレミスのプライマリONTAPシステムからセカンダリストレージシステムおよびNetApp StorageGRIDシステムのオブジェクトストレージへのボリュームデータのバックアップを開始します。

- ① 「オンプレミスのONTAPシステム」には、FAS、AFF、およびONTAP Selectシステムが含まれます。
- ② NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

接続方法を特定する

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の各コンポーネントと、それらの間で準備する必要がある接続を示しています。

オプションで、同じオンプレミスの場所にあるセカンダリONTAPシステムに接続してボリュームを複製することもできます。



コンソール エージェントとオンプレミスのONTAPシステムがインターネットにアクセスできないオンプレミ

スの場所(「ダーク サイト」)にインストールされている場合、StorageGRIDシステムは同じオンプレミスデータセンターに配置する必要があります。ダーク サイト構成では、古いバックアップ ファイルのパブリック クラウドへのアーカイブはサポートされていません。

コンソールエージェントを準備する

コンソール エージェントは、コンソール機能のメイン ソフトウェアです。ONTAPデータをバックアップおよび復元するには、コンソール エージェントが必要です。

コンソールエージェントの作成または切り替え

StorageGRIDにデータをバックアップする場合、オンプレミスでコンソール エージェントが使用可能である必要があります。新しいコンソール エージェントをインストールするか、現在選択されているコンソール エージェントがオンプレミスに存在することを確認する必要があります。コンソール エージェントは、インターネットにアクセスできるサイトにも、アクセスできないサイトにもインストールできます。

- ["コンソールエージェントについて学ぶ"](#)
- ["インターネットにアクセスできる Linux ホストにコンソール エージェントをインストールする"](#)
- ["インターネットにアクセスできない Linux ホストにコンソール エージェントをインストールする"](#)
- ["コンソールエージェント間の切り替え"](#)

コンソールエージェントのネットワーク要件を準備する

コンソール エージェントがインストールさ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経由のStorageGRIDゲートウェイノードへのHTTPS接続
- ポート443経由のONTAPクラスタ管理LIFへのHTTPS接続
- NetApp Backup and Recoveryへのポート 443 経由のアウトバウンド インターネット接続 (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)

プライベートモード (ダークサイト) の考慮事項

- NetApp Backup and Recovery機能は、コンソール エージェントに組み込まれています。プライベート モードでインストールされている場合、新しい機能にアクセスするには、コンソール エージェント ソフトウェアを定期的に更新する必要があります。チェックしてください["NetApp Backup and Recoveryの新機能"](#)NetApp Backup and Recovery の各リリースの新機能を確認してください。新しい機能を使用する場合は、次の手順に従ってください。 ["コンソールエージェントソフトウェアをアップグレードする"](#)。

オブジェクト ストレージへのバックアップの作成に加えて、スナップショットと複製されたボリュームのスケジュール設定と作成の機能を備えたNetApp Backup and Recoveryの新しいバージョンでは、コンソール エージェントのバージョン 3.9.31 以上を使用する必要があります。したがって、すべてのバックアップを管理するには、この最新リリースを入手することをお勧めします。

- SaaS 環境でNetApp Backup and Recovery を使用すると、NetApp Backup and Recovery の構成データがクラウドにバックアップされます。インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合、NetApp Backup and Recovery構成データは、バックアップが保存されているStorageGRIDバケットにバックアップされます。

ライセンス要件を確認する

クラスターに対してNetApp Backup and Recoveryをアクティブ化する前に、NetAppからNetApp Backup and Recovery 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。

ライセンスの有効期間と容量にわたってサービスを使用するには、NetAppからのシリアル番号が必要になります。"[BYOLライセンスの管理方法を学ぶ](#)"。



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

ONTAPクラスタを準備する

ソースのオンプレミスONTAPシステムと、セカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムを準備します。

ONTAPクラスタを準備するには、次の手順を実行します。

- NetApp ConsoleでONTAPシステムを検出する
- ONTAPのシステム要件を確認する
- オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する
- ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp ConsoleでONTAPシステムを検出する

ソースのオンプレミスONTAPシステムとセカンダリのオンプレミスONTAPまたはCloud Volumes ONTAPシステムの両方が、NetApp Consoleの*システム* ページで利用できる必要があります。

クラスターを追加するには、クラスター管理 IP アドレスと管理者ユーザー アカウントのパスワードを知っておく必要があります。<https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html>["クラスターの検出方法を学ぶ"]。

ONTAPのシステム要件を確認する

ONTAPシステムが次の要件を満たしていることを確認してください。

- 最低でもONTAP 9.8、ONTAP 9.8P13 以降が推奨されます。
- SnapMirrorライセンス (プレミアム バンドルまたはデータ保護バンドルの一部として含まれています)。

注: NetApp Backup and Recoveryを使用する場合、「Hybrid Cloud Bundle」は必要ありません。

方法を学ぶ "[クラスターライセンスを管理する](#)"。

- 時間とタイムゾーンは正しく設定されています。方法を学ぶ "[クラスター時間を設定する](#)"。
- データを複製する場合は、ソース システムと宛先システムで互換性のあるONTAPバージョンが実行されていることを確認します。

"[SnapMirror関係に互換性のあるONTAPバージョンを表示する](#)"。

オブジェクトストレージにデータをバックアップするためのONTAPネットワーク要件を確認する

オブジェクト ストレージに接続するシステムでは、次の要件を構成する必要があります。

- ファンアウト バックアップ アーキテクチャを使用する場合は、プライマリ ストレージ システムで次の設定を構成する必要があります。
- カスケード バックアップ アーキテクチャを使用する場合は、セカンダリ ストレージ システムで次の設定を構成する必要があります。

次のONTAPクラスタ ネットワーク要件が必要です。

- ONTAPクラスタは、バックアップおよびリストア操作のために、クラスタ間 LIF からStorageGRIDゲートウェイ ノードへのユーザ指定ポートを介して HTTPS 接続を開始します。ポートはバックアップのセットアップ中に構成可能です。

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 ストレージは開始することなく、応答するだけです。

- ONTAP、コンソール エージェントからクラスタ管理 LIF への着信接続が必要です。コンソール エージェントは社内に常駐する必要があります。
- バックアップするボリュームをホストする各ONTAPノードには、クラスタ間 LIF が必要です。LIF は、ONTAP がオブジェクト ストレージに接続するために使用する IPspace に関連付ける必要があります。["IPspacesについて詳しくはこちら"](#)。

NetApp Backup and Recoveryをセットアップするときに、使用する IPspace の入力を求められます。各 LIF が関連付けられている IPspace を選択する必要があります。これは、「デフォルト」の IPspace の場合もあれば、作成したカスタム IPspace の場合もあります。

- ノードのクラスタ間 LIF はオブジェクト ストアにアクセスできます (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。
- ボリュームが配置されているストレージ VM に対して DNS サーバーが構成されています。方法を見る ["SVMのDNSサービスを構成する"](#)。
- 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 ストレージにアクセスするために静的ルートを作成する必要がある場合があります。
- 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) を介してONTAPからオブジェクト ストレージへのNetApp Backup and Recoveryサービス接続と、ポート 53 (TCP/UDP) を介してストレージ VM から DNS サーバーへの名前解決トラフィックを許可します。

ボリュームを複製するためのONTAPネットワーク要件を確認する

NetApp Backup and Recoveryを使用してセカンダリONTAPシステムに複製ボリュームを作成する場合は、ソース システムと宛先システムが次のネットワーク要件を満たしていることを確認してください。

オンプレミスのONTAPネットワーク要件

- クラスタがオンプレミスにある場合は、企業ネットワークからクラウド プロバイダーの仮想ネットワークへの接続が必要です。これは通常、VPN 接続です。
- ONTAPクラスタは、追加のサブネット、ポート、ファイアウォール、およびクラスタの要件を満たす必要があります。

Cloud Volumes ONTAPまたはオンプレミス システムにレプリケートできるため、オンプレミスONTAP システムのピアリング要件を確認してください。"[ONTAPドキュメントでクラスタピアリングの前提条件を確認する](#)"。

Cloud Volumes ONTAPのネットワーク要件

- インスタンスのセキュリティ グループには、必要な受信ルールと送信ルール (具体的には、ICMP とポート 11104 および 11105 のルール) が含まれている必要があります。これらのルールは、事前定義されたセキュリティ グループに含まれています。

StorageGRIDをバックアップターゲットとして準備する

StorageGRID は次の要件を満たしている必要があります。参照 "[StorageGRIDドキュメント](#)"詳細についてはこちらをご覧ください。

StorageGRIDのDataLockおよびランサムウェア耐性要件の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシーオプション](#)"。

サポートされているStorageGRIDバージョン

StorageGRID 10.3 以降がサポートされています。

バックアップに DataLock & Ransomware Resilience を使用するには、StorageGRIDシステムでバージョン 11.6.0.3 以上を実行している必要があります。

古いバックアップをクラウド アーカイブ ストレージに階層化するには、StorageGRIDシステムでバージョン 11.3 以降を実行している必要があります。さらに、StorageGRIDシステムがコンソールの システム ページで検出される必要があります。

アーカイブ ストレージを使用するには、管理ノードの IP アクセスが必要です。

ゲートウェイ IP アクセスは常に必要です。

S3 認証情報

StorageGRIDストレージへのアクセスを制御するには、S3 テナント アカウントを作成する必要があります。"[詳細についてはStorageGRIDのドキュメントを参照してください](#)。"

StorageGRIDへのバックアップを設定すると、バックアップ ウィザードによってテナント アカウントの S3 アクセス キーとシークレット キーの入力が求められます。テナント アカウントにより、NetApp Backup and Recovery は、バックアップの保存に使用されるStorageGRIDバケットを認証してアクセスできるようになります。キーは、StorageGRID が誰がリクエストを行っているかを認識するために必要です。

これらのアクセス キーは、次の権限を持つユーザー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手動で有効にしないでください。

古いバックアップファイルをパブリッククラウドストレージにアーカイブする準備をする

古いバックアップファイルをアーカイブストレージに階層化することで、必要のないバックアップに安価なストレージクラスを使用することになり、コストを節約できます。StorageGRIDは、アーカイブストレージを提供しないオンプレミス(プライベートクラウド)ソリューションですが、古いバックアップファイルをパブリッククラウドアーカイブストレージに移動できます。この方法で使用すると、クラウドストレージに階層化されたデータ、またはクラウドストレージから復元されたデータは、StorageGRIDとクラウドストレージの間で転送されます。このデータ転送にはコンソールは関与しません。

現在のサポートでは、AWS S3 Glacier/S3 Glacier Deep Archive または Azure Archive ストレージにバックアップをアーカイブできます。

- ONTAP の要件*
- クラスタではONTAP 9.12.1 以上を使用する必要があります。
- StorageGRID の要件*
- StorageGRIDは 11.4 以上を使用する必要があります。
- StorageGRIDは ["コンソールで発見され利用可能"](#)。

Amazon S3 の要件

- アーカイブされたバックアップが保存されるストレージスペース用の Amazon S3 アカウントにサインアップする必要があります。
- バックアップを AWS S3 Glacier または S3 Glacier Deep Archive ストレージに階層化することを選択できます。["AWS アーカイブ層の詳細"](#)。
- StorageGRIDはバケットへのフルコントロールアクセス権を持っている必要があります(s3:*); ただし、これが不可能な場合は、バケットポリシーでStorageGRIDに次の S3 権限を付与する必要があります。
 - s3:AbortMultipartUpload
 - s3:DeleteObject
 - s3:GetObject
 - s3:ListBucket
 - s3:ListBucketMultipartUploads
 - s3:ListMultipartUploadParts
 - s3:PutObject
 - s3:RestoreObject

Azure Blob の要件

- アーカイブされたバックアップが保存されるストレージスペースの Azure サブスクリプションにサインアップする必要があります。
- アクティベーションウィザードを使用すると、既存のリソースグループを使用して、バックアップを保

存する BLOB コンテナを管理したり、新しいリソース グループを作成したりできます。

クラスターのバックアップ ポリシーのアーカイブ設定を定義するときは、クラウド プロバイダーの資格情報を入力し、使用するストレージ クラスを選択します。NetApp Backup and Recovery は、クラスターのバックアップをアクティブ化するとクラウド バケットを作成します。AWS および Azure アーカイブ ストレージに必要な情報を以下に示します。

AWS	Azure
<input checked="" type="checkbox"/> Tier Backups to Archive	<input checked="" type="checkbox"/> Tier Backups to Archive
Cloud Provider AWS	Cloud Provider AZURE
Account Select Account	Azure Subscription Select Account
Region Select Region	Region Select Region
AWS Access Key Enter AWS Access Key	Resource Group Type Select an Existing Resource Group
AWS Secret Key Enter AWS Secret Key	Resource Group Select Resource Group
Archive After (Days) (1-999)	Archive After (Days) (1-999)
Storage Class S3 Glacier	Storage Class Azure Archive

選択したアーカイブ ポリシー設定により、StorageGRIDに情報ライフサイクル管理 (ILM) ポリシーが生成され、設定が「ルール」として追加されます。

- 既存のアクティブな ILM ポリシーがある場合は、データをアーカイブ層に移動するための新しいルールが ILM ポリシーに追加されます。
- 既存の ILM ポリシーが「提案」状態にある場合、新しい ILM ポリシーの作成とアクティブ化はできません。"[StorageGRID ILMポリシーとルールの詳細](#)"。

ONTAPボリューム上のバックアップをアクティブ化する

オンプレミスのシステムからいつでも直接バックアップをアクティブ化できます。

ウィザードに従って、次の主要な手順を実行します。

- [\[バックアップしたいボリュームを選択します\]](#)
- [\[バックアップ戦略を定義する\]](#)
- [\[選択内容を確認する\]](#)

また、[APIコマンドを表示する](#)レビュー ステップでコードをコピーして、将来のシステムのバックアップ アクティベーションを自動化できます。

ウィザードを起動する

手順

1. 次のいずれかの方法で、バックアップと回復のアクティブ化ウィザードにアクセスします。
 - コンソールの システム ページで、システムを選択し、右側のパネルの [バックアップとリカバリ] の横にある [有効化 > バックアップ ボリューム](#) を選択します。

コンソールの [システム] ページにバックアップの保存先がシステムとして存在する場合は、ONTAP クラスターをオブジェクト ストレージにドラッグできます。

- バックアップとリカバリバーで*ボリューム*を選択します。[ボリューム] タブで、アクション (...) オプションを選択し、単一のボリューム (オブジェクト ストレージへのレプリケーションまたはバックアップがまだ有効になっていないもの) に対して バックアップのアクティブ化 を選択します。

ウィザードの「概要」ページには、ローカル スナップショット、レプリケーション、バックアップなどの保護オプションが表示されます。この手順で 2 番目のオプションを実行した場合、ボリュームが 1 つ 選択された状態で「バックアップ戦略の定義」ページが表示されます。

2. 次のオプションを続行します。

- コンソールエージェントがすでにある場合は、設定は完了です。*次へ*を選択してください。
- コンソール エージェントがまだない場合は、[コンソール エージェントの追加] オプションが表示されます。参照[\[コンソールエージェントを準備する\]](#)。

バックアップしたいボリュームを選択します

保護するボリュームを選択します。保護されたボリュームとは、スナップショット ポリシー、レプリケーション ポリシー、オブジェクトへのバックアップ ポリシーの 1 つ以上を持つボリュームです。

FlexVolまたはFlexGroupボリュームを保護することを選択できますが、システムのバックアップをアクティブ化するときにこれらのボリュームを混在して選択することはできません。方法を見る["システム内の追加ボリュームのバックアップを有効にする"](#)(FlexVolまたはFlexGroup) 初期ボリュームのバックアップを構成した後。



- 一度に 1 つのFlexGroupボリューム上でのみバックアップをアクティブ化できます。
- 選択するボリュームには同じSnapLock設定が必要です。すべてのボリュームでSnapLock Enterpriseを有効にするか、SnapLock を無効にする必要があります。

手順

選択したボリュームにスナップショットまたはレプリケーション ポリシーがすでに適用されている場合は、後で選択したポリシーによって既存のポリシーが上書きされます。

1. 「ボリュームの選択」 ページで、保護するボリュームを選択します。
 - 必要に応じて、行をフィルタリングして、特定のボリューム タイプ、スタイルなどを持つボリュームのみを表示し、選択を容易にします。
 - 最初のボリュームを選択したら、すべてのFlexVolボリュームを選択できます (FlexGroupボリュームは一度に 1 つだけ選択できます)。既存のFlexVolボリュームをすべてバックアップするには、まず 1 つのボリュームをチェックし、次にタイトル行のボックスをチェックします。
 - 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をオンにします。
2. *次へ*を選択します。

バックアップ戦略を定義する

バックアップ戦略を定義するには、次のオプションを設定する必要があります。

- ローカルスナップショット、レプリケーション、オブジェクトストレージへのバックアップなど、バックアップオプションのいずれかまたはすべてを使用するかどうか
- アーキテクチャ

- ローカルスナップショットポリシー
- レプリケーションターゲットとポリシー



選択したボリュームのスナップショットおよびレプリケーション ポリシーがこの手順で選択したポリシーと異なる場合、既存のポリシーが上書きされます。

- オブジェクト ストレージ情報へのバックアップ (プロバイダー、暗号化、ネットワーク、バックアップ ポリシー、エクスポート オプション)。

手順

1. 「バックアップ戦略の定義」 ページで、次のいずれかまたはすべてを選択します。デフォルトでは3つすべてが選択されています。
 - ローカル スナップショット: オブジェクト ストレージへのレプリケーションまたはバックアップを実行する場合は、ローカル スナップショットを作成する必要があります。
 - レプリケーション: 別のONTAPストレージ システムに複製されたボリュームを作成します。
 - バックアップ: ボリュームをオブジェクト ストレージにバックアップします。
2. アーキテクチャ: レプリケーションとバックアップの両方を選択した場合は、次のいずれかの情報フローを選択します。
 - カスケード: 情報はプライマリからセカンダリへ流れ、次にセカンダリからオブジェクト ストレージへ流れます。
 - ファンアウト: 情報はプライマリからセカンダリへ、そしてプライマリからオブジェクト ストレージへ流れます。

これらのアーキテクチャの詳細については、"[保護の旅を計画する](#)"。
3. ローカル スナップショット: 既存のスナップショット ポリシーを選択するか、新しいポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
 - 通常は異なる頻度のスケジュールを最大5つ選択します。
 - *作成*を選択します。
4. レプリケーション: 次のオプションを設定します。
 - レプリケーション ターゲット: 宛先システムと SVM を選択します。必要に応じて、複製先のアグリゲート (複数可) と、複製されたボリューム名に追加されるプレフィックスまたはサフィックスを選択します。
 - レプリケーション ポリシー: 既存のレプリケーション ポリシーを選択するか、新しいレプリケーション ポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- *作成*を選択します。

5. オブジェクトにバックアップ: *バックアップ*を選択した場合は、次のオプションを設定します。

- プロバイダー: *StorageGRID*を選択します。
- プロバイダー設定: プロバイダー ゲートウェイ ノードの FQDN の詳細、ポート、アクセス キー、およびシークレット キーを入力します。

アクセス キーとシークレット キーは、ONTAP クラスターにバケットへのアクセス権を付与するために作成した IAM ユーザー用です。

- ネットワーク: バックアップするボリュームが存在するONTAPクラスター内の IPspace を選択します。この IPspace のクラスタ間 LIF には、アウトバウンド インターネット アクセスが必要です (コンソール エージェントが「ダーク」サイトにインストールされている場合は必要ありません)。



適切な IPspace を選択すると、NetApp Backup and Recovery がONTAPからStorageGRIDオブジェクトストレージへの接続を確立できるようになります。

- バックアップ ポリシー: 既存のオブジェクト ストレージへのバックアップ ポリシーを選択するか、新しいポリシーを作成します。



カスタムポリシーを作成するには、"[ポリシーを作成します。](#)"。

ポリシーを作成するには、[新しいポリシーの作成] を選択し、次の操作を行います。

- ポリシーの名前を入力します。
- 通常は異なる頻度のスケジュールを最大 5 つ選択します。
- オブジェクトへのバックアップ ポリシーの場合は、DataLock と Ransomware Resilience の設定を行います。DataLockとランサムウェア耐性の詳細については、以下を参照してください。"[オブジェクトへのバックアップポリシー設定](#)"。

クラスターでONTAP 9.11.1 以降を使用している場合は、*DataLock* と *Ransomware Resilience* を構成することで、バックアップを削除やランサムウェア攻撃から保護することができます。*DataLock* はバックアップ ファイルが変更されたり削除されたりするのを防ぎ、*Ransomware Resilience* はバックアップ ファイルをスキャンして、バックアップ ファイル内のランサムウェア攻撃の証拠を探します。

- *作成*を選択します。

クラスターがONTAP 9.12.1 以上を使用しており、StorageGRIDシステムがバージョン 11.4 以上を使用している場合は、一定の日数後に古いバックアップをパブリック クラウド アーカイブ層に階層化することを選択できます。現在サポートされているのは、AWS S3 Glacier/S3 Glacier Deep Archive または Azure Archive ストレージ層です。[この機能を使用するためにシステムを構成する方法をご覧ください。](#)

- パブリック クラウドへの階層化バックアップ: バックアップを階層化するクラウド プロバイダーを選択し、プロバイダーの詳細を入力します。

新しいStorageGRIDクラスターを選択または作成します。コンソールが検出できるStorageGRIDクラ

スタの作成の詳細については、"[StorageGRIDドキュメント](#)"。

- 既存のスナップショットをバックアップ コピーとしてオブジェクト ストレージにエクスポートする: このシステムで選択したバックアップ スケジュール ラベル (たとえば、毎日、毎週など) に一致する、このシステムのボリュームのローカル スナップショットがある場合は、この追加プロンプトが表示されます。このボックスをオンにすると、すべての履歴スナップショットがバックアップ ファイルとしてオブジェクト ストレージにコピーされ、ボリュームの保護が最も完全になります。

6. *次へ*を選択します。

選択内容を確認する

ここで選択内容を確認し、必要に応じて調整を行うことができます。

手順

1. 「レビュー」 ページで選択内容を確認します。
2. オプションで、スナップショット ポリシー ラベルをレプリケーション ポリシー ラベルおよびバックアップ ポリシー ラベルと自動的に同期する チェックボックスをオンにします。これにより、レプリケーションおよびバックアップ ポリシーのラベルと一致するラベルを持つスナップショットが作成されます。
3. *バックアップの有効化*を選択します。

結果

NetApp Backup and Recovery はボリュームの初期バックアップを開始します。複製されたボリュームとバックアップ ファイルのベースライン転送には、ソース データの完全なコピーが含まれます。後続の転送には、スナップショットに含まれるプライマリ ストレージ データの差分コピーが含まれます。

複製されたボリュームが宛先クラスターに作成され、プライマリ ストレージ ボリュームと同期されます。

入力した S3 アクセスキーとシークレットキーで示されるサービスアカウントに S3 バケットが作成され、そこにバックアップファイルが保存されます。

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。

バックアップと復元ジョブのステータスを監視することもできます。"[ジョブ監視ページ](#)"。

APIコマンドを表示する

バックアップとリカバリのアクティブ化ウィザードで使用される API コマンドを表示し、必要に応じてコピーすることもできます。将来のシステムでバックアップのアクティベーションを自動化するには、これを実行する必要がある場合があります。

手順

1. バックアップとリカバリのアクティブ化ウィザードから、*API リクエストの表示*を選択します。
2. コマンドをクリップボードにコピーするには、[コピー] アイコンを選択します。

NetApp Backup and RecoveryでSnapMirrorを使用してボリュームを Cloud Resync に移行する

NetApp Backup and RecoveryのSnapMirror to Cloud Resync 機能は、NetApp環境での

ボリューム移行中のデータ保護と継続性を効率化します。SnapMirror Logical Replication (LRSE) を使用してボリュームをオンプレミスのNetApp展開から別の展開へ、またはCloud Volumes ONTAPなどのクラウドベースのソリューションに移行した場合、SnapMirror to Cloud Resyncにより、既存のクラウドバックアップがそのままの状態で作動し続けることが保証されます。

この機能により、再ベースライン プロセスが不要になり、移行後もバックアップを続行できるようになります。この機能は、FlexVol と FlexGroup の両方をサポートし、ワークロード移行シナリオで役立ち、ONTAPバージョン 9.16.1 以降で利用できます。



この機能は、2025 年 5 月にリリースされたNetApp Backup and Recoveryバージョン 4.0.3 以降で利用できます。

SnapMirror to Cloud Resync は、環境間でバックアップの継続性を維持し、ハイブリッドおよびマルチクラウド設定でのデータ管理を容易にします。



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

開始する前に

次の前提条件が満たされていることを確認してください。

- 宛先ONTAPクラスタでは、ONTAPバージョン 9.16.1 以降が実行されている必要があります。
- 古いソースONTAPクラスタは、NetApp Backup and Recoveryを使用して保護する必要があります。
- SnapMirror to Cloud Resync 機能は、2025 年 5 月にリリースされたNetApp Backup and Recoveryバージョン 4.0.3 以降で利用できます。
- オブジェクト ストレージ内の最新のバックアップが、古いソース、新しいソース、およびオブジェクトストア全体の共通スナップショットであることを確認します。オブジェクト ストレージにバックアップされた最新のスナップショットよりも古い共通スナップショットを使用しないでください。
- 再同期操作を開始する前に、古いONTAPクラスタで使用されていたスナップショット ポリシーとSnapMirrorポリシーの両方を、新しいONTAPクラスタに作成する必要があります。再同期プロセスでポリシーを使用する場合は、そのポリシーも作成する必要があります。再同期操作ではポリシーは作成されません。
- 移行ボリュームのSnapMirror関係に適用されるSnapMirrorポリシーに、クラウド関係で使用されるものと同じラベルが含まれていることを確認します。問題を回避するには、ボリュームとすべてのスナップショットの正確なミラーを管理するポリシーを使用します。



SVM-Migrate、SVM-DR、またはヘッドスワップ方式を使用した移行後のSnapMirrorから Cloud Resync への転送は現在サポートされていません。

NetApp Backup and RecoverySnapMirrorからクラウド再同期への仕組み

技術的な更新を完了したり、ボリュームを 1 つのONTAPクラスタから別のクラスタに移行したりする場合には、バックアップが中断されることなく継続して機能することが重要です。NetApp Backup and Recovery SnapMirror to Cloud Resync は、ボリュームの移行後もクラウドバックアップの一貫性が維持されるようにすることで、この問題を解決します。

次に例を示します。

Vol1a というオンプレミスのボリュームがあるとします。このボリュームには、S1、S2、S3 の 3 つのスナップショットがあります。これらのスナップショットは復元ポイントです。Vol1 は SnapMirror to Cloud (SM-C) を使用してクラウドにバックアップされていますが、オブジェクトストアには S1 と S2 のみが存在します。

ここで、Vol1 を別の ONTAP クラスタに移行します。これを行うには、Vol1b という新しいクラウド ボリュームへの SnapMirror 論理レプリケーション (LRSE) 関係を作成します。これにより、3 つのスナップショット (S1、S2、S3) すべてが Vol1a から Vol1b に転送されます。

移行が完了すると、次の設定になります。

- 元の SM-C 関係 (Vol1a → オブジェクトストア) は削除されます。
- LRSE 関係 (Vol1a → Vol1b) も削除されます。
- Vol1b がアクティブ ボリュームになりました。

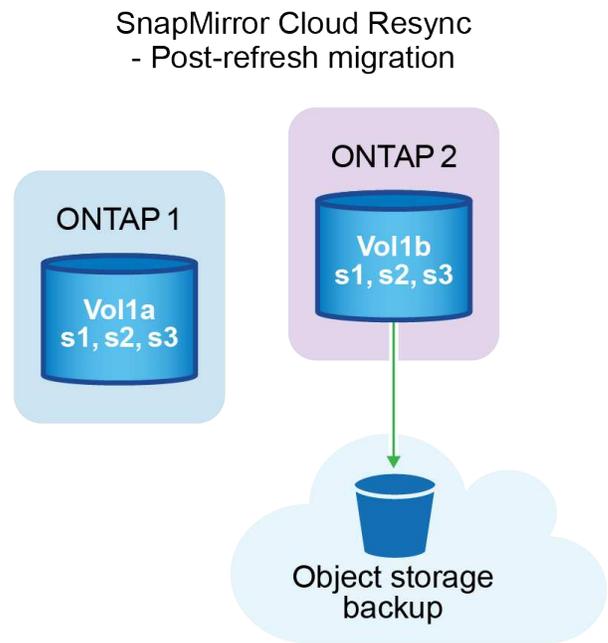
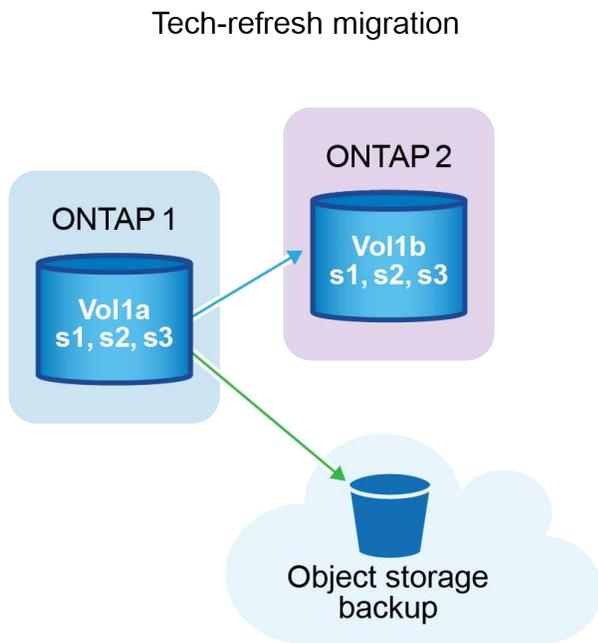
この時点で、Vol1b を同じクラウド エンドポイントにバックアップし続ける必要があります。ただし、最初から完全なバックアップを開始する代わりに (時間とリソースがかかります)、SnapMirror を使用して Cloud Resync を実行します。

再同期の仕組みは次のとおりです。

- システムは、Vol1a とオブジェクトストア間の共通スナップショットをチェックします。この場合、両方とも S2 を持ちます。
- この共有スナップショットにより、システムは S2 と S3 間の増分変更のみを転送する必要があります。

つまり、ボリューム全体ではなく、S2 以降に追加された新しいデータのみがオブジェクトストアに送信されます。

このプロセスにより、重複したバックアップが防止され、帯域幅が節約され、移行後もバックアップが継続されます。



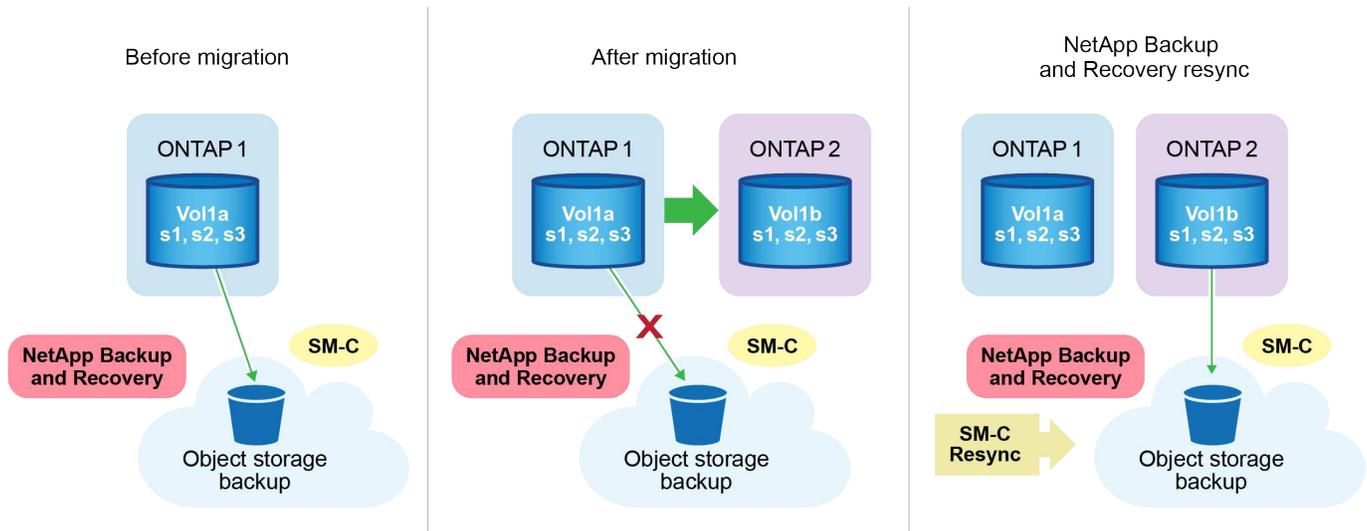
手順に関する注意事項

- 移行と技術更新は、NetApp Backup and Recoveryを使用して実行されません。これらは、専門のサービス チームまたは資格のあるストレージ管理者が実行する必要があります。
- NetApp移行チームは、ボリュームの移動を容易にするために、ソース ONTAP クラスタと宛先ONTAP クラスタの間にSnapMirror関係を作成します。
- 技術更新中の移行がSnapMirrorベースの移行に基づいていることを確認します。

SnapMirrorを使用してボリュームをCloud Resyncに移行する方法

SnapMirrorを使用してボリュームを Cloud Resync に移行するには、次の主要な手順が必要です。各手順については以下で詳しく説明します。

- 移行前のチェックリストに従う: 移行を開始する前に、NetApp Tech Refresh チームは、データの損失を回避し、スムーズな移行プロセスを確実に実行するために、次の前提条件が満たされていることを確認します。
- 移行後のチェックリストに従う: 移行後、NetApp Tech Refresh チームは、保護を確立し、再同期の準備を整えるために次の手順が完了していることを確認します。
- * SnapMirrorからクラウドへの再同期を実行する*: 移行後、NetApp Tech Refresh チームはSnapMirrorからクラウドへの再同期操作を実行し、新しく移行されたボリュームからクラウド バックアップを再開します。



移行前のチェックリストに従う

移行前に、NetApp Tech Refresh チームはこれらの前提条件をチェックして、データの損失を防ぎ、スムーズなプロセスを確保します。

1. 移行するすべてのボリュームがNetApp Backup and Recoveryを使用して保護されていることを確認します。
2. ボリュームインスタンスの UUID を記録します。移行を開始する前に、すべてのボリュームのインスタンス UUID を書き留めておきます。これらの識別子は、後のマッピングおよび再同期操作にとって重要です。
3. SnapMirror関係を削除する前に、各ボリュームの最終スナップショットを取得して最新の状態を保存します。
4. SnapMirrorポリシーを文書化します。各ボリュームの関係に現在添付されているSnapMirrorポリシーを記録します。これは、後でSnapMirrorからクラウドへの再同期プロセス中に必要になります。
5. オブジェクトストアとのSnapMirror Cloud 関係を削除します。
6. 新しいONTAPクラスタとの標準のSnapMirror関係を作成し、ボリュームを新しいターゲットONTAPクラスタに移行します。

移行後のチェックリストに従う

移行後、NetApp Tech Refresh チームは、保護を確立し、再同期の準備を整えるために次の手順が完了していることを確認します。

1. 移行先のONTAPクラスタ内のすべての移行されたボリュームの新しいボリューム インスタンス UUID を記録します。
2. 古いONTAPクラスタで使用可能だったすべての必要なSnapMirrorポリシーが、新しいONTAPクラスタで正しく設定されていることを確認します。
3. コンソールの システム ページで、新しいONTAPクラスタをシステムとして追加します。



ボリューム ID ではなく、ボリューム インスタンス UUID を使用する必要があります。ボリューム インスタンス UUID は移行全体で一貫性が保たれる一意の識別子ですが、ボリューム ID は移行後に変更される可能性があります。

SnapMirrorを実行してクラウドを再同期する

移行後、NetApp Tech Refresh チームはSnapMirror to Cloud Resync 操作を実行し、新しく移行されたボリュームからクラウド バックアップを再開します。

1. コンソールの システム ページで、新しいONTAPクラスタをシステムとして追加します。
2. NetApp Backup and Recoveryボリューム ページを参照して、古いソース システムの詳細が利用可能であることを確認します。
3. NetApp Backup and Recoveryボリューム ページから、バックアップ設定 を選択します。
 - バックアップ設定ページで、[すべて表示] を選択します。
 - 新しいソースの右側にある [アクション...] メニューから、バックアップの再同期 を選択します。
4. 「システムの再同期」 ページで、次の操作を行います。
 - a. 新しいソース システム: ボリュームが移行された新しいONTAPクラスタを入力します。
 - b. 既存のターゲット オブジェクト ストア: 古いソース システムからのバックアップが含まれているターゲット オブジェクト ストアを選択します。
5. 再同期の詳細 Excel シートをダウンロードするには、[CSV テンプレートのダウンロード] を選択します。このシートを使用して、移行するボリュームの詳細を入力します。CSV ファイルに次の詳細を入力します。
 - ソースクラスタの古いボリュームインスタンスUUID
 - 宛先クラスタからの新しいボリュームインスタンスUUID
 - 新しい関係に適用されるSnapMirrorポリシー。
6. ボリューム マッピングの詳細のアップロード の下の アップロード を選択して、完了した CSV シートをNetApp Backup and Recovery UI にアップロードします。



ボリューム ID ではなく、ボリューム インスタンス UUID を使用する必要があります。ボリューム インスタンス UUID は移行全体で一貫性が保たれる一意の識別子ですが、ボリューム ID は移行後に変更される可能性があります。

7. 再同期操作に必要なプロバイダーとネットワーク構成情報を入力します。
8. 検証プロセスを開始するには、[送信] を選択します。

NetApp Backup and Recovery は、再同期対象として選択された各ボリュームが最新のスナップショットであり、少なくとも 1 つの共通スナップショットがあることを検証します。これにより、ボリュームがSnapMirrorから Cloud Resync 操作の準備が整っていることが保証されます。

9. 新しいソース ボリューム名や各ボリュームの再同期ステータスなどの検証結果を確認します。
10. ボリュームの適格性を確認します。システムはボリュームが再同期の対象となるかどうかを確認します。ボリュームが不適格な場合は、最新のスナップショットではないか、共通のスナップショットが見つからなかったことを意味します。



ボリュームがSnapMirrorから Cloud Resync への操作の対象であり続けるようにするには、移行前のフェーズでSnapMirror関係を削除する前に、各ボリュームの最終スナップショットを作成します。これにより、データの最新の状態が保持されます。

11. 再同期操作を開始するには、「再同期」を選択します。システムは最新の共通スナップショットを使用し

て増分変更のみを転送し、バックアップの継続性を保証します。

12. ジョブ モニター ページで再同期プロセスを監視します。

ダークサイトでのNetApp Backup and Recovery構成データの復元

インターネットにアクセスできないサイトでNetApp Backup and Recoveryを使用する場合 (プライベート モード と呼ばれます)、 NetApp Backup and Recovery の構成データは、バックアップが保存されているStorageGRIDまたはONTAP S3 バケットにバックアップされます。コンソール エージェント ホスト システムに問題がある場合は、新しいコンソール エージェントを展開して、重要なNetApp Backup and Recoveryデータを復元できます。



この手順はONTAPボリューム データにのみ適用されます。

クラウド プロバイダーまたはインターネットに接続された独自のホストにコンソール エージェントを導入した SaaS 環境でNetApp Backup and Recoveryを使用すると、システムによってクラウド内のすべての重要な構成データがバックアップされ、保護されます。コンソール エージェントに問題がある場合は、新しいコンソール エージェントを作成し、システムを追加します。バックアップの詳細は自動的に復元されます。

バックアップされるデータには 2 種類あります。

- NetApp Backup and Recoveryデータベース - すべてのボリューム、バックアップ ファイル、バックアップ ポリシー、および構成情報のリストが含まれています。
- インデックス カタログ ファイル - 検索と復元機能に使用される詳細なインデックスが含まれており、復元するボリューム データを探すときに、検索を非常に迅速かつ効率的に行うことができます。

このデータは 1 日に 1 回深夜にバックアップされ、各ファイルの最大 7 つのコピーが保持されます。コンソール エージェントが複数のオンプレミスのONTAPシステムを管理している場合、 NetApp Backup and Recoveryファイルは、最初にアクティブ化されたシステムのバケットに保存されます。



NetApp Backup and Recoveryデータベースまたはインデックス カタログ ファイルにはボリューム データは含まれません。

NetApp Backup and Recoveryデータを新しいコンソール エージェントに復元します

オンプレミスのコンソール エージェントが動作を停止した場合は、新しいコンソール エージェントをインストールし、 NetApp Backup and Recoveryデータを新しいコンソール エージェントに復元する必要があります。

NetApp Backup and Recoveryシステムを動作状態に戻すには、次のタスクを実行する必要があります。

- 新しいコンソールエージェントをインストールする
- NetApp Backup and Recoveryデータベースを復元する
- インデックスカタログファイルを復元する
- オンプレミスのONTAPシステムとStorageGRIDシステムをすべてNetApp ConsoleUIに再検出します。

システムが動作していることを確認したら、新しいバックアップ ファイルを作成します。

要件

バックアップ ファイルが保存されているStorageGRIDまたはONTAP S3 バケットから最新のデータベースとインデックスのバックアップにアクセスする必要があります。

- NetApp Backup and RecoveryMySQL データベース ファイル

このファイルはバケット内の次の場所にあります netapp-backup-<GUID>/mysql_backup/`と名付けられています `CBS_DB_Backup_<day>_<month>_<year>.sql。

- インデックスカタログのバックアップ zip ファイル

このファイルはバケット内の次の場所にあります netapp-backup-<GUID>/catalog_backup/`と名付けられています `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip。

新しいオンプレミス Linux ホストに新しいコンソール エージェントをインストールする

新しいコンソール エージェントをインストールするときは、元のエージェントと同じソフトウェア バージョンをダウンロードします。NetApp Backup and Recoveryデータベースを変更すると、新しいソフトウェア バージョンが古いデータベース バックアップで動作しなくなる可能性があります。あなたはできる **"バックアップデータベースを復元した後、コンソールエージェントソフトウェアを最新バージョンにアップグレードします。"**。

1. ["新しいオンプレミス Linux ホストにコンソール エージェントをインストールする"](#)
2. 先ほど作成した管理者ユーザーの資格情報を使用してコンソールにログインします。

NetApp Backup and Recoveryデータベースを復元する

1. バックアップ場所から新しいコンソール エージェント ホストに MySQL バックアップをコピーします。以下では、サンプルファイル名「CBS_DB_Backup_23_05_2023.sql」を使用します。
2. Docker コンテナまたは Podman コンテナのどちらを使用しているかに応じて、次のいずれかのコマンドを使用して、バックアップを MySQL Docker コンテナにコピーします。

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Docker コンテナまたは Podman コンテナのどちらを使用しているかに応じて、次のいずれかのコマンドを使用して MySQL コンテナ シェルに入ります。

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. コンテナ シェルで、「env」をデプロイします。
5. MySQL DB パスワードが必要になるので、キー「MYSQL_ROOT_PASSWORD」の値をコピーします。
6. 次のコマンドを使用して、NetApp Backup and Recovery MySQL DB を復元します。

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 次の SQL コマンドを使用して、NetApp Backup and Recovery MySQL DB が正しく復元されたことを確認します。

```
mysql -u root -p cloud_backup
```

8. パスワードを入力してください。

```
mysql> show tables;  
mysql> select * from volume;
```

9. 表示されるボリュームが元の環境に存在していたボリュームと同じであることを確認します。

インデックスカタログファイルを復元する

1. インデックス付きカタログのバックアップ zip ファイル (サンプル ファイル名は「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」を使用します) を、バックアップ場所から「/opt/application/netapp/cbs」フォルダー内の新しいコンソール エージェント ホストにコピーします。
2. 次のコマンドを使用して、「Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip」ファイルを解凍します。

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. **ls** コマンドを実行して、フォルダー「catalogdb1」が作成され、その下にサブフォルダー「changes」と「snapshots」が作成されていることを確認します。

ONTAP クラスタと StorageGRID システムを発見

1. ["オンプレミスのONTAPシステムをすべて見る"](#)以前の環境で利用可能でした。これには、S3 サーバーとして使用したONTAPシステムが含まれます。
2. ["StorageGRIDシステムを発見"](#)。

StorageGRID 環境の詳細を設定する

元のコンソールエージェントセットアップで設定されたとおりに、ONTAPシステムに関連付けられたStorageGRIDシステムの詳細を追加します。 ["NetApp ConsoleAPI"](#)。

次の情報は、NetApp Console3.9.xx 以降のプライベート モード インストールに適用されます。古いバージョン

ンの場合は、次の手順に従います。"DarkSite クラウドバックアップ: MySQL とインデックスカタログのバックアップと復元"。

StorageGRIDにデータをバックアップするシステムごとにこれらの手順を実行する必要があります。

1. 次の oauth/token API を使用して認証トークンを抽出します。

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"password"}'> '
```

IP アドレス、ユーザー名、パスワードはカスタム値ですが、アカウント名はカスタム値ではありません。アカウント名は常に「account-DARKSITE1」になります。また、ユーザー名には電子メール形式の名前を使用する必要があります。

この API は次のような応答を返します。認証トークンは以下のように取得できます。

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbnB9uYW1lIjoiYWRTaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWx1IiwiaWF0IjoxNjc5NzY2MDIzLCJleHAiOiE2NzI3NTc2MjMsImIzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CjRrRDY23PokyLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykODNDmrv5At_f9HHp0-xVMYHqywZ4nNFalMvAh4xEsc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSolIwIeHXZJJV-Uswun9daNgiYd_wX-4WWJVIGEnDzzwOKfUoUoelFg3ch--7JFkFl-rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. tenancy/external/resource API を使用して、システム ID と X-Agent-Id を抽出します。

ともできます。



ストレージ システム上またはクラウド プロバイダー環境からバックアップ ファイルを直接管理または変更しないでください。これによりファイルが破損し、サポートされない構成になる可能性があります。



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

システム内のボリュームのバックアップステータスを表示します

ボリューム バックアップ ダッシュボードで、現在バックアップ中のすべてのボリュームのリストを表示できます。これには、スナップショット、複製されたボリューム、オブジェクト ストレージ内のバックアップ ファイルなど、すべての種類のバックアップが含まれます。現在バックアップされていないシステム内のボリュームを表示することもできます。

手順

1. コンソール メニューから、保護 > バックアップとリカバリ を選択します。
2. ボリューム メニューを選択して、Cloud Volumes ONTAPおよびオンプレミスのONTAPシステムのバックアップされたボリュームのリストを表示します。
3. 特定のシステム内の特定のボリュームを探している場合は、システムとボリューム別にリストを絞り込むことができます。検索フィルターを使用したり、ボリューム スタイル (FlexVolまたはFlexGroup)、ボリューム タイプなどに基づいて列を並べ替えたりすることもできます。

追加の列 (集計、セキュリティ スタイル (Windows または UNIX) 、スナップショット ポリシー、レプリケーション ポリシー、バックアップ ポリシー) を表示するには、プラス記号を選択します。

4. 「既存の保護」列で保護オプションのステータスを確認します。3つのアイコンは、「ローカル スナップショット」、「複製されたボリューム」、「オブジェクト ストレージ内のバックアップ」を表します。

各アイコンは、そのバックアップ タイプがアクティブになっているときは点灯し、バックアップ タイプが非アクティブになっているときは灰色になります。各アイコンの上にカーソルを置くと、使用されているバックアップ ポリシーや、各バックアップ タイプに関するその他の関連情報が表示されます。

システム内の追加ボリュームでバックアップを有効にする

NetApp Backup and Recovery を最初に有効にしたときに、システム内の一部のボリュームでのみバックアップをアクティブ化した場合は、後で追加のボリュームでバックアップをアクティブ化できます。

手順

1. ボリューム*タブから、バックアップをアクティブ化するボリュームを特定し、アクションメニューを選択します。... 行の末尾にある **[*3-2-1 保護を有効にする]** を選択します。
2. [バックアップ戦略の定義] ページで、バックアップ アーキテクチャを選択し、ローカル スナップショット、レプリケートされたボリューム、およびバックアップ ファイルのポリシーとその他の詳細を定義します。このシステムでアクティブ化した初期ボリュームからのバックアップ オプションの詳細を参照してください。次に「次へ」を選択します。
3. このボリュームのバックアップ設定を確認し、「バックアップのアクティブ化」を選択します。

既存のボリュームに割り当てられたバックアップ設定を変更する

ポリシーが割り当てられている既存のボリュームに割り当てられたバックアップ ポリシーを変更できます。ローカル スナップショット、複製されたボリューム、およびバックアップ ファイルのポリシーを変更できます。ボリュームに適用する新しいスナップショット、レプリケーション、またはバックアップ ポリシーがすでに存在している必要があります。

単一ボリュームのバックアップ設定を編集する

手順

1. ボリューム*メニューから、ポリシー設定を変更するボリュームを見つけ、アクションメニューを選択します。*** 行の末尾にある [*バックアップ戦略の編集] を選択します。
2. [バックアップ戦略の編集] ページで、ローカル スナップショット、複製されたボリューム、およびバックアップ ファイルの既存のバックアップ ポリシーを変更し、[次へ] を選択します。

このクラスターのNetApp Backup and Recovery をアクティブ化するときに、初期バックアップ ポリシーでクラウド バックアップに対して *DataLock* と *Ransomware Resilience* を有効にした場合は、DataLock で構成された他のポリシーのみが表示されます。また、NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock が設定されていない他のクラウド バックアップ ポリシーのみが表示されます。

3. このボリュームのバックアップ設定を確認し、「バックアップのアクティブ化」を選択します。

複数のボリュームのバックアップ設定を編集する

複数のボリュームで同じバックアップ設定を使用する場合は、複数のボリュームで同時にバックアップ設定をアクティブ化または編集できます。バックアップ設定がないボリューム、スナップショット設定のみがあるボリューム、クラウドへのバックアップ設定のみがあるボリュームなどを選択し、さまざまなバックアップ設定を持つこれらすべてのボリュームに対して一括変更を行うことができます。

複数のボリュームを操作する場合、すべてのボリュームに次の共通の特性が必要です。

- 同じシステム
- 同じスタイル (FlexVolまたはFlexGroupボリューム)
- 同じタイプ (読み取り/書き込みまたはデータ保護ボリューム)

バックアップに5つ以上のボリュームが有効になっている場合、NetApp Backup and Recovery は一度に5つのボリュームのみを初期化します。これらが完了すると、すべてのボリュームが初期化されるまで5つのグループごとに続行されます。

手順

1. ボリューム タブから、ボリュームが存在するシステムでフィルタリングします。
2. バックアップ設定を管理するボリュームをすべて選択します。
3. 設定するバックアップ アクションの種類に応じて、[一括アクション] メニューのボタンをクリックします。

バックアップアクション...	このボタンを選択してください...
スナップショットバックアップ設定を管理する	ローカルスナップショットの管理

バックアップアクション...	このボタンを選択してください...
レプリケーションバックアップ設定を管理する	レプリケーションの管理
クラウドへのバックアップ設定を管理する	バックアップの管理
複数の種類のバックアップ設定を管理します。このオプションを使用すると、バックアップ アーキテクチャも変更できます。	バックアップとリカバリの管理

- 表示されるバックアップ ページで、ローカル スナップショット、複製されたボリューム、またはバックアップ ファイルの既存のバックアップ ポリシーを変更し、[保存] を選択します。

このクラスターのNetApp Backup and Recovery をアクティブ化するとき、初期バックアップ ポリシーでクラウド バックアップに対して *DataLock* と *Ransomware Resilience* を有効にした場合は、DataLock で構成された他のポリシーのみが表示されます。また、NetApp Backup and Recoveryをアクティブ化するとき *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock が設定されていない他のクラウド バックアップ ポリシーのみが表示されます。

いつでも手動でボリュームバックアップを作成

いつでもオンデマンド バックアップを作成して、ボリュームの現在の状態をキャプチャできます。これは、ボリュームに非常に重要な変更が加えられ、そのデータを保護するために次のスケジュールされたバックアップまで待ちたくない場合に役立ちます。この機能を使用すると、現在バックアップされていないボリュームのバックアップを作成し、その現在の状態をキャプチャすることもできます。

ボリュームのオブジェクト ストアにアドホック スナップショットまたはバックアップを作成できます。アドホック複製ボリュームを作成することはできません。

バックアップ名にはタイムスタンプが含まれるため、オンデマンド バックアップを他のスケジュールされたバックアップと区別できます。

このクラスターのNetApp Backup and Recovery をアクティブ化するとき *DataLock* と *Ransomware Resilience* を有効にした場合、オンデマンド バックアップも DataLock で構成され、保持期間は 30 日間になります。アドホック バックアップではランサムウェア スキャンはサポートされていません。["DataLockとランサムウェア対策について詳しくはこちら"](#)。

アドホック バックアップを作成すると、ソース ボリュームにスナップショットが作成されます。このスナップショットは通常のスナップショット スケジュールの一部ではないため、オフにはなりません。バックアップが完了したら、ソース ボリュームからこのスナップショットを手動で削除することをお勧めします。これにより、このスナップショット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-`。"[ONTAP CLIを使用してスナップショットを削除する方法をご覧ください](#)"。



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ていません。

手順

- ボリューム*タブから、...ボリュームを選択し、[*バックアップ]>[アドホック バックアップの作成*] を選択します。

バックアップが作成されるまで、そのボリュームのバックアップ ステータス列には「進行中」と表示されません。

各ボリュームのバックアップのリストを表示する

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、宛先の場所、最後に実行されたバックアップ、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。

手順

1. *ボリューム*タブから、...ソースボリュームの[ボリュームの詳細を表示]を選択します。

ボリュームの詳細とスナップショットのリストが表示されます。

2. スナップショット、レプリケーション、または*バックアップ*を選択すると、各バックアップ タイプの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。

オブジェクトストレージ内のボリュームバックアップでランサムウェアスキャンを実行する

NetApp Backup and Recovery は、オブジェクト ファイルへのバックアップが作成される際、およびバックアップ ファイルからデータが復元される際に、バックアップ ファイルをスキャンしてランサムウェア攻撃の証拠を探します。また、いつでもオンデマンド スキャンを実行して、オブジェクト ストレージ内の特定のバックアップ ファイルの使用可能かどうかを確認することもできます。これは、特定のボリュームでランサムウェアの問題が発生し、そのボリュームのバックアップが影響を受けていないことを確認したい場合に役立ちます。

この機能は、ボリューム バックアップがONTAP 9.11.1 以降のシステムから作成され、オブジェクトへのバックアップ ポリシーで *DataLock* および *Ransomware Resilience* が有効になっている場合にのみ使用できます。

手順

1. *ボリューム*タブから、...ソースボリュームの[ボリュームの詳細を表示]を選択します。

ボリュームの詳細が表示されます。

2. バックアップ を選択すると、オブジェクト ストレージ内のバックアップ ファイルのリストが表示されます。
3. 選択...ランサムウェアをスキャンするボリューム バックアップ ファイルを選択し、[ランサムウェアのスキャン] をクリックします。

ランサムウェア耐性列には、スキャンが進行中であることが示されます。

ソースボリュームとのレプリケーション関係を管理する

2つのシステム間のデータ レプリケーションを設定したら、データ レプリケーションの関係を管理できます。

手順

1. *ボリューム*タブから、...ソースボリュームに対して*レプリケーション*オプションを選択します。利用可能なオプションをすべて確認できます。
2. 実行するレプリケーション アクションを選択します。

次の表では、利用可能なアクションについて説明します。

アクション	説明
ビューのレプリケーション	ボリューム関係の詳細（転送情報、最終転送情報、ボリュームの詳細、関係に割り当てられた保護ポリシーに関する情報）を表示します。
更新レプリケーション	増分転送を開始し、宛先ボリュームを更新してソース ボリュームと同期させます。
レプリケーションを一時停止	スナップショットの増分転送を一時停止して、宛先ボリュームを更新します。増分更新を再開したい場合は、後で再開できます。
レプリケーションを中断する	ソース ボリュームと宛先ボリュームの関係を解除し、宛先ボリュームをデータ アクセス用にアクティブ化して、読み取り/書き込み可能にします。このオプションは通常、データの破損、誤った削除、オフライン状態などのイベントによりソース ボリュームがデータを提供できない場合に使用されます。 https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html ["ONTAPドキュメントで、データアクセス用に宛先ボリュームを設定し、ソースボリュームを再アクティブ化する方法について学習します。"]
レプリケーションを中止する	このボリュームの宛先システムへのバックアップを無効にし、ボリュームを復元する機能も無効にします。既存のバックアップは削除されません。これによって、ソース ボリュームと宛先ボリューム間のデータ保護関係は削除されません。
逆再同期	ソース ボリュームと宛先ボリュームの役割を逆にします。元のソース ボリュームの内容は、宛先ボリュームの内容によって上書きされます。これは、オフラインになったソース ボリュームを再アクティブ化する場合に役立ちます。最後のデータ複製からソース ボリュームが無効になった時点までの間に元のソース ボリュームに書き込まれたデータは保持されません。
関係の削除	ソース ボリュームと宛先ボリューム間のデータ保護関係を削除します。これにより、ボリューム間でデータのレプリケーションは行われなくなります。このアクションでは、データ アクセス用に宛先ボリュームがアクティブ化されません。つまり、読み取り/書き込み可能になりません。システム間に他のデータ保護関係がない場合、このアクションにより、クラスタ ピア関係とストレージ VM (SVM) ピア関係も削除されます。

結果

アクションを選択すると、コンソールは関係を更新します。

既存のクラウドへのバックアップ ポリシーを編集する

システム内の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に影響します。



- このクラスタのNetApp Backup and Recovery をアクティブ化するときに、初期ポリシーで *DataLock* と *Ransomware Resilience* を有効にした場合、編集するポリシーはすべて同じ *DataLock* 設定 (ガバナンスまたはコンプライアンス) で構成する必要があります。また、NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、現在 *DataLock* を有効にすることはできません。
- AWS でバックアップを作成するときに、NetApp Backup and Recoveryをアクティブ化するときに最初のバックアップポリシーで *S3 Glacier* または *S3 Glacier Deep Archive* を選択した場合、バックアップポリシーを編集するときに使用できるアーカイブ層はその層のみになります。また、最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合は、ポリシーを編集するときに、*S3 Glacier* が唯一のアーカイブ オプションになります。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. バックアップ設定 ページで、...ポリシー設定を変更するシステムを選択し、[ポリシーの管理] を選択します。
3. [ポリシーの管理] ページで、そのシステムで変更するバックアップ ポリシーの [編集] を選択します。
4. [ポリシーの編集] ページで下矢印を選択して [ラベルと保持] セクションを展開し、スケジュールやバックアップの保持を変更して [保存] を選択します。

クラスタでONTAP 9.10.1 以降を実行している場合は、一定の日数後にアーカイブ ストレージへのバックアップの階層化を有効または無効にするオプションもあります。

"AWS アーカイブストレージの使用について詳しくはこちら"。"Azure アーカイブ ストレージの使用について詳しく見る"。"Google アーカイブ ストレージの使用について詳しくは、こちらをご覧ください。"。
(ONTAP 9.12.1 が必要です。)

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 ファイルはすべてその階層に残り、標準階層に自動的に戻されないことに注意してください。新しいボリューム バックアップのみが標準層に保存されます。

新しいクラウドへのバックアップポリシーを追加する

システムに対してNetApp Backup and Recovery 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。異なる復旧ポイント目標 (RPO) を持つ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、そのクラスタに追加のポリシーを作成し、それら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。

システム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、まずそのバックアップ ポリシーをシステムに追加する必要があります。そうするとそのシステム内のボリュームにポリシーを適用する。



- このクラスターのNetApp Backup and Recovery をアクティブ化するときに初期ポリシーで *DataLock and Ransomware Resilience* を有効にした場合、作成する追加ポリシーは同じ DataLock 設定 (ガバナンスまたはコンプライアンス) で構成する必要があります。また、NetApp Backup and Recoveryをアクティブ化するときに *DataLock and Ransomware Resilience* を有効にしなかった場合は、DataLock を使用する新しいポリシーを作成することはできません。
- AWS でバックアップを作成するときに、NetApp Backup and Recoveryをアクティブ化するときに最初のバックアップポリシーで *S3 Glacier* または *S3 Glacier Deep Archive* を選択した場合、その層がそのクラスターの将来のバックアップポリシーで使用できる唯一のアーカイブ層になります。また、最初のバックアップ ポリシーでアーカイブ層を選択しなかった場合は、将来のポリシーでは *S3 Glacier* が唯一のアーカイブ オプションになります。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. _バックアップ設定_ ページで、...新しいポリシーを追加するシステムの [ポリシーの管理] を選択します。
3. [ポリシーの管理] ページで、[新しいポリシーの追加] を選択します。
4. [新しいポリシーの追加] ページで下矢印を選択して [ラベルと保持] セクションを展開し、スケジュールとバックアップの保持期間を定義して [保存] を選択します。

クラスターでONTAP 9.10.1 以降を実行している場合は、一定の日数後にアーカイブ ストレージへのバックアップの階層化を有効または無効にするオプションもあります。

"AWS アーカイブストレージの使用について詳しくはこちら"。"Azure アーカイブ ストレージの使用について詳しく見る"。"Google アーカイブ ストレージの使用について詳しくは、こちらをご覧ください。"。
(ONTAP 9.12.1 が必要です。)

バックアップの削除

NetApp Backup and Recovery を使用すると、単一のバックアップ 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、システム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。バックアップが不要になった場合、またはソース ボリュームを削除してすべてのバックアップを削除する場合は、すべてのバックアップを削除する必要がある場合があります。

DataLock とランサムウェア保護を使用してロックしたバックアップ ファイルは削除できません。ロックされたバックアップ ファイルを 1 つ以上選択した場合、UI から「削除」オプションは使用できません。



バックアップがあるシステムまたはクラスターを削除する予定の場合は、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。NetApp Backup and Recoveryでは、システムを削除してもバックアップは自動的に削除されません。また、システムの削除後にバックアップを削除するための UI は現在サポートされていません。残りのバックアップについては、オブジェクト ストレージ コストが引き続き請求されます。

システムのすべてのバックアップファイルを削除する

システムのオブジェクト ストレージ上のすべてのバックアップを削除しても、このシステム内のボリュームの将来のバックアップは無効になりません。システム内のすべてのボリュームのバックアップの作成を停止したい場合は、バックアップを非アクティブ化できます。ここで説明されているように。

このアクションはスナップショットや複製されたボリュームには影響しないことに注意してください。これら

の種類バックアップ ファイルは削除されません。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. 選択...すべてのバックアップを削除するシステムを選択し、[すべてのバックアップを削除]を選択します。
3. 確認ダイアログボックスで、システムの名前を入力します。
4. *詳細設定*を選択します。
5. バックアップの強制削除: すべてのバックアップを強制的に削除するかどうかを指定します。

極端なケースでは、NetApp Backup and Recovery がバックアップにアクセスできないようにする必要があります。これは、たとえば、サービスがバックアップ バケットにアクセスできなくなった場合や、バックアップが DataLock で保護されているが不要になった場合に発生する可能性があります。以前は、これらを自分で削除することはできず、NetAppサポートに連絡する必要がありました。このリリースでは、バックアップを強制的に削除するオプション (ボリューム レベルとシステム レベル) を使用できるようになりました。



このオプションは慎重に使用し、極端なクリーンアップが必要な場合にのみ使用してください。オブジェクト ストレージでバックアップが削除されていない場合でも、NetApp Backup and Recovery はこれらのバックアップにアクセスできなくなります。クラウド プロバイダーにアクセスして、バックアップを手動で削除する必要があります。

6. *削除*を選択します。

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、そのボリュームの今後のバックアップも無効になります。

手順

1. *ボリューム*タブから、...ソースボリュームの[詳細とバックアップリスト]を選択します。
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. アクション > *すべてのバックアップを削除*を選択します。
3. ボリューム名を入力します。
4. *詳細設定*を選択します。
5. バックアップの強制削除: すべてのバックアップを強制的に削除するかどうかを指定します。

極端なケースでは、NetApp Backup and Recovery がバックアップにアクセスできないようにする必要があります。これは、たとえば、サービスがバックアップ バケットにアクセスできなくなった場合や、バックアップが DataLock で保護されているが不要になった場合に発生する可能性があります。以前は、これらを自分で削除することはできず、NetAppサポートに連絡する必要がありました。このリリースでは、バックアップを強制的に削除するオプション (ボリューム レベルとシステム レベル) を使用できるようになりました。



このオプションは慎重に使用し、極端なクリーンアップが必要な場合にのみ使用してください。オブジェクト ストレージでバックアップが削除されていない場合でも、NetApp Backup and Recovery はこれらのバックアップにアクセスできなくなります。クラウド プロバイダーにアクセスして、バックアップを手動で削除する必要があります。

6. *削除*を選択します。

ボリュームの単一のバックアップファイルを削除する

不要になったバックアップ ファイルを 1 つ削除できます。これには、ボリューム スナップショットの単一のバックアップまたはオブジェクト ストレージ内のバックアップの単一のバックアップの削除が含まれます。

複製されたボリューム (データ保護ボリューム) は削除できません。

手順

1. *ボリューム*タブから、**...**ソースボリュームの[ボリュームの詳細を表示]を選択します。

ボリュームの詳細が表示され、スナップショット、レプリケーション、または*バックアップ*を選択して、ボリュームの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。デフォルトでは、利用可能なスナップショットが表示されます。

2. 削除するバックアップ ファイルの種類を確認するには、[スナップショット] または [バックアップ] を選択します。
3. 選択**...**削除するボリューム バックアップ ファイルを選択し、[削除] を選択します。
4. 確認ダイアログボックスで、[削除] を選択します。

ボリュームバックアップ関係を削除する

ボリュームのバックアップ関係を削除すると、新しいバックアップ ファイルの作成を停止し、ソース ボリュームを削除しながら、既存のバックアップ ファイルはすべて保持する場合に、アーカイブ メカニズムが提供されます。これにより、ソース ストレージ システムのスペースをクリアしながら、必要に応じて将来バックアップ ファイルからボリュームを復元できるようになります。

必ずしもソースボリュームを削除する必要はありません。ボリュームのバックアップ関係を削除し、ソース ボリュームを保持することができます。この場合、後でボリューム上のバックアップを「アクティブ化」することができます。この場合、元のベースライン バックアップ コピーが引き続き使用されます。新しいベースライン バックアップ コピーは作成されず、クラウドにエクスポートされません。バックアップ関係を再アクティブ化すると、ボリュームにはデフォルトのバックアップ ポリシーが割り当てられることに注意してください。

この機能は、システムでONTAP 9.12.1 以降を実行している場合にのみ使用できます。

NetApp Backup and Recoveryユーザー インターフェイスからソース ボリュームを削除することはできません。ただし、コンソールの*システム*ページでボリュームの詳細ページを開いて、"[そこからボリュームを削除します](#)"。



関係が削除されると、個々のボリュームのバックアップ ファイルを削除することはできません。ただし、ボリュームのすべてのバックアップを削除することは可能です。

手順

1. ボリューム*タブから、...ソースボリュームの*バックアップ>*関係の削除*を選択します。

システムのNetApp Backup and Recoveryを非アクティブ化する

システムに対してNetApp Backup and Recoveryを非アクティブ化すると、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、ボリュームを復元する機能も無効になります。既存のバックアップは削除されません。これにより、このシステムからバックアップサービスの登録が解除されるわけではありません。基本的には、すべてのバックアップおよび復元アクティビティを一定期間一時停止できるようになります。

バックアップに使用する容量については、クラウドプロバイダーからオブジェクトストレージの料金が引き続き請求されます。[バックアップを削除する](#)。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. [_バックアップ設定ページ_](#)から、...バックアップを無効にするシステムで、[バックアップの無効化]を選択します。
3. 確認ダイアログボックスで、「非アクティブ化」を選択します。



バックアップが無効になっている間、そのシステムに対してバックアップをアクティブ化 ボタンが表示されます。そのシステムのバックアップ機能を再度有効にする場合は、このボタンを選択できます。

システムのNetApp Backup and Recoveryの登録を解除する

バックアップ機能を使用する必要がなくなり、そのシステムでのバックアップに対する課金を停止したい場合は、システムのNetApp Backup and Recovery の登録を解除できます。通常、この機能は、システムを削除する予定があり、バックアップ サービスをキャンセルする場合に使用されます。

クラスターのバックアップが保存される宛先オブジェクト ストアを変更する場合にも、この機能を使用できます。システムからNetApp Backup and Recoveryを登録解除した後、新しいクラウド プロバイダー情報を使用してそのクラスターに対してNetApp Backup and Recovery を有効にすることができます。

NetApp Backup and Recoveryを登録解除する前に、次の手順をこの順序で実行する必要があります。

- システムのNetApp Backup and Recoveryを無効にします
- そのシステムのすべてのバックアップを削除します

これら 2 つのアクションが完了するまで、登録解除オプションは使用できません。

手順

1. *ボリューム*タブから*バックアップ設定*を選択します。
2. [_バックアップ設定ページ_](#)から、...バックアップ サービスを登録解除するシステムで、[登録解除]を選択します。
3. 確認ダイアログボックスで、[登録解除]を選択します。

ONTAPバックアップからの復元

NetApp Backup and Recoveryを使用してバックアップファイルから**ONTAP**データを復元する

ONTAPボリュームデータのバックアップは、スナップショットとして、複製されたボリューム上、またはオブジェクトストレージに保存されます。特定の時点でこれらのいずれかの場所からデータを復元できます。NetApp Backup and Recoveryを使用すると、必要に応じてボリューム全体、フォルダ、または個々のファイルを復元できます。



NetApp Backup and Recoveryのワークロードを切り替えるには、"[さまざまなNetApp Backup and Recoveryワークロードに切り替える](#)"。

- ボリューム (新しいボリュームとして) を元のシステム、同じクラウド アカウントを使用している別のシステム、またはオンプレミスのONTAPシステムに復元できます。
- フォルダー を元のシステムのボリューム、同じクラウド アカウントを使用している別のシステムのボリューム、またはオンプレミスのONTAPシステム上のボリュームに復元できます。
- ファイル を元のシステムのボリューム、同じクラウド アカウントを使用している別のシステムのボリューム、またはオンプレミスのONTAPシステム上のボリュームに復元できます。

実稼働システムにデータを復元するには、有効なNetApp Backup and Recoveryライセンスが必要です。

要約すると、ボリューム データをONTAPシステムに復元するために使用できる有効なフローは次のとおりです。

- バックアップファイル → 復元されたボリューム
- 複製されたボリューム → 復元されたボリューム
- スナップショット → 復元されたボリューム



復元操作が完了しない場合は、ジョブ モニターに「失敗」と表示されるまで待ってから、復元操作を再試行してください。



ONTAPデータのリストアに関する制限については、"[ONTAPボリュームのバックアップとリストアの制限](#)"。

復元ダッシュボード

復元ダッシュボードを使用して、ボリューム、フォルダー、およびファイルの復元操作を実行します。復元ダッシュボードにアクセスするには、コンソール メニューから [バックアップと復元] を選択し、[復元] タブを選択します。選択することもできます  > サービス パネルのバックアップと復元サービスから 復元ダッシュボードを表示 します。



NetApp Backup and Recovery は少なくとも 1 つのシステムに対してすでにアクティブ化されており、初期バックアップ ファイルが存在している必要があります。

復元ダッシュボードでは、バックアップ ファイルからデータを復元する方法として、「参照と復元」と「検

索と復元」の2つの方法が提供されています。

参照と復元と検索と復元の比較

一般的に言えば、参照と復元は、過去1週間または1か月間の特定のボリューム、フォルダー、またはファイルを復元する必要がある場合に適しています。この場合、ファイルの名前と場所、およびファイルが最後に正常な状態であった日付が分かっています。通常、ボリューム、フォルダー、またはファイルを復元する必要があるが、正確な名前や、それらが存在するボリューム、またはそれらが最後に正常な状態であった日付を覚えていない場合は、検索と復元の方が適しています。

この表は、2つの方法の機能の比較を示しています。

閲覧と復元	検索と復元
フォルダー形式の構造を参照して、単一のバックアップファイル内のボリューム、フォルダー、またはファイルを見つけます。	部分的または完全なボリューム名、部分的または完全なフォルダー/ファイル名、サイズの範囲、追加の検索フィルターを使用して、すべてのバックアップファイル間でボリューム、フォルダー、またはファイルを検索します。
ファイルが削除または名前変更され、ユーザーが元のファイル名を知らない場合、ファイルの回復は処理されません。	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を処理します
クイック復元がサポートされています。	クイック復元はサポートされていません。

この表には、バックアップファイルが存在する場所に基づいて、有効な復元操作の一覧が示されています。

バックアップタイプ	閲覧と復元			検索と復元		
	ボリュームを復元	ファイルを復元	フォルダを復元	ボリュームを復元	ファイルを復元	フォルダを復元
Snapshot	はい	いいえ	いいえ	はい	はい	はい
複製ボリューム	はい	いいえ	いいえ	はい	はい	はい
バックアップファイル	はい	はい	はい	はい	はい	はい

いずれかの復元方法を使用する前に、リソース要件を満たすように環境を構成します。詳細については、次のセクションを参照してください。

使用する復元操作の種類に応じた要件と復元手順を参照してください。

- ["参照と復元を使用してボリュームを復元する"](#)
- ["参照と復元を使用してフォルダとファイルを復元する"](#)
- ["検索と復元を使用してボリューム、フォルダ、ファイルを復元する"](#)

検索と復元を使用してONTAPバックアップから復元する

検索と復元を使用して、ONTAPバックアップファイルからボリューム、フォルダー、

またはファイルを回復できます。検索と復元を使用すると、正確なシステム名、ボリューム名、ファイル名を必要とせずに、すべてのバックアップ (ローカル スナップショット、複製されたボリューム、オブジェクト ストレージを含む) を検索できます。

通常、ローカル スナップショットまたは複製されたボリュームからの復元は、オブジェクト ストレージからの復元よりも高速でコストも低くなります。

ボリューム全体を復元する場合、NetApp Backup and Recovery はバックアップ データを使用して新しいボリュームを作成します。元のシステム、同じクラウド アカウント内の別のシステム、またはオンプレミスのONTAPシステムに復元できます。フォルダーとファイルは、元の場所、同じシステム内の別のボリューム、同じクラウド アカウント内の別のシステム、またはオンプレミス システムに復元できます。

復元機能はONTAP のバージョンによって異なります。

- フォルダ: ONTAP 9.13.0 以降を使用すると、すべてのファイルとサブフォルダを含むフォルダを復元できます。それ以前のバージョンでは、フォルダ内のファイルのみを復元できます。
- アーカイブ ストレージ: アーカイブ ストレージ (ONTAP 9.10.1 以降で利用可能) からの復元は遅くなり、追加コストが発生する可能性があります。
- 宛先クラスタの要件:
 - ボリュームリストア: ONTAP 9.10.1 以上
 - ファイル復元: ONTAP 9.11.1 以上
 - Google Archive およびStorageGRID: ONTAP 9.12.1 以上
 - フォルダの復元: ONTAP 9.13.1 以上

["AWSアーカイブストレージからの復元の詳細"](#)。 ["Azure アーカイブ ストレージからの復元の詳細"](#)。 ["Google アーカイブ ストレージからの復元の詳細"](#)。



- オブジェクト ストレージ内のバックアップ ファイルに DataLock および Ransomware 保護が設定されている場合、ONTAPバージョンが 9.13.1 以上の場合にのみフォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、バックアップ ファイルからボリューム全体を復元し、必要なフォルダーとファイルにアクセスできます。
- オブジェクト ストレージ内のバックアップ ファイルがアーカイブ ストレージに存在する場合、ONTAPバージョンが 9.13.1 以上の場合にのみ、フォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、アーカイブされていない新しいバックアップ ファイルからフォルダを復元するか、アーカイブされたバックアップからボリューム全体を復元して、必要なフォルダとファイルにアクセスすることができます。
- Azure アーカイブ ストレージからStorageGRIDシステムにデータを復元する場合、「高」復元優先度はサポートされません。
- 現在、ONTAP S3 オブジェクト ストレージ内のボリュームからのフォルダーの復元はサポートされていません。

開始する前に、復元するボリュームまたはファイルの名前または場所をある程度把握しておく必要があります。

検索と復元がサポートされているシステムとオブジェクト ストレージ プロバイダー

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから、次のシステムにONTAPデータを復元できます。スナップショットはソース システム上に存在し、同じシステムにのみ復元できます。

注意: ボリュームとファイルはどのタイプのバックアップ ファイルからでも復元できますが、現時点では、フォルダーを復元できるのはオブジェクト ストレージ内のバックアップ ファイルからのみです。

バックアップファイルの場所		宛先システム
オブジェクトストア (バックアップ)	セカンダリシステム (レプリケーション)	
Amazon S3	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP	AWS オンプレミスONTAPシステムのCloud Volumes ONTAP
Azure ブロブ	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム
Google Cloud Storage	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
NetAppStorageGRID	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム
ONTAP S3	オンプレミスのONTAPシステムCloud Volumes ONTAP	オンプレミスのONTAPシステム

検索と復元の場合、コンソール エージェントは次の場所にインストールできます。

- Amazon S3の場合、コンソールエージェントはAWSまたはオンプレミスに導入できます。
- Azure Blobの場合、コンソールエージェントはAzureまたはオンプレミスに展開できます。
- Google Cloud Storage の場合、コンソール エージェントを Google Cloud Platform VPC にデプロイする必要があります。
- StorageGRIDの場合、コンソールエージェントは、インターネットアクセスの有無にかかわらず、お客様の敷地内に導入する必要があります。
- ONTAP S3の場合、コンソールエージェントは、オンプレミス (インターネットアクセスの有無にかかわらず) またはクラウドプロバイダー環境に導入できます。

「オンプレミスのONTAPシステム」への参照には、FAS、AFF、およびONTAP Selectシステムが含まれることに注意してください。

検索と復元の前条件

検索と復元を有効にする前に、環境が次の要件を満たしていることを確認してください。

- クラスタの要件：
 - ONTAPバージョンは 9.8 以上である必要があります。
 - ボリュームが存在するストレージ VM (SVM) には、データ LIF が設定されている必要があります。
 - ボリューム上で NFS を有効にする必要があります (NFS ボリュームと SMB/CIFS ボリュームの両方がサポートされています)。

- SnapDiff RPC サーバを SVM 上でアクティブ化する必要があります。システムでインデックス作成を有効にすると、コンソールはこれを自動的に実行します。(SnapDiff は、スナップショット間のファイルとディレクトリの違いをすばやく識別するテクノロジーです。)
- NetApp、検索と復元の回復力を高めるために、コンソール エージェントに別のボリュームをマウントすることを推奨しています。手順については、[ボリュームをマウントしてカタログのインデックスを再作成する](#)。

レガシー検索と復元的前提条件（インデックスカタログ v1 を使用）

従来のインデックスを使用する場合の検索と復元の要件は次のとおりです。

- AWS 要件:

- コンソールに権限を付与するユーザー ロールに、特定の Amazon Athena、AWS Glue、および AWS S3 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てください](#)"。

以前に設定したコンソール エージェントで NetApp Backup and Recovery をすでに使用していた場合は、コンソール ユーザー ロールに Athena および Glue 権限を追加する必要があることに注意してください。これらは検索と復元に必要です。

- Azure の要件:

- Azure Synapse Analytics リソース プロバイダー (「Microsoft.Synapse」と呼ばれます) をサブスクリプションに登録する必要があります。"[このリソースプロバイダーをサブスクリプションに登録する方法をご覧ください](#)"。リソース プロバイダーに登録するには、サブスクリプションの所有者 または 投稿者 である必要があります。
- コンソールに権限を付与するユーザー ロールに、特定の Azure Synapse ワークスペースおよび Data Lake Storage アカウント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てください](#)"。

以前に構成したコンソール エージェントで NetApp Backup and Recovery を既に使用していた場合は、Azure Synapse ワークスペースと Data Lake ストレージ アカウントのアクセス許可をコンソール ユーザー ロールに追加する必要があることに注意してください。これらは検索と復元に必要です。

- コンソール エージェントは、インターネットへの HTTP 通信用にプロキシ サーバーなしで構成する必要があります。コンソール エージェントに HTTP プロキシ サーバーを構成している場合は、検索と復元機能は使用できません。

- Google Cloud の要件:

- NetApp Console に権限を付与するユーザー ロールに、特定の Google BigQuery 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てください](#)"。

以前に構成したコンソール エージェントで NetApp Backup and Recovery をすでに使用していた場合は、コンソール ユーザー ロールに BigQuery 権限を追加する必要があります。これらは検索と復元に必要です。

- StorageGRID および ONTAP S3 の要件:

構成に応じて、検索と復元を実装する方法は 2 つあります。

- アカウントにクラウド プロバイダーの資格情報がない場合、インデックス カタログ情報はコンソール エージェントに保存されます。

インデックス カタログ v2 の詳細については、インデックス カタログを有効にする方法に関する以下のセクションを参照してください。

- プライベート (ダーク) サイトでコンソール エージェントを使用している場合、インデックス カタログ情報はコンソール エージェントに保存されます (コンソール エージェント バージョン 3.9.25 以上が必要です)。
- もしあなたが "[AWS 認証情報](#)" または "[Azure 資格情報](#)" アカウントにインデックス カタログがある場合は、クラウドに展開されたコンソール エージェントと同様に、インデックス カタログはクラ

クラウドプロバイダーに保存されます。(両方の認証情報がある場合、デフォルトで AWS が選択されます。)

オンプレミスのコンソール エージェントを使用している場合でも、コンソール エージェントの権限とクラウド プロバイダー リソースの両方について、クラウド プロバイダーの要件を満たす必要があります。この実装を使用する場合は、上記の AWS および Azure の要件を参照してください。

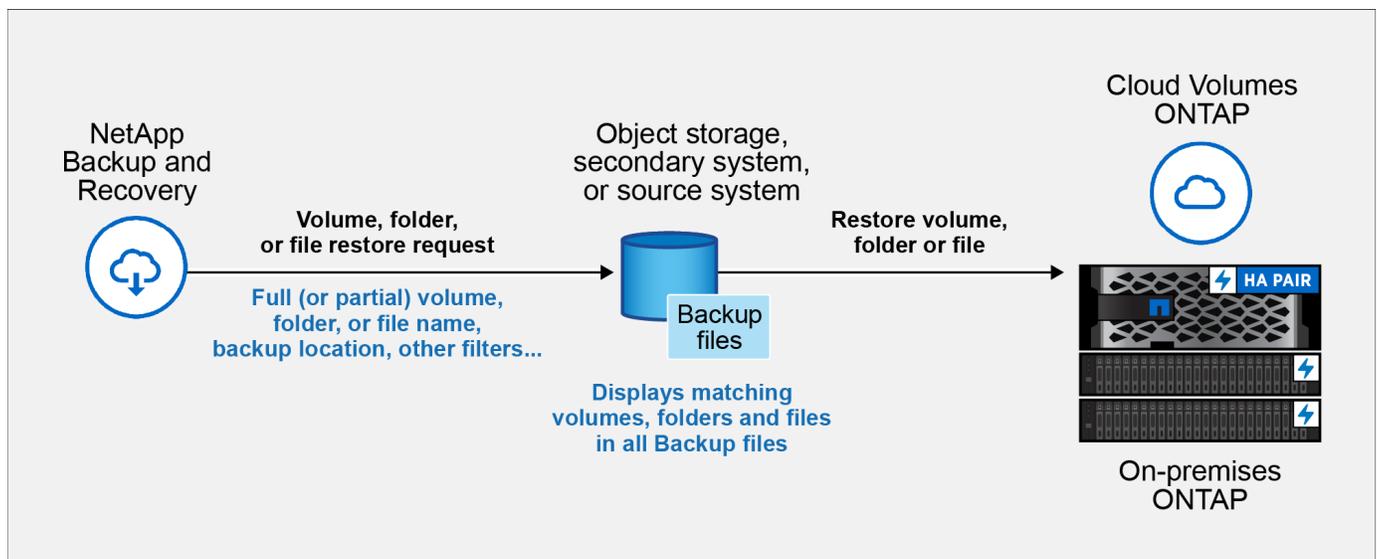
検索と復元のプロセス

プロセスは次のようになります。

1. 検索と復元を使用する前に、ボリューム データを復元する各ソース システムで「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 カタログは各ボリュームのバックアップ ファイルを追跡できるようになります。
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] を選択します。
3. ボリューム名の一部または全部、ファイル名の一部または全部、バックアップ場所、サイズの範囲、作成日の範囲、その他の検索フィルターでボリューム、フォルダー、またはファイルの検索条件を入力し、[検索] を選択します。

「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がある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を表示」を選択し、使用する実際のバックアップ ファイルで「復元」を選択します。
5. ボリューム、フォルダー、またはファイルを復元する場所を選択し、「復元」を選択します。
6. ボリューム、フォルダー、またはファイルが復元されます。



名前の一部を知るだけで、NetApp Backup and Recovery は検索に一致するすべてのバックアップ ファイルを検索します。

各システムでインデックスカタログを有効にする

検索と復元を使用する前に、ボリュームまたはファイルを復元する予定の各ソース システムで「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 カタログは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ようになり、検索が非常に迅速かつ効率的になります。

インデックス カタログは、システム内のすべてのボリュームとバックアップ ファイルに関するメタデータを保存するデータベースです。これは、復元するデータが含まれているバックアップ ファイルをすばやく見つけるために、検索と復元機能によって使用されます。

インデックスカタログ機能

NetApp Backup and Recovery、インデックス カタログを使用する場合、別のバケットはプロビジョニングされません。代わりに、AWS、Azure、Google Cloud Platform、StorageGRID、またはONTAP S3 に保存されているバックアップの場合、サービスはコンソール エージェントまたはクラウド プロバイダー環境にスペースをプロビジョニングします。

インデックス カタログは以下をサポートします。

- 3分以内にグローバル検索を効率化
- 最大50億ファイル
- クラスタあたり最大5000ボリューム
- ボリュームあたり最大10万個のスナップショット
- ベースライン インデックスの最大時間は 7 日未満です。実際の時間は環境によって異なります。

システムのインデックス作成を有効にする手順:

システム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み、データを復元してください。

まず、カタログ ファイルを保持するための別のボリュームをマウントする必要があります。これにより、スナップショットを保持するファイルのサイズが大きくなりすぎた場合にデータが失われるのを防ぎます。これはすべてのクラスタで必要なわけではなく、環境内の任意のクラスタから任意の 1 つのボリュームをマウントできます。これを行わないと、インデックスが正しく機能しない可能性があります。

マウントされたボリュームについては、次のサイズ設定ガイダンスを使用します。

- NetApp NFSボリュームを使用する
- 300 MB/秒のディスク スループットを備えたAFFストレージを推奨します。スループットが低下すると、検索やその他の操作に影響します。
- NetAppスナップショットを有効にして、カタログバックアップzipファイルに加えてカタログメタデータを保護します。
- 10億ファイルあたり50GB
- カタログデータ用に 20 GB、zip ファイル作成および一時ファイル用の追加スペース

カタログのインデックスを再作成するためにボリュームをマウントする手順

1. ボリュームをマウントする `/opt/application/netapp/cbs` 次のコマンドを入力します。

◦ `volume name` カatalogファイルが保存されるクラスタ上のボリュームです

° /opt/application/netapp/cbs マウントされているパスです

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

例：

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

インデックスを有効にする手順

1. 次のいずれかを実行します。
 - ° システムがインデックスされていない場合は、復元ダッシュボードの [検索と復元] で [システムのインデックスを有効にする] を選択します。
 - ° 少なくとも 1 つのシステムがすでにインデックスされている場合は、復元ダッシュボードの [検索と復元] で [インデックス設定] を選択します。
2. システムに対して*インデックスを有効にする*を選択します。

結果

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、システムは「アクティブ」として表示されます。

システム内のボリュームのサイズと、3 つのバックアップ場所すべてにあるバックアップ ファイルの数によっては、初期のインデックス作成プロセスに最大 1 時間かかる場合があります。その後は、最新の状態を維持するために、1 時間ごとに段階的な変更が透過的に更新されます。

検索と復元を使用してボリューム、フォルダ、ファイルを復元する

完了したら[システムのインデックスを有効にしました](#)、検索と復元を使用してボリューム、フォルダー、およびファイルを復元できます。これにより、幅広いフィルターを使用して、すべてのバックアップ ファイルから復元するファイルまたはボリュームを正確に見つけることができます。

手順

1. コンソール メニューから、保護 > バックアップとリカバリ を選択します。
2. *復元*タブを選択すると、復元ダッシュボードが表示されます。
3. [検索と復元] セクションから、[検索と復元] を選択します。
4. [検索と復元] セクションから、[検索と復元] を選択します。
5. 検索と復元ページから：
 - a. 検索バー に、ボリューム名、フォルダー名、またはファイル名の完全または一部を入力します。
 - b. リソースの種類を選択します: ボリューム、ファイル、フォルダー、または*すべて*。
 - c. [フィルター条件] 領域で、フィルター条件を選択します。たとえば、データが存在するシステムとファイルの種類 (.JPEG ファイルなど) を選択できます。または、オブジェクト ストレージ内の利用可能なスナップショットまたはバックアップ ファイル内のみで結果を検索する場合は、バックアップの場所のタイプを選択できます。

6. *検索*を選択すると、検索結果領域に、検索に一致するファイル、フォルダー、またはボリュームを持つすべてのリソースが表示されます。
7. 復元するデータがあるリソースを見つけて、[すべてのバックアップを表示]を選択し、一致するボリューム、フォルダー、またはファイルを含むすべてのバックアップ ファイルを表示します。
8. データの復元に使用するバックアップ ファイルを見つけて、[復元]を選択します。

結果には、検索したファイルを含むローカル ボリュームのスナップショットとリモートの複製ボリュームが識別されることに注意してください。クラウド バックアップ ファイル、スナップショット、または複製されたボリュームから復元することを選択できます。

9. ボリューム、フォルダー、またはファイルを復元する宛先の場所を選択し、[復元]を選択します。
 - ボリュームの場合、元の宛先システムを選択することも、代替システムを選択することもできます。FlexGroupボリュームを復元する場合は、複数のアグリゲートを選択する必要があります。
 - フォルダーの場合は、元の場所に復元することも、システム、ボリューム、フォルダーなどの別の場所を選択することもできます。
 - ファイルについては、元の場所へ復元することも、システム、ボリューム、フォルダーなどの別の場所を選択することもできます。元の場所を選択するときに、ソース ファイルを上書きするか、新しいファイルを作成するかを選択できます。

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構成していない場合は、追加情報の入力を求められます。

- Amazon S3 から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択し、作成したユーザーのアクセス キーとシークレット キーを入力してONTAPクラスターに S3 バケットへのアクセス権を付与し、オプションで安全なデータ転送のためにプライベート VPC エンドポイントを選択します。["これらの要件の詳細については、こちらをご覧ください。"](#)
- Azure Blob から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を選択し、オプションで VNet とサブネットを選択して、安全なデータ転送のためのプライベート エンドポイントを選択します。["これらの要件の詳細については、こちらをご覧ください。"](#)
- Google Cloud Storage から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace と、オブジェクト ストレージにアクセスするためのアクセス キーとシークレット キーを選択します。["これらの要件の詳細については、こちらをご覧ください。"](#)
- StorageGRIDから復元する場合は、StorageGRIDサーバーの FQDN と、ONTAP がStorageGRID との HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスター内の IPspace を入力します。["これらの要件の詳細については、こちらをご覧ください。"](#)
- ONTAP S3 からリストアする場合は、ONTAP S3 サーバーの FQDN と、ONTAP がONTAP S3 との HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスター内の IPspace を選択します。["これらの要件の詳細については、こちらをご覧ください。"](#)

結果

ボリューム、フォルダー、またはファイルが復元され、復元ダッシュボードに戻り、復元操作の進行状況を確認できます。また、*ジョブ監視*タブを選択して、復元の進行状況を確認することもできます。見る["ジョブ モニターページ"](#)。

参照と復元を使用してONTAPデータを復元する

NetApp Backup and Recoveryでは、Browse & Restore を使用してONTAPデータを復元します。復元する前に、ソース ボリューム名、ソース システムと SVM、およびバックアップ ファイルの日付をメモします。スナップショット、複製されたボリューム、またはオブジェクト ストレージに保存されたバックアップからONTAPデータを復元できます。

復元機能はONTAP のバージョンによって異なります。

- フォルダ: ONTAP 9.13.0 以降を使用すると、すべてのファイルとサブフォルダを含むフォルダを復元できます。それ以前のバージョンでは、フォルダ内のファイルのみを復元できます。
- アーカイブ ストレージ: アーカイブ ストレージ (ONTAP 9.10.1 以降で利用可能) からの復元は遅くなり、追加コストが発生する可能性があります。
- 宛先クラスタの要件:
 - ボリュームリストア: ONTAP 9.10.1 以上
 - ファイル復元: ONTAP 9.11.1 以上
 - Google Archive およびStorageGRID: ONTAP 9.12.1 以上
 - フォルダの復元: ONTAP 9.13.1 以上

["AWSアーカイブストレージからの復元の詳細"](#)。 ["Azure アーカイブ ストレージからの復元の詳細"](#)。 ["Google アーカイブ ストレージからの復元の詳細"](#)。



Azure アーカイブ ストレージからStorageGRIDシステムにデータを復元する場合、高優先度はサポートされません。

サポートされているシステムとオブジェクト ストレージ プロバイダーを参照および復元する

セカンダリ システム (複製されたボリューム) またはオブジェクト ストレージ (バックアップ ファイル) にあるバックアップ ファイルから、次のシステムにONTAPデータを復元できます。スナップショットはソース システム上に存在し、同じシステムにのみ復元できます。

注: ボリュームはどのタイプのバックアップ ファイルからでも復元できますが、現時点では、フォルダーまたは個々のファイルはオブジェクト ストレージ内のバックアップ ファイルからのみ復元できます。

オブジェクトストアから (バックアップ)	プライマリから (スナップショット)	セカンダリシステムから (レプリケーション)	宛先システムへ
Amazon S3	AWS オンプレミスONTAPシステム のCloud Volumes ONTAP	AWS オンプレミスONTAPシステム のCloud Volumes ONTAP	Azure ブロブ
Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Azure のCloud Volumes ONTAPオンプレミスONTAPシステム	Google Cloud Storage	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	NetAppStorageGRID	オンプレミスのONTAPシステム	オンプレミスのONTAPシステム Cloud Volumes ONTAP

オブジェクトストアから (バックアップ)	プライマリから (スナップショット)	セカンダリシステムから (レプリケーション)	宛先システムへ
オンプレミスのONTAPシステムへ	ONTAP S3	オンプレミスのONTAPシステム	オンプレミスのONTAPシステム Cloud Volumes ONTAP

参照と復元の場合、コンソール エージェントは次の場所にインストールできます。

- Amazon S3の場合、コンソールエージェントはAWSまたはオンプレミスに導入できます。
- Azure Blobの場合、コンソールエージェントはAzureまたはオンプレミスに展開できます。
- Google Cloud Storage の場合、コンソール エージェントを Google Cloud Platform VPC にデプロイする必要があります。
- StorageGRIDの場合、コンソールエージェントは、インターネットアクセスの有無にかかわらず、お客様の敷地内に導入する必要があります。
- ONTAP S3の場合、コンソールエージェントは、オンプレミス（インターネットアクセスの有無にかかわらず）またはクラウドプロバイダー環境に導入できます。

「オンプレミスのONTAPシステム」への参照には、FAS、AFF、およびONTAP Selectシステムが含まれることに注意してください。



システムのONTAPバージョンが 9.13.1 未満の場合、バックアップ ファイルが DataLock & Ransomware で構成されていると、フォルダーまたはファイルを復元できません。この場合、バックアップ ファイルからボリューム全体を復元し、必要なファイルにアクセスできます。

参照と復元を使用してボリュームを復元する

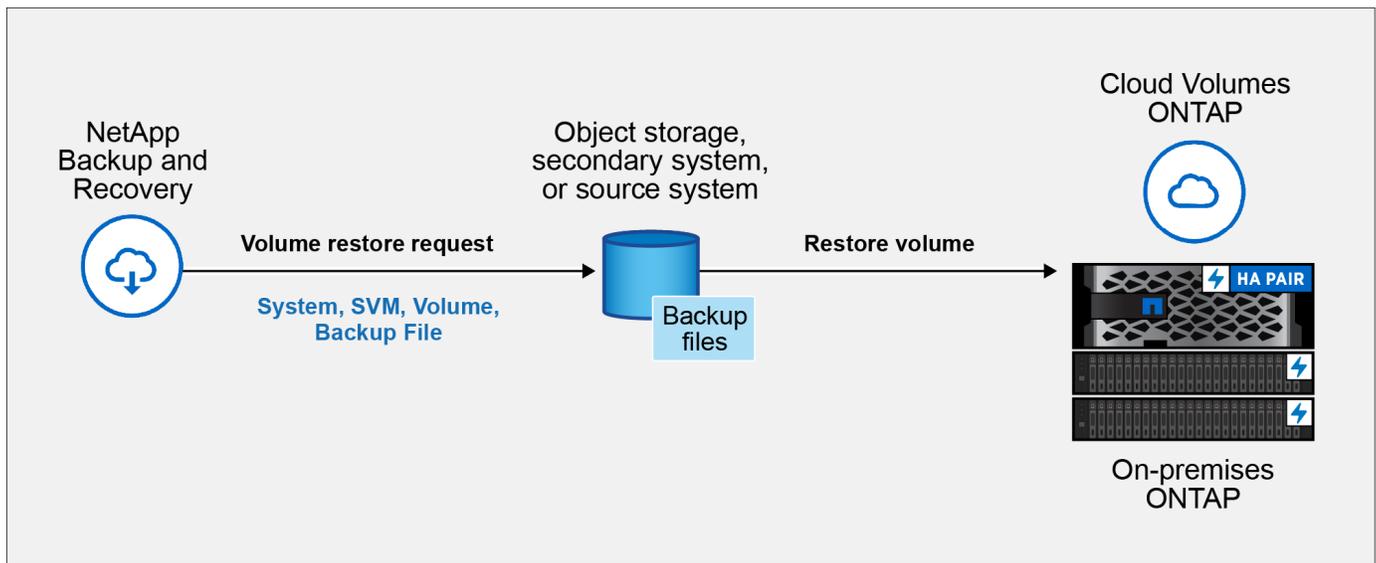
バックアップ ファイルからボリュームを復元すると、NetApp Backup and Recovery はバックアップのデータを使用して新しいボリュームを作成します。オブジェクト ストレージからのバックアップを使用すると、データを元のシステムのボリューム、ソース システムと同じクラウド アカウントにある別のシステム、またはオンプレミスのONTAPシステムに復元できます。

ONTAP 9.13.0 以降を使用しているCloud Volumes ONTAPシステム、またはONTAP 9.14.1 を実行しているオンプレミスのONTAPシステムにクラウド バックアップを復元する場合は、クイック リストア 操作を実行するオプションがあります。クイック リストアは、ボリュームへのアクセスをできるだけ早く提供する必要があります災害復旧の状況に最適です。クイック リストアでは、バックアップ ファイル全体を復元するのではなく、バックアップ ファイルからボリュームにメタデータを復元します。クイック リストアは、パフォーマンスや待ち時間が重要となるアプリケーションには推奨されません。また、アーカイブ ストレージ内のバックアップではサポートされません。



クイック リストアは、クラウド バックアップが作成されたソース システムでONTAP 9.12.1 以降が実行されている場合にのみ、FlexGroupボリュームに対してサポートされます。また、ソース システムでONTAP 9.11.0 以降が実行されている場合にのみ、SnapLockボリュームでサポートされます。

複製されたボリュームから復元する場合、ボリュームを元のシステム、Cloud Volumes ONTAPまたはオンプレミスのONTAPシステムに復元できます。



ボリュームを復元するには、ソース システム名、ストレージ VM、ボリューム名、およびバックアップ ファイルの日付が必要です。

手順

1. コンソール メニューから、保護 > バックアップとリカバリ を選択します。
2. *復元*タブを選択すると、復元ダッシュボードが表示されます。
3. [参照と復元] セクションから、[ボリュームの復元] を選択します。
4. [ソースの選択] ページで、復元するボリュームのバックアップ ファイルに移動します。復元する日付/タイムスタンプを持つ システム、ボリューム、および バックアップ ファイルを選択します。

場所 列には、バックアップ ファイル (スナップショット) が ローカル (ソース システム上のスナップショット)、セカンダリ (セカンダリ ONTAP システム上の複製されたボリューム)、または オブジェクト ストレージ (オブジェクト ストレージ内のバックアップ ファイル) のいずれであるかが表示されます。復元するファイルを選択します。

5. *次へ*を選択します。

オブジェクト ストレージ内のバックアップ ファイルを選択し、そのバックアップに対してランサムウェア耐性がアクティブになっている場合 (バックアップ ポリシーで DataLock とランサムウェア耐性を有効にした場合)、データを復元する前に、バックアップ ファイルに対して追加のランサムウェア スキャンを実行するように求められます。バックアップ ファイルをランサムウェアのスキャン対象とすることをお勧めします。(バックアップ ファイルの内容にアクセスするには、クラウド プロバイダーから追加の送信コストが発生します。)

6. [宛先の選択] ページで、ボリュームを復元する システム を選択します。
7. オブジェクト ストレージからバックアップ ファイルを復元するときに、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構成していない場合は、追加情報の入力を求められます。
 - Amazon S3 から復元する場合は、宛先ボリュームが存在する ONTAP クラスター内の IPspace を選択し、作成したユーザーのアクセス キーとシークレット キーを入力して ONTAP クラスターに S3 バケットへのアクセス権を付与し、オプションで安全なデータ転送のためにプライベート VPC エンドポイントを選択します。
 - Azure Blob から復元する場合は、宛先ボリュームが存在する ONTAP クラスター内の IPspace を選択

し、オブジェクトストレージにアクセスするための Azure サブスクリプションを選択し、オプションで VNet とサブネットを選択して、安全なデータ転送のためのプライベート エンドポイントを選択します。

- Google Cloud Storage から復元する場合は、Google Cloud プロジェクトとアクセス キーおよびシークレット キーを選択して、オブジェクトストレージ、バックアップが保存されるリージョン、および宛先ボリュームが存在する ONTAP クラスター内の IPspace にアクセスします。
- StorageGRID から復元する場合は、StorageGRID サーバーの FQDN と、ONTAP が StorageGRID との HTTPS 通信に使用するポートを入力し、オブジェクトストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在する ONTAP クラスター内の IPspace を選択します。
- ONTAP S3 からリストアする場合は、ONTAP S3 サーバーの FQDN と、ONTAP が ONTAP S3 との HTTPS 通信に使用するポートを入力し、オブジェクトストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在する ONTAP クラスター内の IPspace を選択します。

8. 復元されたボリュームに使用する名前を入力し、ボリュームが保存されるストレージ VM とアグリゲートを選択します。FlexGroup ボリュームを復元する場合は、複数のアグリゲートを選択する必要があります。デフォルトでは、ボリューム名として `<source_volume_name>_restore` が使用されます。

オブジェクトストレージから ONTAP 9.13.0 以上を使用する Cloud Volumes ONTAP システム、または ONTAP 9.14.1 を実行する オンプレミスの ONTAP システムにバックアップを復元する場合は、クイック復元操作を実行するオプションがあります。

また、アーカイブ ストレージ層 (ONTAP 9.10.1 以降で利用可能) にあるバックアップ ファイルからボリュームを復元する場合は、復元優先度を選択できます。

"AWS アーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"

。"Google アーカイブ ストレージからの復元の詳細"。Google アーカイブ ストレージ層のバックアップ ファイルはほぼ即座に復元されるため、復元の優先順位は必要ありません。

9. [次へ] を選択して、通常の復元プロセスを実行するか、クイック復元プロセスを実行するかを選択します。
- 通常の復元: 高いパフォーマンスが必要なボリュームでは通常の復元を使用します。復元プロセスが完了するまでボリュームは使用できません。
 - クイック復元: 復元されたボリュームとデータはすぐに利用できるようになります。クイック リストア プロセス中はデータへのアクセスが通常よりも遅くなる可能性があるため、高パフォーマンスが必要なボリュームではこれを使用しないでください。

10. *復元*を選択すると、復元ダッシュボードに戻り、復元操作の進行状況を確認できます。

結果

NetApp Backup and Recovery 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。

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復元する場合、アーカイブ層と復元の優先度に応じて数分から数時間かかる場合があることに注意してください。復元の進行状況を確認するには、[ジョブ監視] タブを選択します。

参照と復元を使用してフォルダとファイルを復元する

ONTAP ボリューム バックアップから少数のファイルのみを復元する必要がある場合は、ボリューム全体を復元するのではなく、フォルダーまたは個々のファイルを復元することを選択できます。フォルダーとファイル

を元のシステムの既存のボリュームに復元することも、同じクラウド アカウントを使用している別のシステムに復元することもできます。オンプレミスのONTAPシステム上のボリュームにフォルダーとファイルを復元することもできます。



現時点では、オブジェクト ストレージ内のバックアップ ファイルからのみフォルダーまたは個々のファイルを復元できます。現在、ローカル スナップショットまたはセカンダリ システム (複製されたボリューム) にあるバックアップ ファイルからのファイルとフォルダーの復元はサポートされていません。

複数のファイルを選択した場合、それらは同じ宛先ボリュームに復元されます。ファイルを別のボリュームに復元するには、プロセスを複数回実行します。

ONTAP 9.13.0 以降を使用している場合は、フォルダーとその中のすべてのファイルおよびサブフォルダーを復元できます。9.13.0 より前のバージョンのONTAPを使用する場合、そのフォルダのファイルのみが復元され、サブフォルダまたはサブフォルダ内のファイルは復元されません。

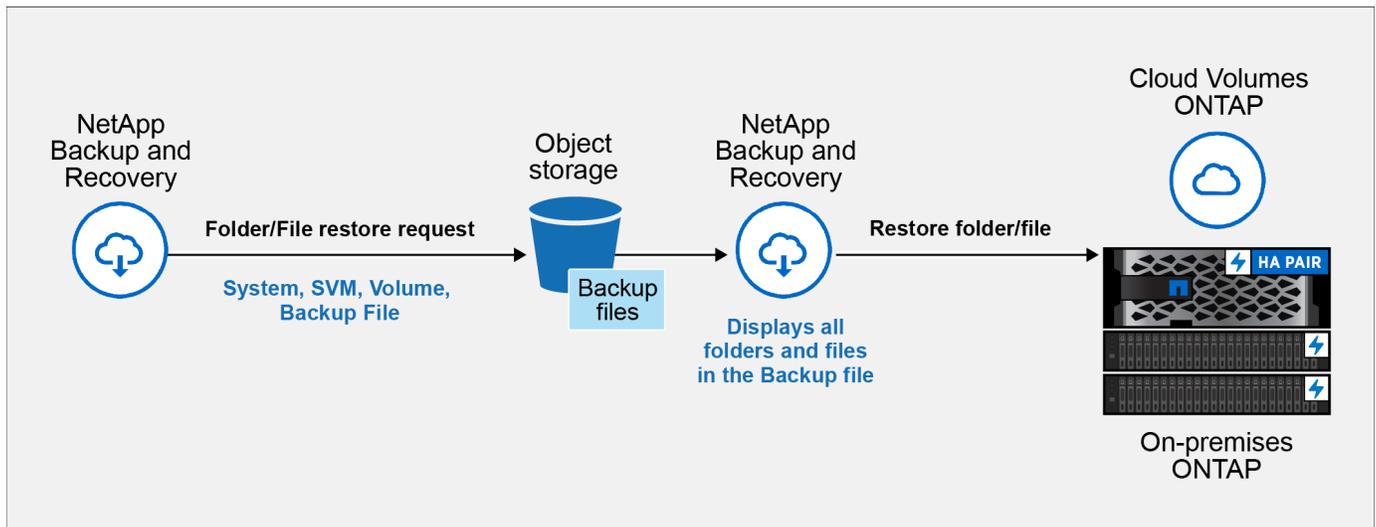


- バックアップ ファイルに DataLock および Ransomware 保護が設定されている場合、ONTAPバージョンが 9.13.1 以上の場合にのみフォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、バックアップ ファイルからボリューム全体を復元し、必要なフォルダーとファイルにアクセスできます。
- バックアップ ファイルがアーカイブ ストレージに存在する場合、ONTAPバージョンが 9.13.1 以上の場合にのみ、フォルダー レベルの復元がサポートされます。以前のバージョンのONTAPを使用している場合は、アーカイブされていない新しいバックアップ ファイルからフォルダを復元するか、アーカイブされたバックアップからボリューム全体を復元して、必要なフォルダとファイルにアクセスすることができます。
- ONTAP 9.15.1では、「参照して復元」オプションを使用してFlexGroupフォルダを復元できます。

特別なフラグを使用してテストすることができます。"[NetApp Backup and Recovery 2024 年 7 月リリース ブログ](#)"。

フォルダとファイルを復元する

ONTAPボリューム バックアップからボリュームにフォルダーまたはファイルを復元するには、次の手順に従います。フォルダーまたはファイルを復元するために使用するボリュームの名前とバックアップ ファイルの日付を知っておく必要があります。この機能はライブ ブラウジングを使用するため、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。



開始する前に

- `_ファイル_`復元操作を実行するには、ONTAPバージョンが 9.6 以上である必要があります。
- フォルダの復元操作を実行するには、ONTAPバージョンが 9.11.1 以上である必要があります。データがアーカイブ ストレージにある場合、またはバックアップ ファイルで DataLock およびランサムウェア保護が使用されている場合は、ONTAPバージョン 9.13.1 が必要です。
- 参照と復元オプションを使用してFlexGroupディレクトリを復元するには、ONTAPバージョンが 9.15.1 p2 以上である必要があります。

手順

1. コンソール メニューから、保護 > バックアップとリカバリ を選択します。
2. *復元*タブを選択すると、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、[ファイルまたはフォルダの復元] を選択します。
4. [ソースの選択] ページで、復元するフォルダまたはファイルが含まれているボリュームのバックアップファイルに移動します。ファイルを復元する日付/タイムスタンプを持つシステム、ボリューム、およびバックアップを選択します。
5. [次へ] を選択すると、ボリューム バックアップのフォルダとファイルのリストが表示されます。

アーカイブ ストレージ層にあるバックアップ ファイルからフォルダまたはファイルを復元する場合は、復元の優先順位を選択できます。

"AWSアーカイブストレージからの復元の詳細"。"Azure アーカイブ ストレージからの復元の詳細"。"Google アーカイブ ストレージからの復元の詳細"。Google アーカイブ ストレージ層のバックアップファイルはほぼ即座に復元されるため、復元の優先順位は必要ありません。

また、バックアップ ファイルに対して Ransomware Resilience がアクティブになっている場合 (バックアップ ポリシーで DataLock と Ransomware Resilience を有効にした場合)、データを復元する前に、バックアップ ファイルに対して追加のランサムウェア スキャンを実行するように求められます。バックアップ ファイルをランサムウェアのスキャン対象とすることをお勧めします。(バックアップ ファイルの内容にアクセスするには、クラウド プロバイダーから追加の送信コストが発生します。)

6. [アイテムの選択] ページで、復元するフォルダまたはファイルを選択し、[続行] を選択します。アイテムを見つける際に役立つ情報:
 - フォルダまたはファイル名が表示されている場合はそれを選択できます。

- 検索アイコンを選択し、フォルダーまたはファイルの名前を入力すると、アイテムに直接移動できます。
- 行の末尾にある下矢印を使用してフォルダー内の下のレベルに移動し、特定のファイルを見つけることができます。

ファイルを選択すると、ページの左側に追加されるので、すでに選択したファイルを確認できます。必要に応じて、ファイル名の横にある **x** を選択して、このリストからファイルを削除できます。

7. [宛先の選択] ページで、アイテムを復元する システム を選択します。

オンプレミス クラスターを選択し、オブジェクト ストレージへのクラスター接続をまだ構成していない場合は、追加情報の入力を求められます。

- Amazon S3 から復元する場合は、宛先ボリュームが存在するONTAPクラスターの IPspace と、オブジェクト ストレージにアクセスするために必要な AWS アクセス キーとシークレット キーを入力します。クラスターへの接続にプライベート リンク構成を選択することもできます。
- Azure Blob から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace を入力します。クラスターへの接続にプライベート エンドポイント構成を選択することもできます。
- Google Cloud Storage から復元する場合は、宛先ボリュームが存在するONTAPクラスター内の IPspace と、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キーを入力します。
- StorageGRIDから復元する場合は、StorageGRIDサーバーの FQDN と、ONTAP がStorageGRIDとの HTTPS 通信に使用するポートを入力し、オブジェクト ストレージにアクセスするために必要なアクセス キーとシークレット キー、および宛先ボリュームが存在するONTAPクラスター内の IPspace を入力します。

8. 次に、フォルダーまたはファイルを復元する ボリューム と フォルダー を選択します。

フォルダーやファイルを復元する際の場所についてはいくつかのオプションがあります。

- 上記のように*ターゲットフォルダーの選択*を選択した場合:
 - 任意のフォルダを選択できます。
 - フォルダーの上にマウスを移動し、行の末尾をクリックしてサブフォルダーにドリルダウンし、フォルダーを選択できます。
- ソース フォルダ/ファイルが配置されていたのと同じ宛先システムとボリュームを選択した場合は、[ソース フォルダ パスを維持] を選択して、フォルダまたはファイルをソース構造に存在していたのと同じフォルダに復元できます。同じフォルダーとサブフォルダーがすべてすでに存在している必要があります。フォルダーは作成されません。ファイルを元の場所に復元する場合、ソース ファイルを上書きするか、新しいファイルを作成するかを選択できます。

9. 復元 を選択して復元ダッシュボードに戻り、復元操作の進行状況を確認します。

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。