S3オブジェクト ストレージの管理

ONTAP 9

NetApp
February 13, 2026

目次

S3オブジェクト ストレージの管理

ONTAP 9でのS3のサポートの詳細

ONTAP S3の構成について学ぶ

ONTAP 9.8以降では、ONTAPクラスタでONTAP Simple Storage Service（S3）オブジェクト ストレージ サーバを有効にして、ONTAP System Managerのような使い慣れた管理ツールを使用してONTAPでの開発と運用のためのハイパフォーマンスなオブジェクト ストレージを迅速にプロビジョニングしたり、ONTAPのStorage Efficiencyとセキュリティを活用したりできます。

> 2024年7月より、これまでPDF形式で公開されていたテクニカルレポートの内容がONTAP製品ドキュメントに統合されました。ONTAP S3ドキュメントには、_TR-4814：S3 in ONTAPベストプラクティス_の内容が含まれるようになりました。

System Managerおよび**ONTAP CLI**を使用した**S3**の設定

ONTAP S3は、System ManagerおよびONTAP CLIを使用して設定および管理できます。シンプルな操作を実現するため、System ManagerでS3を有効にしてバケットを作成すると、ベストプラクティスに基づくデフォルトの設定が選択されます。設定パラメータを指定する必要がある場合は、ONTAP CLIを使用できます。S3サーバおよびバケットをCLIで設定した場合も、必要に応じてSystem Managerで管理することができ、その逆も同様です。

System Managerを使用してS3バケットを作成すると、ONTAPはシステムで利用可能な最高のデフォルトパフォーマンスサービスレベルを設定します。たとえば、AFFシステムでは、デフォルト設定は*Extreme*になります。パフォーマンスサービスレベルは、事前定義されたアダプティブQuality of Service（QoS）ポリシーグループです。デフォルトのサービスレベルの1つではなく、カスタムQoSポリシーグループまたはポリシーグループなしを指定できます。

事前に定義されたアダプティブQoSポリシー グループは次のとおりです。

- **Extreme**: 最も低いレイテンシと最高のパフォーマンスが期待されるアプリケーションに使用されます。
- **Performance**：パフォーマンスのニーズとレイテンシが中程度のアプリケーションに使用されます。
- **Value**：レイテンシよりもスループットと容量が重要なアプリケーションに使用されます。
- カスタム：カスタム QoS ポリシーを指定するか、QoS ポリシーを指定しません。

*階層化に使用*を選択した場合、パフォーマンスサービスレベルは選択されず、システムは階層化されたデータに最適なパフォーマンスを持つ低コストのメディアを選択しようとします。

参照："アダプティブQoSポリシー グループの使用"

ONTAPは、選択したサービス レベルを満たす、最も適切なディスクを含むローカル階層にバケットをプロビジョニングします。ただし、バケットに含めるディスクを指定する必要がある場合は、CLIでローカル階層（アグリゲート）を指定してS3オブジェクト ストレージを設定する方法もあります。CLIでS3サーバを設定した場合も、必要に応じてSystem Managerで管理できます。

バケットに使用するアグリゲートはCLIでしか指定できません。

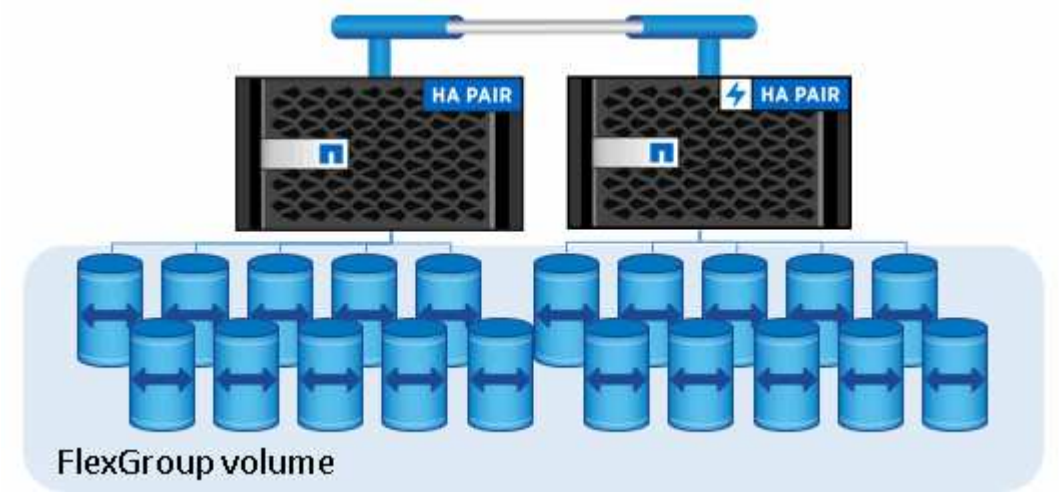
Cloud Volumes ONTAPでのS3バケットの設定

Cloud Volumes ONTAPからバケットを提供する場合は、基盤となるアグリゲートを手動で選択し、1つのノードのみを使用していることを確認することを強くお勧めします。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題が発生しやすくなるため、パフォーマンスに影響する可能性があります。したがって、Cloud Volumes ONTAP環境では、CLIからS3バケットを設定するする必要があります。

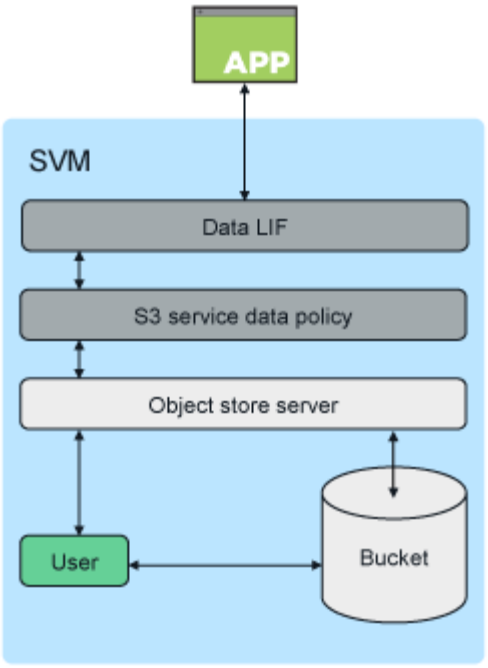
そうしないと、Cloud Volumes ONTAP上のS3サーバはオンプレミス環境と同じように設定され、管理されます。

FlexGroup ボリュームを使用した ONTAP S3 アーキテクチャ

ONTAPでは、バケットの基盤となるアーキテクチャは"FlexGroupボリューム"です。これは、複数の構成メンバーボリュームから構成される単一のネームスペースですが、単一のボリュームとして管理されます。



バケットへのアクセスは、権限があるユーザとクライアント アプリケーションにのみ許可されます。



FabricPoolエンドポイントとしての用途など、バケットがS3アプリケーション専用になっている場合、基盤となるFlexGroupボリュームではS3プロトコルのみがサポートされます。

ONTAP 9.12.1以降では、NASプロトコルを使用するように事前設定されている"マルチプロトコルNASボリューム"でもS3プロトコルを有効にできるようになりました。マルチプロトコルNASボリュームでS3プロトコルを有効にすると、クライアントアプリケーションはNFS、SMB、S3を使用してデータの読み取りと書き込みを行うことができます。

バケットの制限

最小容量

最小バケット容量は ONTAP プラットフォームによって決まります。

- オンプレミスプラットフォームの場合は95GB。
- Lab on Demandの場合は1.6GB。
- ONTAP Selectの場合は200MB。

最大サイズ

最大バケット容量は、最大FlexGroupサイズの60PBに制限されます。

バケットの最大数

バケットの最大数はFlexGroupボリュームあたり1,000個、またはクラスタあたり12,000個（FlexGroupボリューム12個使用）です。

ONTAP 9.14.1以降での**FlexGroup**の自動サイズ変更

ONTAP 9.14.1以降、デフォルトのFlexGroupサイズは、含まれるバケットのサイズに基づいています。FlexGroupボリュームは、バケットが追加または削除されると自動的に拡大または縮小されます。

例えば、最初のBucket_Aが100GBにプロビジョニングされている場合、FlexGroupはシンプロビジョニングによって100GBに設定されます。300GBのBucket_Bと500GBのBucket_Cという2つの追加バケットが作成されると、FlexGroupボリュームは900GBに拡張されます。

（Bucket_A：100GB + Bucket_B：300GB + Bucket_C：500GB = 900GB）

Bucket_Aを削除すると、基盤となるFlexGroupボリュームは800GBに縮小されます。

ONTAP 9.13.1以前の**FlexGroup**のデフォルト固定サイズ

バケットを拡張するための容量を確保するには、FlexGroupボリュームのすべてのバケットの使用済み容量の合計が、クラスタ上で使用可能なストレージ アグリゲートに基づくFlexGroupボリュームの最大容量の33%未満である必要があります。これが満たされない場合、作成された新しいバケットは、自動的に作成される新しいFlexGroupボリュームにプロビジョニングされます。

ONTAP 9.14.1より前のバージョンでは、FlexGroupのサイズは環境に応じた以下のデフォルト サイズに固定されていました。

- ONTAP：1.6PB
- ONTAP Select：100TB

FlexGroupボリュームをデフォルト サイズでプロビジョニングするのに十分な容量がクラスタにない場合、ONTAPは既存の環境でプロビジョニングできるようになるまで、デフォルト サイズを半分ずつ縮小していきます。

たとえば、300TBの環境では、FlexGroupボリュームは自動的に200TBでプロビジョニングされます（1.6PB、800TB、400TBのFlexGroupボリュームは環境に対して大きすぎるため）。

ONTAP S3の主な使用例

ONTAP S3 サービスへのクライアント アクセスの主な使用例は次のとおりです：

- FabricPoolを使用して非アクティブなデータをONTAP内のバケットに階層化することで、ONTAPからONTAPへの階層化が可能になります。"ローカル クラスタ"内のバケットへの階層化、または"リモート クラスタ"上のバケットへの階層化は、どちらもサポートされています。ONTAP S3への階層化により、非アクティブなデータにはより安価なONTAPシステムを使用でき、追加のFabricPoolライセンスや管理のための新しいテクノロジーを必要とせずに、新しいフラッシュ容量にかかるコストを節約できます。
- ONTAP 9.12.1以降では、NASプロトコルを使用するように事前設定されている"マルチプロトコルNASボリューム"でもS3プロトコルを有効にできるようになりました。マルチプロトコルNASボリュームでS3プロトコルを有効にすると、クライアント アプリケーションはS3、NFS、SMBを使用してデータの読み書きが可能になり、さまざまなユースケースが実現します。最も一般的なユースケースの1つは、NASクライアントがボリュームにデータを書き込み、S3クライアントが同じデータを読み取り、分析、ビジネス インテリジェンス、機械学習、光学式文字認識などの特殊なタスクを実行するというものです。

> ONTAP S3は、追加のハードウェアや管理作業なしに既存のONTAPクラスタでS3機能を有効にしたい場合に最適です。NetApp StorageGRIDは、NetAppのオブジェクト ストレージ向け主力ソリューションです。StorageGRIDは、S3のあらゆるアクション、高度なILM機能、またはONTAPベースのシステムでは実現できない容量を活用する必要があるネイティブS3アプリケーションに推奨されます。詳細については、"StorageGRID ドキュメント"をご覧ください。

関連情報

"FlexGroupボリューム管理"

Plan

S3 オブジェクト ストレージの ONTAP バージョンとプラットフォームのサポート

S3オブジェクト ストレージは、ONTAP 9.8以降を使用するすべてのAFF、FAS、ONTAP Selectプラットフォームでサポートされます。

FC、iSCSI、NFS、NVMe_oF、SMBなどの他のプロトコルと同様に、S3をONTAPで使用するには、ライセンスのインストールが必要です。S3ライセンスは無料ですが、ONTAP 9.8にアップグレードするシステムにはインストールする必要があります。S3ライセンスは、NetAppサポートサイトの"マスターライセンスキーページ"からダウンロードできます。

新しいONTAP 9.8以降のシステムには、S3のライセンスがプリインストールされています。

Cloud Volumes ONTAP

ONTAP S3の設定と機能はCloud Volumes ONTAPでもオンプレミス環境と同じですが、1つだけ違いがあります。

- Cloud Volumes ONTAPでバケットを作成する際には、CLIの手順を使用して、基盤となるFlexGroupボリュームで使用されるアグリゲートが単一のノードのものに限定されるようにしてください。各ノードは地理的に離れたアベイラビリティ ゾーンに配置され、レイテンシの問題の影響を受けやすいため、複数のノードのアグリゲートを使用するとパフォーマンスが低下するおそれがあります。

クラウド プロバイダ	**ONTAP**バージョン
Google Cloud	ONTAP 9.12.1以降
AWS	ONTAP 9.11.0以降
Azure	ONTAP 9.9.1以降

Amazon FSx for NetApp ONTAP

S3オブジェクト ストレージは、ONTAP 9.11以降を使用するAmazon FSx for NetAppサービスでサポートされます。

MetroClusterでのS3のサポート

ONTAP 9.14.1以降では、MetroCluster IP構成およびFC構成のミラーされたアグリゲートのSVMでS3オブジェクト ストレージ サーバを有効にできます。

ONTAP 9.12.1以降では、MetroCluster IP構成のミラーされていないアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にできます。MetroCluster IP構成におけるミラーされていないアグリゲートの制限事項の詳細については、"ミラーされていないアグリゲートに関する考慮事項"を参照してください。

SnapMirror S3 はMetroCluster構成ではサポートされていません。

ONTAP 9.7でのS3のパブリック プレビュー

ONTAP 9.7では、S3オブジェクトストレージがパブリックプレビューとして導入されました。このバージョンは本番環境向けではなく、ONTAP 9.8以降では更新されなくなります。本番環境でS3オブジェクトストレージをサポートしているのは、ONTAP 9.8以降のリリースのみです。

ONTAP 9.7のパブリック プレビューで作成したS3バケットはONTAP 9.8以降でも使用できますが、拡張機能は利用できません。ONTAP 9.7のパブリック プレビューで作成したバケットがある場合は、強化された機能サポート、セキュリティ、パフォーマンスを使用できるよう、バケットのコンテンツをONTAP 9.8のバケットに移行してください。

ONTAP S3でサポートされる処理

ONTAP S3アクションは、以下に示す場合を除き、標準のS3 REST APIでサポートされています。詳細については、"Amazon S3 APIリファレンス"をご覧ください。

> これらのS3アクションは、ONTAPでネイティブS3バケットを使用する場合に特にサポートされます。バージョン管理、オブジェクトロック、その他の機能に関連するアクションなど、一部のアクションは、"S3 NAS バケット（マルチプロトコル NAS ボリューム内の S3）"を使用する場合はサポートされません。

特定の操作について明記されていない限り、ONTAP 9.8以降では次の共通要求ヘッダーがサポートされます：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

バケットの処理

AWS S3 APIを使用するONTAPでサポートされる処理は次のとおりです。

バケットの処理	ONTAPでのサポート開始
CreateBucket ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1

バケットの処理	**ONTAP**でのサポート開始
DeleteBucket ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.11.1
DeleteBucketCors ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
DeleteBucketLifecycle ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
DeleteBucketPolicy ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.12.1
GetBucketAcl ONTAP S3は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
GetBucketCors ONTAP S3は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
GetBucketLifecycleConfiguration ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.13.1 *有効期限アクションのみがサポートされています
GetBucketLocation ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.10.1
GetBucketPolicy ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.12.1
GetBucketVersioning ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.11.1
HeadBucket ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListAllMyBuckets ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListBuckets ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
ListBucketVersions ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9.8 - ONTAP REST APIのみでサポート
PutBucketCors ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8

バケットの処理	**ONTAP**でのサポート開始
PutBucketLifecycleConfiguration ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.13.1 * 有効期限アクションのみがサポートされています
PutBucketPolicy ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.12.1
PutBucketVersioning ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.11.1

オブジェクトの処理

ONTAP 9.9.1以降では、ONTAP S3でオブジェクト メタデータとタグ付けがサポートされます。

- PutObjectとCreateMultipartUploadは、 `x-amz-meta-<key>.`を使用してキーと値のペアを含めます

  例えば： `x-amz-meta-project: ontap_s3`。

- GetObjectとHeadObjectは、ユーザー定義のメタデータを返します。
- メタデータと違って、タグは次の処理でオブジェクトとは別に読み取ることができます。
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

ONTAP 9.11.1以降では、ONTAP S3で、以下のONTAP APIを使用したオブジェクトのバージョン管理と関連処理がサポートされます。

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

特定の操作について明記されていない限り、次の URI クエリパラメータがサポートされます。

- `versionId`（ONTAP 9.12.1以降のオブジェクト操作に必要）

オブジェクトの処理	**ONTAP**でのサポート開始
AbortMultipartUpload ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダー、および次の追加の URI クエリパラメータをサポートしています： `uploadId`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
CompleteMultipartUpload ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダー、および次の追加の URI クエリパラメータをサポートしています： `uploadId`	ONTAP 9.8
CopyObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9.12.1

オブジェクトの処理	**ONTAP**でのサポート開始
CreateMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
DeleteObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `x-amz-bypass-governance-retention`	ONTAP 9.8
DeleteObjects ONTAP S3 は、このリクエストのすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています：* `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.9.1

オブジェクトの処理	**ONTAP**でのサポート開始
GetObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI クエリパラメータをサポートしています： • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` そして、この追加のリクエスト ヘッダー： • 範囲	ONTAP 9.8
GetObjectAcl ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8
GetObjectAttributes ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.14.1
GetObjectTagging ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.9.1
HeadObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
ListMultipartUpload ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8
ListObjects ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8
ListObjectsV2 ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
ListObjectVersions ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1
ListParts ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8
PutObject ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8

オブジェクトの処理	**ONTAP**でのサポート開始
PutObjectLockConfiguration ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.14.1
PutObjectRetention ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加ヘッダーをサポートしています： • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging ONTAP S3 は、この要求のすべての共通パラメータとヘッダーをサポートしています。	ONTAP 9.9.1
UploadPart	ONTAP 9.8
UploadPartCopy ONTAP S3 は、この要求のすべての共通パラメータとヘッダーに加えて、次の追加の URI パラメータをサポートしています： • `partNumber` • `uploadId` 追加のリクエストヘッダーは次のとおりです： • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

グループ ポリシー

以下の処理はS3に固有のものではなく、Identity and Access Management（IAM）プロセスに関連する一般的なものです。ONTAPではこれらのコマンドをサポートしますが、IAM REST APIは使用しません。

- Create Policy
- AttachGroup Policy

ユーザ管理

以下の処理はS3に固有のものではなく、IAMプロセスに関連する一般的なものです。

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

リリース別の**S3**の操作

ONTAP 9.14.1

ONTAP 9.14.1では、S3オブジェクト ロックのサポートが追加されました。

リーガル ホールド処理（保持期間の定義がないロック）はサポートされていません。

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockConfiguration
- PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1では、バケット ライフサイクル管理のサポートが追加されました。

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9.12.1

ONTAP 9.12.1では、バケット ポリシーとオブジェクト コピー機能のサポートが追加されました。

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11.1

ONTAP 9.11.1 では、バージョン管理、署名済み URL、チャンクアップロードのサポート、S3 API を使用したバケットの作成や削除などの一般的な S3 アクションのサポートが追加されました。

- ONTAP S3は、 `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`を使用したチャンクアップロード署名リクエストをサポートするようになりました。
- ONTAP S3 では、署名済み URL を使用してオブジェクトを共有したり、ユーザークレデンシャルを必要とせずに他のユーザーがオブジェクトをアップロードできるようにしたりするクライアントアプリケーションがサポートされるようになりました。
- CreateBucket
- DeleteBucket

- GetBucketVersioning
- ListBucketVersions
- PutBucket
- PutBucketVersioning
- DeleteObjects
- ListObjectVersions

> 基礎となるFlexGroupは最初のバケットが作成されるまで作成されないため、外部クライアントがCreateBucketを使用してバケットを作成する前に、まずONTAPでバケットを作成する必要があります。

ONTAP 9.10.1

ONTAP 9.10.1では、SnapMirror S3とGetBucketLocationのサポートが追加されました。

- GetBucketLocation

ONTAP 9.9.1

ONTAP 9.9.1では、ONTAP S3にオブジェクト メタデータのサポートと、タグ付けのサポートが追加されました。

- PutObjectとCreateMultipartUploadに、 `x-amz-meta-<key>`を使用したキーと値のペアが含まれるようになりました。例： `x-amz-meta-project: ontap_s3`
- GetObjectとHeadObjectで、ユーザ定義のメタデータが返されるようになりました。

タグはバケットでも使用できます。メタデータと違って、タグは次の処理でオブジェクトとは別に読み取ることができます。

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging

ONTAP S3の相互運用性

ONTAP S3サーバは、次の表に明記されている場合を除き、他のONTAP機能と問題なく連携します。

機能領域	サポート	サポート対象外
Cloud Volumes ONTAP	• ONTAP 9.9.1以降のリリースのAzureクライアント • ONTAP 9.11.0以降のリリースのAWSクライアント • ONTAP 9.12.1以降のリリースのGoogle Cloudクライアント	• ONTAP 9.8以前のリリースのクライアントのCloud Volumes ONTAP

機能領域	サポート	サポート対象外
データ保護	• Cloud Sync • オブジェクト ロック、ガバナンスとコンプライアンス（ONTAP 9.14.1以降） • "オブジェクトのバージョン管理"（ONTAP 9.11.1以降） • ミラーされていないMetroClusterアグリゲート（ONTAP 9.12.1以降） • ミラーされたMetroClusterアグリゲート（ONTAP 9.14.1以降） • "SnapMirror S3"（ONTAP 9.10.1以降） • SnapMirror（NASボリュームのみ、ONTAP 9.12.1以降） • SnapLock（NASボリュームのみ、ONTAP 9.14.1以降）	• イレイジャー コーディング • NDMP • SMTape • SnapMirror（同期および非同期） • SnapMirrorクラウド • SVMディザスタ リカバリ • SyncMirror（SyncMirrorミラーアグリゲートは、ONTAP 9.14.1以降のMetroCluster構成でサポートされます。SyncMirrorはMetroCluster構成外ではサポートされません。）
暗号化	• NetApp Aggregate Encryption（NAE） • NetApp Volume Encryption（NVE） • NetApp Storage Encryption（NSE） • TLS / SSL	• SLAG
MetroCluster環境	-	SnapMirror S3
ストレージ効率	• 重複排除 • 圧縮 • コンパクション	• アグリゲートレベルの効率性（同じアグリゲート上に存在するメンバーはボリューム間重複排除を利用できますが、異なるアグリゲート上に存在するメンバーは利用できません） • ONTAP S3バケットを含むFlexGroupボリュームのボリューム クローン • FlexCloneテクノロジー（ボリューム、ファイル、LUN）

機能領域	サポート	サポート対象外
サービス品質（QoS）	• QoSの最大値（上限） • QoSの最小値（下限）	-
その他の機能	• "S3イベントの監査"（ONTAP 9.10.1以降） • "バケットのライフサイクル管理"（ONTAP 9.13.1以降） • FabricPoolクラウド階層（ネイティブS3のみ） • FabricPoolローカル階層（NASボリュームのみ） • FlexCache ボリューム（ONTAP 9.18.1 以降）	• FPolicy • qtree • クォータ • FabricPoolクラウド階層（NASボリュームのみ） • FabricPoolローカル階層（ネイティブS3のみ）

ONTAPでS3を使用する検証済みのサードパーティソリューション

S3は世界標準であり、これはサポートされているアプリケーションの包括的なリストではなく、各パートナーとの連携により検証されたソリューションのリストです。ご希望のソリューションがリストにない場合は、NetAppアカウント担当者にお問い合わせください。

ネイティブ **S3** バケットを使用して検証されたサードパーティソリューション

- Amazon SageMaker
- Apache Hadoop S3Aクライアント
- Apache Kafka
- Apache Spark
- Commvault（V11）
- Confluent Kafka
- NetBackup
- Red Hat Quay
- Rubrik
- Snowflake
- Trino
- Veeam（V12）

これらのソリューションは、ONTAPでネイティブS3バケットを使用する場合に特に検証されます。バージョン管理、オブジェクトロック、その他の機能に関連するソリューションなど、一部のソリューションは、"S3 NAS バケット（マルチプロトコル NAS ボリューム内の S3）"を使用する場合はサポートされません。

設定

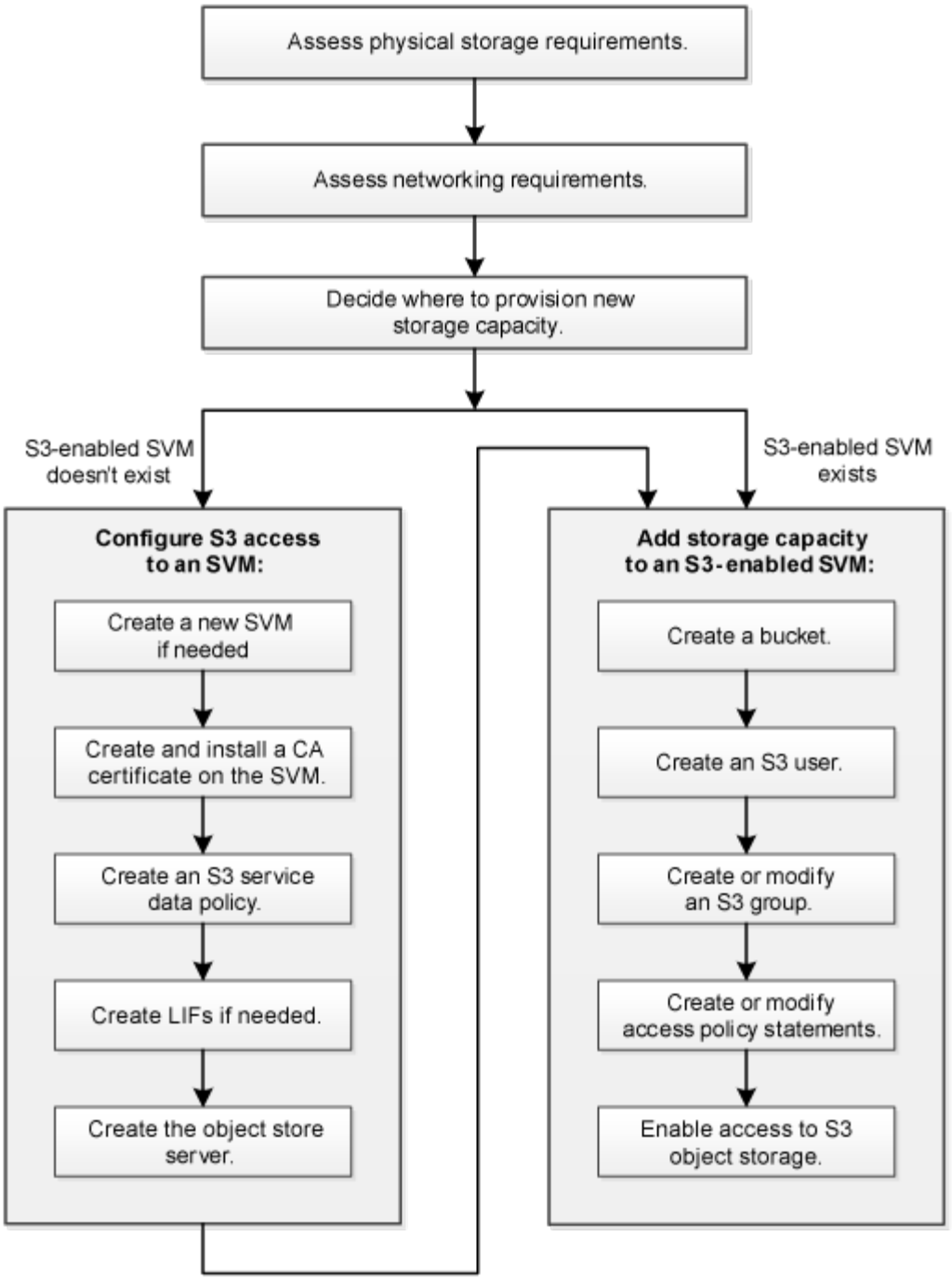
S3の設定プロセスについて

ONTAP S3 構成ワークフロー

S3を設定するには、物理ストレージとネットワークの要件を評価して、目的に応じたワークフローを選択します。新規または既存のSVMへのS3アクセスを設定するか、すでにS3アクセスの設定が完了している既存のSVMにバケットとユーザを追加するかによってワークフローが異なります。

クラスタとクライアント間の時刻同期を確保するには、ネットワーク タイム プロトコル（NTP）の設定が必要です。クライアント アクセスには、ONTAP S3オブジェクト ストアとクライアント間で少なくとも15分の差がある有効なタイムスタンプが必要になることがよくあります。"NTPの設定方法について学ぶ"。

System Managerを使用して新しいStorage VMへのS3アクセスを設定する場合、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクト ストレージ サーバが1回の操作で作成されます。



ONTAP S3物理ストレージ要件を評価する

クライアントのS3ストレージをプロビジョニングする前に、既存のアグリゲート内に新しいオブジェクト ストアのための十分なスペースがあることを確認する必要があります。十分なスペースがない場合は、既存のアグリゲートにディスクを追加するか、必要なタイプの新しいアグリゲートを必要な場所に作成することができます。

タスク概要

S3対応のSVMでS3バケットを作成すると、バケットをサポートするためにFlexGroupボリュームが"自動的に作成されます"作成されます。ONTAPに基盤となるアグリゲートとFlexGroupコンポーネントを自動的に選択させる（デフォルト）ことも、自分で基盤となるアグリゲートとFlexGroupコンポーネントを選択することも

できます。

基盤となるディスクのパフォーマンスについて特定の要件がある場合など、アグリゲートとFlexGroupコンポーネントを自分で指定する場合は、アグリゲートの構成がFlexGroupボリュームのプロビジョニングに関するベストプラクティス ガイドラインに準拠していることを確認してください。詳細については、以下を参照してください。

- "FlexGroupボリューム管理"
- "NetAppテクニカルレポート4571-a：NetApp ONTAP FlexGroupボリュームのベストプラクティス"

Cloud Volumes ONTAPからバケットを提供する場合は、基盤となるアグリゲートを手動で選択し、1つのノードのみを使用していることを確認することを強くお勧めします。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題が発生しやすくなるため、パフォーマンスに影響する可能性があります。"Cloud Volumes ONTAPのバケットの作成"の詳細を確認してください。

ONTAP S3サーバを使用して、ローカルFabricPool容量階層（つまり、パフォーマンス階層と同じクラスタ内）を作成できます。これは、たとえば、SSDディスクが一方のHAペアに接続されていて、_コールド_データを別のHAペアのHDDディスクに階層化する場合などに便利です。このユースケースでは、S3サーバとローカル容量階層を含むバケットは、パフォーマンス階層とは異なるHAペアに配置する必要があります。ローカル階層化は、1ノードおよび2ノードのクラスタではサポートされていません。

手順

1. 既存のアグリゲート内の使用可能なスペースを表示します。

   ```
   storage aggregate show
   ```

   十分なスペースを備えたアグリゲート、または必要なノードの場所にあるアグリゲートがあれば、S3設定用にその名前を記録します。

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 十分なスペースまたは必要なノードの場所を持つアグリゲートがない場合は、 `storage aggregate add-disks`コマンドを使用して既存のアグリゲートにディスクを追加するか、 `storage aggregate create`コマ

ンドを使用して新しいアグリゲートを作成します。

関連情報

- "storage aggregate add-disks"
- "storage aggregate create"

ONTAP S3ネットワーク要件を評価する

クライアントにS3ストレージを提供する前に、ネットワークが正しく設定されてS3のプロビジョニング要件を満たしていることを確認する必要があります。

開始する前に

次のクラスタ ネットワーク オブジェクトを設定する必要があります。

- 物理ポートと論理ポート
- ブロードキャスト ドメイン
- サブネット（必要な場合）
- IPspace（必要に応じて、デフォルトのIPspaceに追加）
- フェイルオーバー グループ（必要に応じて、各ブロードキャスト ドメインのデフォルトのフェイルオーバー グループに追加）
- 外部ファイアウォール

タスク概要

リモートのFabricPool大容量（クラウド）階層およびS3クライアントの場合は、データSVMを使用し、データLIFを設定する必要があります。FabricPoolクラウド階層の場合は、クラスタ間LIFも設定する必要があります。ただしクラスタのピアリングは必要ありません。

ローカルFabricPool容量階層の場合、システムSVM（「`Cluster`」と呼ばれます）を使用する必要がありますが、LIF設定には2つのオプションがあります：

- クラスタLIFを使用する。

  この場合、LIFについて追加の設定は必要ありませんが、クラスタLIFのトラフィックが増加します。また、他のクラスタからローカル階層にアクセスすることはできません。

- データLIFとクラスタ間LIFを使用する。

  この場合、LIFをS3プロトコルに対して有効にするなどの追加の設定が必要ですが、リモートのFabricPoolクラウド階層として他のクラスタからもローカル階層にアクセスできるようになります。

手順

1. 利用可能な物理ポートおよび仮想ポートを表示します。

   ```
   network port show
   ```

   - 可能な場合は、データ ネットワークの速度が最高であるポートを使用する必要があります。
   - 最大限のパフォーマンスを得るためには、データ ネットワーク内のすべてのコンポーネントのMTU設

定が同じである必要があります。

2. サブネット名を使用してLIFのIPアドレスとネットワーク マスク値を割り当てる場合は、そのサブネットが存在し、十分な数のアドレスが使用可能であることを確認します。

   ```
   network subnet show
   ```

   サブネットには、同じレイヤー3サブネットに属するIPアドレスのプールが含まれます。サブネットは`network subnet create`コマンドを使用して作成されます。

   > `network subnet show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-show.html["ONTAPコマンド リファレンス"^]を参照してください。

3. 使用可能なIPspaceを表示します。

   ```
   network ipspace show
   ```

   デフォルトのIPspaceまたはカスタムのIPspaceを使用できます。

4. IPv6アドレスを使用する場合は、IPv6がクラスタで有効になっていることを確認します。

   ```
   network options ipv6 show
   ```

   必要に応じて、 `network options ipv6 modify` コマンドを使用して IPv6 を有効にすることができます。

関連情報

- "network port show"
- "ネットワークオプションIPv6"
- "network ipspace show"
- "ネットワークサブネットの作成"

新しい**ONTAP S3**ストレージ容量をプロビジョニングする場所を決定する

新しいS3バケットを作成する前に、そのバケットを新規と既存どちらのSVMに配置するかを決める必要があります。それによって以降のワークフローが決まります。

オプション

- 新しいSVMまたはS3が有効でないSVMにバケットをプロビジョニングする場合は、次のトピックの手順を実行します。

  "S3用SVMの作成"

  "S3のバケットの作成"

  S3はNFSやSMBと同じSVMに配置することもできますが、次のいずれかに該当する場合は新しいSVMを作成します。

- クラスタ上でS3を初めて有効にする場合。
- S3 サポートを有効にしたくないクラスター内に既存の SVM があります。
- クラスター内にS3対応SVMが1つ以上あり、パフォーマンス特性が異なる別のS3サーバーが必要です。SVMでS3を有効にしたら、バケットのプロビジョニングに進みます。

- 既存のS3対応SVMに1つ目のバケットまたは追加のバケットをプロビジョニングする場合は、次のトピックの手順を実行します。

  "S3のバケットの作成"

SVMへのS3アクセスの設定

ONTAP S3用のSVMを作成する

S3は他のプロトコルと同じSVMに配置することもできますが、ネームスペースやワークロードを分離する場合は新しいSVMを作成します。

タスク概要

SVMをS3のオブジェクト ストレージにのみ使用する場合、S3サーバにDNS設定は必要ありません。ただし、他のプロトコルを使用する場合はSVMにDNSを設定できます。

System Managerを使用して新しいStorage VMへのS3アクセスを設定する場合、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクト ストレージ サーバが1回の操作で作成されます。

例 **1.** 手順

System Manager

S3サーバ名の完全修飾ドメイン名（FQDN）を確認しておきます。クライアントはFQDNでS3にアクセスします。S3サーバのFQDNをバケット名で始めることはできません。

Dataインターフェイス ロールに使用するIPアドレスを確認しておきます。

外部のCA署名証明書を使用している場合は、入力するように求められます。システムで生成された証明書を使用することもできます。

1. Storage VMでS3を有効にします。

   a. 新しいストレージ VM を追加します：ストレージ **>** ストレージ **VM** をクリックし、追加 をクリックします。

      既存のストレージVMがない新しいシステムの場合は、*ダッシュボード>プロトコルの構成*をクリックします。

   既存のストレージ VM に S3 サーバーを追加する場合：ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM を選択して 設定 をクリックし、 **S3** の下の をクリックします。

   a. *S3 を有効にする*をクリックし、S3 サーバー名を入力します。

   b. 証明書タイプを選択します。

      システムで生成された証明書と独自の証明書のどちらを選択した場合も、その証明書がクライアント アクセスで必要になります。

   c. ネットワーク インターフェイスを入力します。

2. システム生成の証明書を選択した場合は、新しいストレージVMの作成が確認されると証明書情報が表示されます。*Download*をクリックし、クライアントがアクセスできるように保存してください。

   - 今後シークレット キーは表示されません。
   - 証明書情報が再度必要になった場合：ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM を選択して、設定 をクリックします。

CLI

1. クラスタでS3のライセンスが有効であることを確認します。

   ```
   system license show -package s3
   ```

   有効でない場合は、営業担当者にお問い合わせください。

2. SVMを作成します。

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- `-rootvolume-security-style`オプションにはUNIX設定を使用します。
- デフォルトの C.UTF-8 `-language` オプションを使用します。
- `ipspace`設定はオプションです。

3. 新しく作成したSVMの設定およびステータスを確認します。

```
vserver show -vserver <svm_name>
```

`Vserver Operational State`フィールドには`running`状態が表示される必要があります。`initializing`状態が表示される場合、ルートボリュームの作成などの中間操作が失敗したことを意味し、`SVM`を削除して再作成する必要があります。

例

次のコマンドは、データ アクセス用のSVMをIPspace ipspaceA内に作成します。

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

次のコマンドは、1GBのルートボリュームを持つSVMが作成され、自動的に起動されて `running`状態になっていることを示しています。ルートボリュームにはルールが含まれていないデフォルトのエクスポートポリシーが適用されているため、作成時にルートボリュームはエクスポートされません。デフォルトでは、vsadminユーザーアカウントが作成され、 `locked`状態になっています。vsadminロールは、デフォルトのvsadminユーザーアカウントに割り当てられています。

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

ONTAP S3 対応 **SVM** に **CA** 証明書を作成してインストールする

S3クライアントは、S3対応SVMにHTTPSトラフィックを送信するために、証明機関（CA）証明書を必要とします。CA証明書は、クライアントアプリケーションとONTAPオブジェクトストアサーバの間に信頼関係を構築します。リモートクライアントからアクセス可能なオブジェクトストアとしてONTAPを使用する前に、ONTAPにCA証明書をインストールする必要があります。

タスク概要

HTTPのみを使用するようにS3サーバを設定したり、CA証明書なしでアクセスできるようにクライアントを設定したりすることも可能ですが、ONTAP S3サーバへのHTTPSトラフィックをCA証明書で保護することを推奨します。

IPトラフィックがクラスタLIFのみを経由するローカルでの階層化では、CA証明書は必要ありません。

この手順では、ONTAPの自己署名証明書を作成してインストールします。自己署名証明書はONTAPに生成させることも可能ですが、サードパーティの認証局が発行する署名済み証明書を使用することが推奨されます。詳細については、管理者の認証に関するドキュメントを参照してください。

"管理者認証とRBAC"

`security certificate`
および追加の構成オプションの詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+certificate["ONTAPコマンド リファレンス"^]を参照してください。

手順

1. 自己署名デジタル証明書を作成します。

   ```
   security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name
   ```

   `-type root-ca`オプションは、認証局（CA）として機能して他の証明書に署名するための自己署名デジタル証明書を作成してインストールします。

   この `-common-name`オプションは、SVMの認証局（CA）名を作成し、証明書の完全な名前を生成するときに使用されます。

   証明書のデフォルト サイズは2048ビットです。

   例

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type root-ca -common-name svm1_ca

   The certificate's generated name for reference: svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   生成された証明書の名前が表示されたら、以降の手順で使用するため記録しておきます。

   `security certificate create`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

2. 証明書署名要求を生成します。

   ```
   security certificate generate-csr -common-name s3_server_name [additional_options]
   ```

   署名リクエストの `-common-name`パラメータは、S3サーバー名（FQDN）である必要があります。

   必要に応じてSVMの場所やその他の詳細情報を指定できます。

`-dns-name`パラメータは、DNS
名のリストを提供するサブジェクト代替名拡張を指定するために、クライアントによって必要とされることがよくあります。

`-ipaddr`パラメータは、IP
アドレスのリストを提供するサブジェクト代替名拡張を指定するために、クライアントによって必要とされることがよくあります。

あとで参照できるように、証明書要求と秘密鍵のコピーを保管しておくように求められます。

`security certificate generate-csr`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-generate-csr.html["ONTAPコマンド リファレンス"^]をご覧ください。

3. SVM_CAを使用してCSRに署名し、S3サーバの証明書を生成します。

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   前の手順で使用したコマンド オプションを入力します。

   - `-ca` — 手順 1 で入力した CA の共通名。
   - `-ca-serial` — 手順 1 の CA シリアル番号。たとえば、CA 証明書名が svm1_ca_159D1587CE21E9D4_svm1_ca の場合、シリアル番号は 159D1587CE21E9D4 です。

     デフォルトでは、署名済み証明書の有効期間は365日です。別の値を選択したり、他の署名の詳細を指定したりできます。

     プロンプトが表示されたら、手順2で保存した証明書要求の文字列をコピーして入力します。

   署名済み証明書が表示されます。あとで使用できるように保存しておきます。

4. S3対応SVMに署名済み証明書をインストールします。

   `security certificate install -type server -vserver` *`svm_name`*

   プロンプトが表示されたら、証明書と秘密鍵を入力します。

   証明書チェーンが必要な場合は、中間証明書を入力できます。

   秘密鍵とCA署名デジタル証明書が表示されたら、あとで参照できるように保存します。

5. 公開鍵証明書を取得します。

   `security certificate show -vserver` *`svm_name`* `-common-name` *`ca_cert_name`* `-type root-ca -instance`

クライアント側の設定で使用するため、公開鍵証明書を保存しておきます。

例

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
           Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

関連情報

- "security certificate install"
- "セキュリティ証明書の表示"
- "security certificate sign"

ONTAP S3サービスデータポリシーを作成する

S3のデータ サービスおよび管理サービス用にサービス ポリシーを作成できます。LIFでS3データ トラフィックを有効にするには、S3サービス データ ポリシーが必要です。

タスク概要

データLIFおよびクラスタ間LIFを使用している場合は、S3サービス データ ポリシーが必要です。ローカルでの階層化にクラスタLIFを使用している場合は必要ありません。

LIFにサービス ポリシーを指定すると、そのポリシーを使用してLIFのデフォルト ロール、フェイルオーバー ポリシー、データ プロトコルのリストが作成されます。

SVMとLIFには複数のプロトコルを設定できますが、オブジェクト データの提供にはS3プロトコルのみを使用することを推奨します。

手順

1. 権限の設定をadvancedに変更します。

   ```
   set -privilege advanced
   ```

2. サービス データ ポリシーを作成します。

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   `data-core`および `data-s3-server`サービスは、ONTAP S3を有効にするために必要な唯一のサービスですが、必要に応じて他のサービスも含めることができます。

   `network interface service-policy create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-service-policy-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP S3のデータ**LIF**を作成する

新しいSVMを作成した場合、S3アクセス専用のLIFとしてデータLIFを作成する必要があります。

開始する前に

- 基盤となる物理または論理ネットワーク ポートが管理 `up`ステータスに設定されている必要があります。"ONTAPコマンド リファレンス"の `up`の詳細を確認してください。
- サブネット名を使用してLIFのIPアドレスとネットワーク マスク値を割り当てる場合は、そのサブネットが存在している必要があります。

  サブネットには、同じレイヤー3サブネットに属するIPアドレスのプールが含まれます。 `network subnet create`コマンドを使用して作成されます。

  `network subnet create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-subnet-create.html["ONTAPコマンド リファレンス"^]を参照してください。

- LIFサービス ポリシーがすでに存在している必要があります。

- ベスト プラクティスとして、データ アクセスに使用されるLIF（data-s3-server）と管理処理に使用されるLIF（management-https）を分けることを推奨します。両方のサービスを同じLIFで有効にしないようにしてください。
- DNSレコードには、data-s3-serverが関連付けられているLIFのIPアドレスだけを含めるようにしてください。他のLIFのIPアドレスがDNSレコードで指定されていると、ONTAP S3要求が他のサーバによって処理され、想定外の応答やデータ損失が発生するおそれがあります。

タスク概要

- 同じネットワーク ポート上にIPv4とIPv6の両方のLIFを作成できます。
- クラスタ内に多数のLIFがある場合は、 `network interface capacity show`コマンドを使用してクラスタでサポートされているLIF容量を確認し、 `network interface capacity details show`コマンド（高度な権限レベル）を使用して各ノードでサポートされているLIF容量を確認できます。

  `network interface capacity show`および `network interface capacity details show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=network+interface+capacity+show["ONTAPコマンド リファレンス"^]をご覧ください。

- リモートのFabricPool容量（クラウド）階層化を有効にする場合、クラスタ間LIFも設定する必要があります。

手順

1. LIFを作成します。

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   service_policy_names -home-node node_name -home-port port_name {-address
   IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
   data -auto-revert {true|false}
   ```

   - `-home-node`は、 `network interface revert`コマンドがLIF上で実行されたときにLIFが戻るノードです。

     `network interface revert`
     の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-revert.html["ONTAPコマンド リファレンス"^]を参照してください。

     `-auto-revert`オプションを使用して、
     LIFがホームノードとホームポートに自動的にリバートするかどうかも指定できます。

   - `-home-port`は、LIF上で `network interface revert`コマンドが実行されたときにLIFが戻る物理ポートまたは論理ポートです。
   - `-address`および `-netmask`オプションを使用してIPアドレスを指定することも、 `-subnet_name`オプションを使用してサブネットからの割り当てを有効にすることもできます。
   - サブネットを使用してIPアドレスとネットワーク マスクを指定した場合、サブネットにゲートウェイ

が定義されていると、そのサブネットを使用してLIFを作成するときにゲートウェイへのデフォルトルートがSVMに自動的に追加されます。

- IPアドレスを手動で割り当てる場合（サブネットを使用せず）、クライアントまたはドメインコントローラが異なるIPサブネット上にある場合は、ゲートウェイへのデフォルトルートを設定する必要がある場合があります。 `network route create`およびSVM内での静的ルートの作成方法の詳細については、"ONTAPコマンド リファレンス"を参照してください。
- `-firewall-policy`オプションには、LIFロールと同じデフォルトの `data`を使用します。

  必要に応じて、カスタム ファイアウォール ポリシーをあとから作成して追加できます。

  ONTAP 9.10.1以降、ファイアウォールポリシーは廃止され、LIFサービスポリシーに完全に置き換えられました。詳細については、"LIFのファイアウォール ポリシーの設定"を参照してください。

- `-auto-revert`では、起動時、管理データベースのステータス変更時、ネットワーク接続時などの状況において、データLIFをホームノードに自動的にリバートするかどうかを指定できます。デフォルト設定は `false`ですが、環境のネットワーク管理ポリシーに応じて `false`に設定できます。
- `-service-policy`オプションでは、作成したデータおよび管理サービスポリシーと、必要なその他のポリシーを指定します。

2. `-address`オプションでIPv6アドレスを割り当てる場合：
   a. `network ndp prefix show`コマンドを使用して、さまざまなインターフェースで学習された RA プレフィックスのリストを表示します。

      `network ndp prefix show`コマンドは、上級権限レベルで使用できます。

   b. `prefix:id`の形式を使用して、IPv6アドレスを手動で構築します。

      `prefix`は、さまざまなインターフェースで学習されたプレフィックスです。

      `id`を導出するには、ランダムな64ビットの16進数を選択します。

3. `network interface show`コマンドを使用して、LIFが正常に作成されたことを確認します。
4. 設定したIPアドレスに到達できることを確認します。

対象	方法
IPv4 アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、 `my-S3-policy`サービスポリシーが割り当てられたS3データLIFを作成する方法を示しています：

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

次のコマンドは、cluster-1内のすべてのLIFを表示します。データLIFのdatalif1とdatalif3にはIPv4アドレスが、datalif4にはIPv6アドレスが設定されています。

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

関連情報

- "network ping"
- "ネットワーク インターフェイス"

- "network ndp prefix show"

ONTAP S3を使用したリモート**FabricPool**階層化用のクラスタ間**LIF**を作成する

ONTAP S3を使用してリモートのFabricPool容量（クラウド）階層化を有効にする場合、クラスタ間LIFを設定する必要があります。データ ネットワークと共有するポートにクラスタ間LIFを設定できます。これにより、クラスタ間ネットワークに必要なポート数を減らすことができます。

開始する前に

- 基盤となる物理または論理ネットワーク ポートが管理 `up`ステータスに設定されている必要があります。"ONTAPコマンド リファレンス"の `up`の詳細を確認してください。
- LIFサービス ポリシーがすでに存在している必要があります。

タスク概要

ローカルのFabricPool階層化や外部のS3アプリにはクラスタ間LIFは必要ありません。

手順

1. クラスタ内のポートの一覧を表示します。

   ```
   network port show
   ```

   次の例は、 `cluster01`のネットワーク ポートを示しています：

   ```
   cluster01::> network port show
                                                                 Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

   `network port show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-port-show.html["ONTAPコマンド リファレンス"^]を参照してください。

2. システムSVMにクラスタ間LIFを作成します。

   `network interface create -vserver Cluster -lif *LIF_name* -service-policy default-intercluster -home-node *node* -home-port *port* -address *port_IP* -netmask *netmask*`

   次の例では、クラスタ間 LIF `cluster01_icl01`と `cluster01_icl02`を作成します：

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

`network interface create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-create.html["ONTAPコマンド リファレンス"^]を参照してください。

3. クラスタ間LIFが作成されたことを確認します。

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. クラスタ間LIFが冗長構成になっていることを確認します。

```
network interface show -service-policy default-intercluster -failover
```

次の例は、 `e0c`ポート上のクラスタ間LIF `cluster01_icl01`および `cluster01_icl02`が `e0d`ポートにフェイルオーバーすることを示しています。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

`network interface show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP S3オブジェクトストアサーバを作成する

ONTAPオブジェクト ストア サーバは、ファイル ストレージやブロック ストレージを提供するONTAP NAS / SANサーバとは異なり、S3オブジェクトとしてのデータを管理します。

開始する前に

S3 サーバー名を完全修飾ドメイン名（FQDN）として入力できるように準備しておいてください。クライアントはこれを使用して S3 にアクセスします。FQDN はバケット名で始まってはなりません。仮想ホスト形式でバケットにアクセスする場合、サーバー名は `mydomain.com`として使用されます。例：`bucketname.mydomain.com`。

自己署名CA証明書（前の手順で作成）または外部CAベンダーが署名した証明書が必要です。IPトラフィックがクラスタLIFのみを経由するローカルでの階層化では、CA証明書は必要ありません。

タスク概要

オブジェクトストアサーバを作成すると、UID 0のルートユーザーが作成されます。このルートユーザーに対してはアクセスキーとシークレットキーは生成されません。ONTAP管理者は `object-store-server users regenerate-keys`コマンドを実行して、このユーザーのアクセスキーとシークレットキーを設定する必要があります。

このrootユーザは使用しないことを推奨します。このrootユーザのアクセス キーまたはシークレット キーを使用するクライアント アプリケーションには、オブジェクト ストア内のすべてのバケットとオブジェクトに対するフル アクセスが付与されます。

`vserver object-store-server`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=vserver+object-store-server["ONTAPコマンド リファレンス"^]をご覧ください。

例 **2.** 手順

System Manager

既存のストレージVMにS3サーバーを追加する場合は、この手順を使用してください。新しいストレージVMにS3サーバーを追加するには、"S3用のストレージSVMを作成する"を参照してください。

Dataインターフェイス ロールに使用するIPアドレスを確認しておきます。

1. 既存のStorage VMでS3を有効にします。
   a. ストレージ VM を選択します。ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM を選択して、設定 をクリックし、**S3** の下の をクリックします。
   b. *S3 を有効にする*をクリックし、S3 サーバー名を入力します。
   c. 証明書タイプを選択します。

      システムで生成された証明書と独自の証明書のどちらを選択した場合も、その証明書がクライアント アクセスで必要になります。

   d. ネットワーク インターフェイスを入力します。
2. システム生成の証明書を選択した場合は、新しいストレージVMの作成が確認されると証明書情報が表示されます。*Download*をクリックし、クライアントがアクセスできるように保存してください。
   - 今後シークレット キーは表示されません。
   - 証明書情報が再度必要になった場合は、ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM を選択して、設定 をクリックします。

CLI

1. S3サーバを作成します。

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   追加のオプションは、S3サーバの作成時または作成後いつでも指定できます。

   - ローカル階層化を構成する場合、SVM名はデータSVMまたはシステムSVM（クラスタ）名のいずれかになります。
   - 証明書名は、サーバー CA 証明書（中間またはルート CA 証明書）ではなく、サーバー証明書（エンド ユーザー証明書またはリーフ証明書）の名前である必要があります。
   - HTTPS はポート 443 でデフォルトで有効になっています。 `-secure-listener-port`オプションを使用してポート番号を変更できます。

     HTTPSを有効にすると、SSL / TLSと適切に統合するためにCA証明書が必要になります。ONTAP 9.15.1以降では、S3オブジェクト ストレージでTLS1.3がサポートされます。

   - HTTPはデフォルトで無効になっています。有効にすると、サーバーはポート80でリッスンします。 `-is-http-enabled`オプションで有効にするか、 `-listener-port`オプションでポート番号を変更できます。

HTTPが有効な場合、要求と応答はクリア テキストでネットワークに送信されます。

2. S3が設定済みであることを確認します。

```
vserver object-store-server show
```

例

次のコマンドは、すべてのオブジェクト ストレージ サーバの設定値を確認します。

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                     HTTP Enabled: false
                                    HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

S3対応SVMへのストレージ容量の追加

ONTAP S3バケットを作成する

S3オブジェクトは_バケット_に保存されます。他のディレクトリ内のディレクトリ内にファイルとしてネストされることはありません。

開始する前に

S3サーバを含むStorage VMがすでに存在している必要があります。

タスク概要

- ONTAP 9.14.1以降では、S3 FlexGroupボリューム上にバケットを作成するとサイズ自動変更が有効になります。これにより、既存および新規のFlexGroupボリューム上でのバケットの作成時に、容量が過剰に割り当てられる事態を防止できます。FlexGroupボリュームは、以下のガイドラインに基づく必要最小限のサイズに変更されます。必要最小限のサイズとは、FlexGroupボリューム内のすべてのS3バケットの合計サイズです。
  - ONTAP 9.14.1以降では、新規バケットの作成の一環としてS3 FlexGroupボリュームが作成された場合、必要最小限のサイズになります。
  - ONTAP 9.14.1より前のバージョンで作成されたS3 FlexGroupボリュームについては、ONTAP 9.14.1以降で初めてバケットが作成または削除された際に必要最小限のサイズに変更されます。
  - ONTAP 9.14.1より前のバージョンでS3 FlexGroupボリュームが作成されており、すでに必要最小限のサイズに設定されている場合、ONTAP 9.14.1以降でバケットが作成または削除されてもボリュームのサイズは変更されません。

- ストレージサービスレベルは、事前定義されたアダプティブなQuality of Service（QoS）ポリシーグループで、*value*、*performance*、_extreme_のデフォルトレベルが用意されています。デフォルトのストレージサービスレベルの代わりに、カスタムQoSポリシーグループを定義してバケットに適用することもできます。ストレージサービス定義の詳細については、"ストレージ サービスの定義"を参照してください。パフォーマンス管理の詳細については、"パフォーマンス管理"を参照してください。ONTAP 9.8以降では、ストレージをプロビジョニングする際にQoSがデフォルトで有効になっています。プロビジョニングプロセス中または後で、QoSを無効にしたり、カスタムQoSポリシーを選択したりすることができます。
- ローカルでの容量階層化を設定する場合は、S3サーバが配置されているシステムStorage VMではなく、データStorage VMにバケットとユーザを作成します。
- リモート クライアント アクセスには、S3対応のStorage VMにバケットを設定する必要があります。S3対応でないStorage VMに作成したバケットは、ローカルの階層化にしか使用できません。
- ONTAP 9.14.1以降では、"MetroCluster構成内のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットを作成する"できます。
- CLIでバケットを作成するときは、次の2つのプロビジョニング オプションから選択できます。
  - 使用するアグリゲートとFlexGroupコンポーネントをONTAPで選択（デフォルト）
    - ONTAPでアグリゲートが自動的に選択され、最初のバケットのFlexGroupボリュームが作成されて設定されます。プラットフォームで使用可能な最上位のサービス レベルが自動的に選択されます。または、任意のストレージ サービス レベルを指定することもできます。以降このStorage VMに追加するすべてのバケットには同じFlexGroupボリュームが使用されます。
    - バケットを階層化に使用するかどうかを指定することもできます。指定した場合、階層化データ用に最適なパフォーマンスで低コストのメディアが選択されます。
  - 基盤となるアグリゲートとFlexGroupコンポーネントを選択します（高度な権限を持つコマンドオプションが必要です）：バケットとそれを含むFlexGroupボリュームを作成するアグリゲートを手動で選択し、各アグリゲートの構成要素の数を指定することもできます。バケットを追加する場合：
    - 新しいバケット用のアグリゲートとコンスティチュエントを指定した場合、バケット用に新しいFlexGroupが作成されます。
    - 新しいバケットの集計と構成要素を指定しない場合、新しいバケットは既存のFlexGroupに追加されます。詳細については、FlexGroupボリューム管理を参照してください。

      バケット作成時にアグリゲートとコンスティチュエントを指定した場合、QoSポリシーグループ（デフォルトまたはカスタム）は適用されません。後から `vserver object-store-server bucket modify`コマンドを使用して適用できます。

      `vserver object-store-server bucket modify`
      の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-object-store-server-show.html["ONTAPコマンドリファレンス"^]を参照してください。

注： Cloud Volumes ONTAPからバケットを提供している場合は、CLI手順を使用してください。基盤となるアグリゲートを手動で選択し、1つのノードのみを使用していることを確認することを強くお勧めします。両方のノードのアグリゲートを使用すると、ノードが地理的に離れたアベイラビリティゾーンに配置され、レイテンシの問題が発生しやすくなるため、パフォーマンスに影響する可能性があります。

ONTAP CLIを使用したS3バケットの作成

1. アグリゲートとFlexGroupコンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合は、admin権限レベルで十分です）： `set -privilege advanced`
2. バケットを作成します。

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -size [integer{KB|MB|GB|TB|PB}] [-comment text]
   [additional_options]
   ```

   ストレージVM名は、データストレージVMまたは `Cluster`（ローカル階層化を設定する場合のシステムストレージVM名）のいずれかです。

   パフォーマンスまたは使用量に基づいてバケットを作成する場合は、次のいずれかのオプションを使用します。

   - サービス レベル

     `-storage-service-level`オプションに次のいずれかの値を指定します： `value`、`performance`、または `extreme`。

   - 階層化

     `-used-as-capacity-tier true`オプションを含めます。

     使用するFlexGroupボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。

   - `-aggr-list`パラメータは、FlexGroupボリュームの構成要素に使用されるアグリゲートのリストを指定します。

     指定したエントリごとに、そのアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

   FlexGroupボリューム全体で一貫したパフォーマンスが得られるように、ディスク タイプとRAIDグループ構成をすべてのアグリゲートで同じにする必要があります。

   - `-aggr-list-multiplier`パラメータは、FlexGroupボリュームの作成時に `-aggr-list`パラメータでリストされているアグリゲートを反復処理する回数を指定します。

     `-aggr-list-multiplier`パラメータのデフォルト値は4です。

3. 必要に応じてQoSポリシー グループを追加します。

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. バケットが作成されたことを確認します。

```
vserver object-store-server bucket show [-instance]
```

例

次の例では、ストレージ VM `vs1`のサイズ `1TB`のバケットを作成し、アグリゲートを指定します：

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

System Managerを使用したS3バケットの作成

1. S3対応Storage VMに新しいバケットを追加します。
   a. *Storage > Buckets*をクリックし、*Add*をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。
      - この時点で*保存*をクリックすると、次のデフォルト設定でバケットが作成されます：
        - すでに有効なグループ ポリシーがないかぎり、いずれのユーザにもバケットへのアクセスは許可されません。

> S3のrootユーザにはオブジェクト ストアへの無制限のアクセスが付与されるため、ONTAPオブジェクト ストレージの管理や権限の共有には使用しないでください。代わりに、管理者権限を割り当てたユーザまたはグループを作成してください。

        - システムで使用できる最も高いQuality of Service（パフォーマンス）レベル。
      - これらのデフォルト値でバケットを作成するには、*保存*をクリックします。

追加の権限と制限の設定

バケットを構成するときに、[その他のオプション] をクリックしてオブジェクトのロック、ユーザー権限、パフォーマンスレベルの設定を構成することも、後でこれらの設定を変更することもできます。

S3オブジェクトストアをFabricPool階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に使用（階層化されたデータに最適なパフォーマンスを備えた低コストのメディアを使用する）を選択することを検討してください。

バケットでバージョン管理が有効になっている場合、S3 クライアントを使用して、オブジェクトの特定のバージョンに Object Lock 保持期間を設定できます。オブジェクトの特定のバージョンをロックしても、オブジェクトの他のバージョンが削除されることは防止されません。後でリカバリできるようにオブジェクトのバージョン管理を有効にする場合は、**Enable Versioning** を選択します。バケットでオブジェクトロックを有効にすると、バージョン管理はデフォルトで有効になります。オブジェクトのバージョン管理の詳細については、"AmazonのS3バケットでバージョニングを使用する"を参照してください。

9.14.1以降、S3バケットでオブジェクトロックがサポートされます。S3 Object Lockは、バケットの作成時に

有効にする必要があります。既存のバケットではObject Lockを有効にできません。Object Lockは、ネイティブS3ユースケースでのみ使用できます。S3プロトコルを使用するように設定されたマルチプロトコルNASボリュームでは、SnapLockを使用してデータをWORMストレージにコミットする必要があります。S3オブジェクトロックには標準のSnapLockライセンスが必要です。このライセンスは"ONTAP One"に含まれています。

ONTAP Oneより前は、SnapLockライセンスはSecurity and Complianceバンドルに含まれていました。Security and Complianceバンドルは現在提供されていませんが、引き続き有効です。現在は必須ではありませんが、既存のお客様は"ONTAP Oneにアップグレード"を選択できます。バケットでオブジェクトロックを有効にする場合は、"SnapLockライセンスがインストールされていることを確認する"が必要です。SnapLockライセンスがインストールされていない場合は、オブジェクトロックを有効にする前に"インストール"する必要があります。

SnapLockライセンスがインストールされていることを確認したら、バケット内のオブジェクトが削除または上書きされるのを防ぐため、*オブジェクトのロックを有効にする*を選択します。ロックは、すべてのオブジェクトまたは特定のバージョンのオブジェクトに対して有効にできます。また、SnapLockコンプライアンス クロックがクラスタノードに対して初期化されている場合にのみ有効にできます。以下の手順に従ってください：

1. SnapLockコンプライアンス クロックがクラスタ内のどのノードでも初期化されていない場合は、*Initialize SnapLock Compliance Clock*ボタンが表示されます。*Initialize SnapLock Compliance Clock*をクリックして、クラスタ ノードでSnapLockコンプライアンス クロックを初期化します。
2. *ガバナンス*モードを選択すると、時間ベースのロックが有効になり、オブジェクトに対して_Write Once, Read Many (WORM)_権限が許可されます。_ガバナンス_モードでも、特定の権限を持つ管理者ユーザーはオブジェクトを削除できます。
3. オブジェクトの削除と更新に関してより厳格なルールを適用する場合は、*Compliance*モードを選択してください。このオブジェクトロックモードでは、指定された保持期間の経過後にのみオブジェクトが期限切れになります。保持期間が指定されていない場合、オブジェクトは無期限にロックされたままになります。
4. ロックを一定の期間だけ有効にする場合は、ロックの保持期間を日単位または年単位で指定します。

ロックは、バージョン管理に対応しているS3バケットとバージョン管理に対応していないS3バケットに適用されます。オブジェクト ロックは、NASオブジェクトには適用されません。

バケットの保護と権限の設定、およびパフォーマンス サービス レベルを設定できます。

権限を設定するには、事前にユーザとグループを作成しておく必要があります。

詳細については、"新規バケット用ミラーの作成"を参照してください。

バケットへのアクセスの確認

S3クライアント アプリケーション（ONTAP S3または外部のサードパーティ アプリケーション）では、以下を入力して、新しく作成したバケットへのアクセスを確認できます。

- S3サーバのCA証明書。
- ユーザのアクセス キーとシークレット キー。
- S3サーバのFQDN名とバケット名。

ONTAP S3バケットサイズを増減する

必要に応じて、既存バケットのサイズを増減できます。

手順

System ManagerまたはONTAP CLIを使用してバケット サイズを管理できます。

System Manager

1. **Storage > Buckets** を選択し、変更するバケットを見つけます。
2. バケット名の横にあるをクリックし、*編集*を選択します。
3. *Edit bucket*ウィンドウで、バケットの容量を変更します。
4. 保存

CLI

1. バケットの容量を変更します。

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

MetroCluster構成内のミラーされたアグリゲートまたはミラーされていないアグリゲートに ONTAP S3 バケットを作成する

ONTAP 9.14.1以降では、MetroCluster FC構成およびIP構成のミラーされたアグリゲートまたはミラーされていないアグリゲートにバケットをプロビジョニングできます。

タスク概要

- デフォルトでは、バケットはミラーされたアグリゲートにプロビジョニングされます。
- "バケットの作成"で概説されているのと同じプロビジョニングガイドラインが、MetroCluster環境でバケットを作成する場合に適用されます。
- 次の S3 オブジェクト ストレージ機能は MetroCluster 環境ではサポートされて*いません*：
  - SnapMirror S3
  - S3バケットのライフサイクル管理
  - **Compliance** モードでの S3 オブジェクトロック

    ガバナンス モードでの S3 オブジェクトロックがサポートされています。

  - ローカルFabricPool階層化

開始する前に

S3サーバを含むSVMがすでに存在している必要があります。

CLI

1. アグリゲートとFlexGroupコンポーネントを自分で選択する場合は、権限レベルをadvancedに設定します（それ以外の場合は、admin権限レベルで十分です）： `set -privilege advanced`
2. バケットを作成します。

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   `-use-mirrored-aggregates`オプションを `true`または`false`に設定します。ミラーされたアグリゲートとミラーされていないアグリゲートのどちらを使用するかによって異なります。

   デフォルトでは、 `-use-mirrored-aggregates`オプションは `true`に設定されています。

   - SVM名はデータSVMである必要があります。
   - オプションを指定しない場合、800GBのバケットが作成され、システムで使用可能な最上位のサービス レベルが設定されます。
   - パフォーマンスまたは使用量に基づいてバケットを作成する場合は、次のいずれかのオプションを使用します。
     - サービス レベル

       `-storage-service-level`オプションに次のいずれかの値を指定します： `value`、 `performance`、または `extreme`。

     - 階層化

       `-used-as-capacity-tier true`オプションを含めます。

   - 使用するFlexGroupボリュームを作成するアグリゲートを指定する場合は、次のオプションを使用します。
     - `-aggr-list`パラメータは、FlexGroupボリュームの構成要素に使用されるアグリゲートのリストを指定します。

       指定したエントリごとに、そのアグリゲート上にコンスティチュエントが1つ作成されます。同じアグリゲートを複数回指定すると、そのアグリゲート上に複数のコンスティチュエントを作成できます。

FlexGroupボリューム全体で一貫したパフォーマンスが得られるように、ディスク タイプとRAIDグループ構成をすべてのアグリゲートで同じにする必要があります。

   - `-aggr-list-multiplier`パラメータは、FlexGroupボリュームの作成時に `-aggr-list`パラメータでリ

ストされているアグリゲートを反復処理する回数を指定します。

`-aggr-list-multiplier`パラメータのデフォルト値は4です。

3. 必要に応じてQoSポリシー グループを追加します。

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. バケットが作成されたことを確認します。

```
vserver object-store-server bucket show [-instance]
```

例

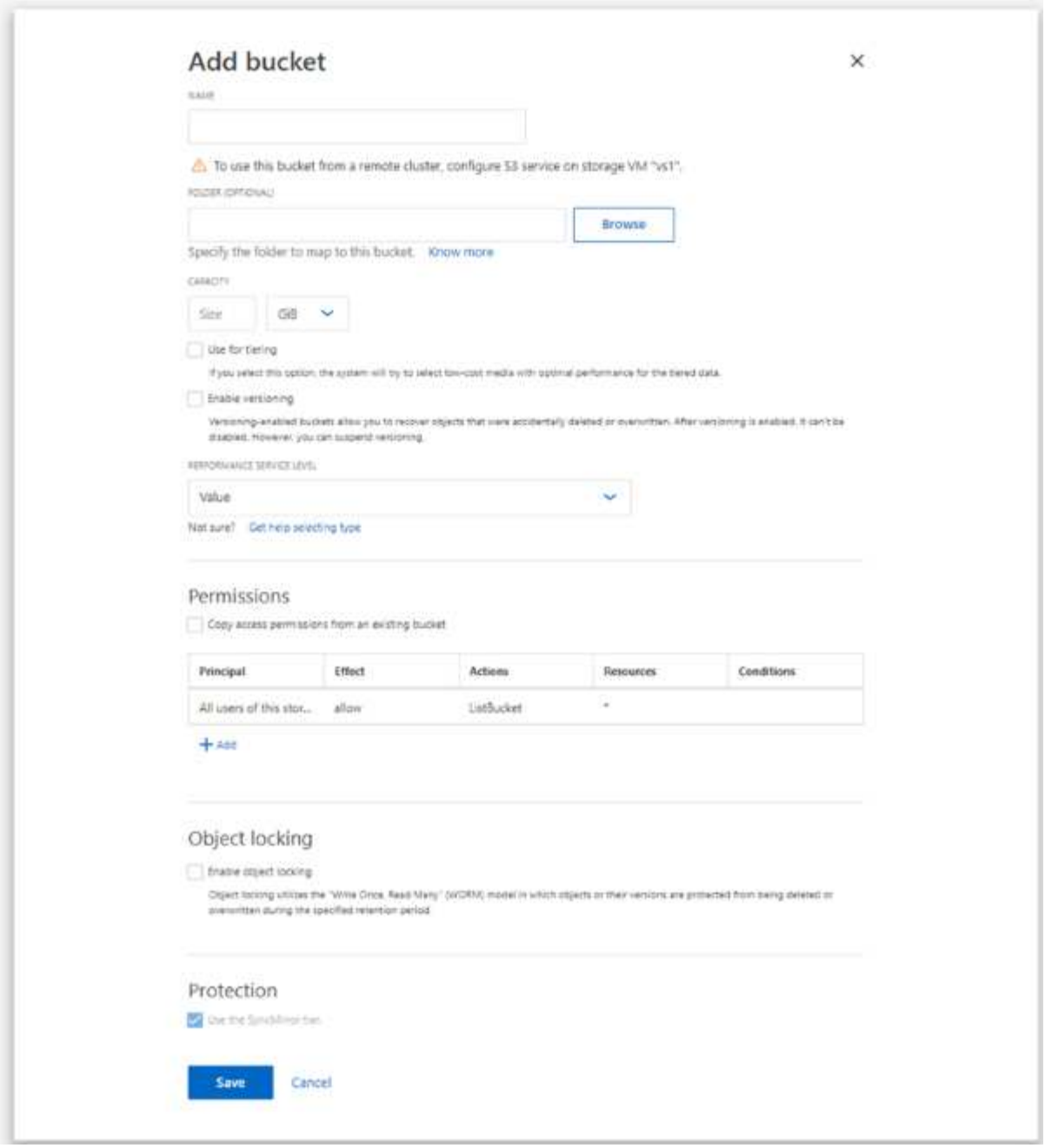
次の例では、ミラーされたアグリゲートにサイズが1TBのSVM vs1のバケットを作成しています。

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. S3対応Storage VMに新しいバケットを追加します。
   a. *Storage > Buckets*をクリックし、*Add*をクリックします。
   b. 名前を入力し、Storage VMを選択してサイズを入力します。

      デフォルトでは、バケットはミラーリングされたアグリゲート上にプロビジョニングされます。ミラーされていないアグリゲート上にバケットを作成する場合は、「その他のオプション」を選択し、「保護」の下にある「**SyncMirror**階層を使用」のチェックボックスをオフにしてください（次の図を参照）：



- この時点で*保存*をクリックすると、次のデフォルト設定でバケットが作成されます：
  - すでに有効なグループ ポリシーがないかぎり、いずれのユーザにもバケットへのアクセスは許可されません。

> S3のrootユーザにはオブジェクト ストアへの無制限のアクセスが付与されるため、ONTAPオブジェクト ストレージの管理や権限の共有には使用しないでください。代わりに、管理者権限を割り当てたユーザまたはグループを作成してください。

  - システムで使用できる最も高いQuality of Service（パフォーマンス）レベル。
- バケットを構成するときに、[その他のオプション] をクリックしてユーザー権限とパフォーマンスレベルを構成することも、後でこれらの設定を変更することもできます。

- *その他のオプション*を使用して権限を設定する前に、ユーザーとグループを作成しておく必要があります。
- S3オブジェクトストアをFabricPool階層化に使用する場合は、パフォーマンスサービスレベルではなく、階層化に使用（階層化されたデータに最適なパフォーマンスを備えた低コストのメディアを使用する）を選択することを検討してください。

2. S3クライアントアプリ（別のONTAPシステムまたは外部のサードパーティアプリ）で、次のように入力して新しいバケットへのアクセスを確認します：
   - S3サーバのCA証明書。
   - ユーザのアクセス キーとシークレット キー。
   - S3サーバのFQDN名とバケット名。

ONTAP S3バケットライフサイクル管理ルールを作成する

ONTAP 9.13.1以降では、ライフサイクル管理ルールを作成して、S3バケット内のオブジェクトのライフサイクルを管理できます。バケット内の特定のオブジェクトに対して削除ルールを定義し、そのルールを適用してバケット オブジェクトを期限切れにできます。これにより、保持要件を満たしたり、S3オブジェクト ストレージ全体を効率的に管理したりできます。

バケットオブジェクトに対してオブジェクトロックが有効になっている場合、オブジェクトの有効期限に関するライフサイクル管理ルールはロックされたオブジェクトには適用されません。オブジェクトロックの詳細については、"バケットの作成"をご覧ください。

開始する前に

- S3サーバーとバケットを含むS3対応SVMが既に存在している必要があります。詳細については、"S3用SVMの作成"を参照してください。
- マルチプロトコル NAS ボリュームで S3 を使用する場合、またはMetroCluster構成で S3 を使用する場合、バケットライフサイクル管理ルールはサポートされません。

タスク概要

ライフサイクル管理ルールを作成する際にバケット オブジェクトに適用できる削除操作は、以下のとおりです。

- 現在のバージョンの削除 - このアクションは、ルールで識別されたオブジェクトを期限切れにします。バケットでバージョニングが有効になっている場合、S3 は期限切れのオブジェクトをすべて利用不可にします。バージョニングが有効になっていない場合、このルールはオブジェクトを完全に削除します。CLI アクションは `Expiration`です。
- 非現行バージョンの削除 - このアクションは、S3 が非現行オブジェクトを永久に削除できるタイミングを指定します。CLI アクションは `NoncurrentVersionExpiration`です。

非最新バージョンは、現在のバージョンの作成または変更時刻に基づいています。非最新オブジェクトの削除を遅延すると、オブジェクトを誤って削除または上書きした場合に役立ちます。たとえば、非最新バージョンが最新でなくなってから5日後に削除するように有効期限ルールを設定できます。たとえば、2014年1月1日午前10時30分（UTC）に、`photo.gif`（バージョンID `111111`）というオブジェクトを作成したとします。2014年1月2日午前11時30分（UTC）に、`photo.gif`（バージョンID `111111`）を誤って削除し、新しいバージョンID（バージョンID `4857693`など）の削除マーカーが作成されます。削除が完全になるまでに、`photo.gif`（バージョンID `111111`）の元のバージョンを復元する5日間の猶予があります。2014年1月8日午前0時（UTC）に、有効期限のライフサイクルルールが実行され、`photo.gif`（バージョンID `111111`）が非最新バージョンになってから5日後に完全に削除されます。

- 期限切れの削除マーカーの削除 - このアクションは、期限切れのオブジェクト削除マーカーを削除します。バージョニング対応のバケットでは、削除マーカーが付いたオブジェクトが現在のバージョンになります。オブジェクト自体は削除されず、それらに対してアクションを実行することはできません。これらのオブジェクトは、現在のバージョンが関連付けられていない場合、期限切れになります。CLIアクションは `Expiration`です。
- 未完了のマルチパートアップロードの削除 - このアクションは、マルチパートアップロードの進行中状態を保持する最大期間（日数）を設定します。この期間を過ぎると、マルチパートアップロードは削除されます。CLIアクションは `AbortIncompleteMultipartUpload`です。

使用するインターフェースによって手順が異なります。ONTAP 9.13.1ではCLIを使用する必要があります。ONTAP 9.14.1以降では、System Managerも使用できます。

CLIを使用したライフサイクル管理ルールの管理

ONTAP 9.13.1以降では、ONTAP CLIを使用して、S3バケット内のオブジェクトを期限切れにするライフサイクル管理ルールを作成できます。

開始する前に

CLIでバケット ライフサイクル管理ルールを作成する際には、それぞれの有効期限操作タイプの必須フィールドを定義する必要があります。これらのフィールドは、ルールの作成後に変更できます。次の表に、それぞれの操作タイプに固有のフィールドを示します。

操作タイプ	固有のフィールド
NonCurrentVersionExpiration	• `-non-curr-days` - 最新ではないバージョンが削除されるまでの日数 • `-new-non-curr-versions` - 保持する最新の非現行バージョンの数
Expiration	• `-obj-age-days` - 作成から現在のバージョンのオブジェクトを削除できるまでの日数 • `-obj-exp-date` - オブジェクトの有効期限が切れる特定の日付 • `-expired-obj-del-markers` - オブジェクトの削除マーカーをクリーンアップする
AbortIncompleteMultipartUpload	• `-after-initiation-days` - アップロードを中止できる開始後の日数

バケット ライフサイクル管理ルールを特定のオブジェクトにのみ適用するには、ルールの作成時に各フィルタを設定する必要があります。ルールの作成時にフィルタが設定されていない場合、ルールはバケット内のすべてのオブジェクトに適用されます。

すべてのフィルタは、最初の作成後に変更できます（次の項目を_除く_）：+

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

手順

1. 有効期限アクションタイプの必須フィールドを指定した `vserver object-store-server bucket lifecycle-management-rule create`コマンドを使用して、バケットライフサイクル管理ルールを作成します。

例

次のコマンドは、NonCurrentVersionExpirationバケット ライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

例

次のコマンドは、Expirationバケット ライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

例

次のコマンドは、AbortIncompleteMultipartUploadバケット ライフサイクル管理ルールを作成します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

System Managerを使用したライフサイクル管理ルールの管理

ONTAP 9.14.1以降では、System Managerを使用してS3オブジェクトの有効期限を設定できるようになりました。S3オブジェクトのライフサイクル管理ルールを追加、編集、削除できます。また、あるバケット用に作成したライフサイクルルールをインポートし、別のバケット内のオブジェクトに適用することも可能です。有効なルールを無効にして、後で有効にすることも可能です。

ライフサイクル管理ルールの追加

1. *Storage > Buckets*をクリックします。
2. 有効期限ルールを指定するバケットを選択します。
3. ⋮アイコンをクリックして、*ライフサイクルルールの管理*を選択します。
4. 追加 **>** ライフサイクルルール をクリックします。
5. [Add a lifecycle rule]ページで、ルールの名前を追加します。
6. ルールのスコープを定義します。ルールをバケット内のすべてのオブジェクトに適用するか、特定のオブジェクトに適用するかを指定します。オブジェクトを指定する場合は、次のいずれかのフィルタ条件を少なくとも1つ追加します。
   a. プレフィックス：ルールを適用するオブジェクトキー名のプレフィックスを指定します。通常は、オブジェクトのパスまたはフォルダです。ルールごとに1つのプレフィックスを入力できます。有効なプレフィックスを指定しない限り、ルールはバケット内のすべてのオブジェクトに適用されます。
   b. タグ：ルールを適用するオブジェクトのキーと値のペア（タグ）を最大3つ指定します。フィルタリングには有効なキーのみが使用されます。値は任意です。ただし、値を追加する場合は、対応するキーに有効な値のみを追加するようにしてください。
   c. サイズ：オブジェクトの最小サイズと最大サイズの範囲を制限できます。どちらか一方または両方の値を入力できます。デフォルトの単位はMiBです。
7. 操作を指定します。
   a. オブジェクトの現在のバージョンを期限切れにする：作成から指定した日数後、または指定した日付に、現在のすべてのオブジェクトを永久に使用不可にするルールを設定します。*期限切れオブジェクトの削除マーカーを削除する*オプションが選択されている場合、このオプションは使用できません。
   b. 現在のバージョン以外を完全に削除する：現在のバージョン以外を削除するまでの日数と、保持するバージョンの数を指定します。
   c. 期限切れのオブジェクトの削除マーカーを削除：期限切れの削除マーカーを持つオブジェクト、つまり、関連付けられている現在のオブジェクトのない削除マーカーを削除するには、このアクションを選択します。

このオプションは、保持期間後にすべてのオブジェクトが自動的に削除される*オブジェクトの現在のバージョンを期限切れにする*オプションを選択すると使用できなくなります。また、オブジェクトタグがフィルタリングに使用されている場合も、このオプションは使用できなくなります。

d. 不完全なマルチパートアップロードを削除：不完全なマルチパートアップロードを削除するまでの日数を設定します。指定した保存期間内に進行中のマルチパートアップロードが失敗した場合、不完全なマルチパートアップロードを削除できます。このオプションは、オブジェクトタグをフィルタリングに使用している場合は使用できません。

e. *保存*をクリックします。

ライフサイクル ルールのインポート

1. *Storage > Buckets*をクリックします。
2. 有効期限ルールのインポート先のバケットを選択します。
3. ⋮アイコンをクリックして、*ライフサイクルルールの管理*を選択します。
4. *追加 > ルールのインポート*をクリックします。
5. ルールをインポートするバケットを選択します。選択したバケットに対して定義されているライフサイクル管理ルールが表示されます。
6. インポートするルールを選択します。ルールは一度に1つずつ選択できます。デフォルトでは最初のルールが選択されています。
7. *インポート*をクリックします。

ルールの編集、削除、または無効化

編集できるのは、ルールに関連付けられたライフサイクル管理アクションのみです。ルールがオブジェクトタグでフィルタリングされている場合、*期限切れのオブジェクト削除マーカーを削除*および*不完全なマルチパートアップロードを削除*オプションは使用できません。

ルールを削除すると、そのルールはそれまで関連付けられていたオブジェクトには適用されなくなります。

1. *Storage > Buckets*をクリックします。
2. ライフサイクル管理ルールを編集、削除、または無効にするバケットを選択します。
3. ⋮アイコンをクリックして、*ライフサイクルルールの管理*を選択します。
4. 目的のルールを選択します。編集と無効化は、一度に1つのルールに対して行うことができます。削除は一度に複数のルールに対して行うことができます。
5. 編集、削除、または*無効化*を選択して手順を完了します。

ONTAP S3ユーザーを作成する

特定の権限を指定してS3ユーザを作成します。許可されたクライアントだけに接続を制限するには、すべてのONTAPオブジェクト ストアでユーザ認証が必要です。

開始する前に

S3対応のStorage VMがすでに存在している必要があります。

タスク概要

S3ユーザにはStorage VM内の任意のバケットへのアクセスを許可できます。S3ユーザを作成すると、そのユーザのアクセス キーとシークレット キーも生成されます。それらとともに、オブジェクト ストアのFQDNとバケット名をユーザと共有する必要があります。

セキュリティ強化のため、ONTAP 9.15.1以降では、アクセスキーとシークレットキーはS3ユーザーの作成時にのみ表示され、再表示はできなくなります。キーを紛失した場合は、"新しいキーを再生成する必要がある"。

バケット ポリシーまたはオブジェクト サーバ ポリシーで、S3ユーザに特定のアクセス権限を付与できます。

新しいオブジェクト ストア サーバを作成すると、ONTAPによって、すべてのバケットにアクセスできる権限を持つrootユーザ（UID 0）が作成されます。ONTAP S3をrootユーザとして管理するのではなく、特定の権限を設定したadminユーザ ロールを作成することを推奨します。

CLI

1. S3 ユーザーを作成します
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - コメントの追加は任意です。
   - ONTAP 9.14.1以降では、 `-key-time-to-live`パラメータでキーの有効期間を定義できます。アクセスキーの有効期限を示す保持期間を次の形式で追加できます：`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`例えば、1日2時間3分4秒の保持期間を入力する場合は、値を `P1DT2H3M4S`と入力します。指定がない限り、キーは無期限に有効です。

     以下の例では、ストレージ VM `vs0`上に名前 `sm_user1`のユーザーを作成し、キーの保持期間は 1 週間です。

   ```
   vserver object-store-server user create -vserver vs0 -user sm_user1 -key-time-to-live P1W
   ```

2. アクセス キーとシークレット キーは必ず保存してください。これらは、S3クライアントからのアクセスに必要になります。

System Manager

1. *ストレージ > ストレージVM*をクリックします。ユーザーを追加するストレージVMを選択し、*設定*を選択してから、S3の下の をクリックします。
2. ユーザーを追加するには、*Users > Add*をクリックします。
3. ユーザの名前を入力します。
4. ONTAP 9.14.1以降では、ユーザ用に作成されるアクセスキーの保持期間を指定できます。保持期間は日、時間、分、または秒で指定でき、この期間を過ぎるとキーは自動的に期限切れになります。デフォルトでは、値は `0`に設定されており、キーが無期限に有効であることを示します。
5. *Save*をクリックします。ユーザーが作成され、ユーザーのアクセスキーとシークレットキーが生成されます。
6. アクセス キーとシークレット キーをダウンロードまたは保存します。これらは、S3クライアントからのアクセスに必要になります。

次の手順

- S3グループの作成と変更

バケットへのアクセスを制御するために**ONTAP S3**ユーザーグループを作成または変更する

適切なアクセス許可を設定したユーザのグループを作成すると、バケットへのアクセス管理が簡単になります。

開始する前に

S3ユーザがS3対応SVMにすでに存在している必要があります。

タスク概要

S3グループのユーザにはある1つSVMの任意のバケットへのアクセスを許可できますが、複数のSVMへのアクセスは許可できません。グループのアクセス権限は次の2つの方法で設定できます。

- バケット レベル

  S3ユーザのグループを作成したあと、バケット ポリシーのステートメントでグループの権限を指定します。この権限はそのバケットにのみ適用されます。

- SVMレベル

  S3ユーザのグループを作成したあと、グループ定義にオブジェクト サーバ ポリシーの名前を指定します。これらのポリシーがグループ メンバーのバケットとアクセスを決定します。

System Manager

1. ストレージ VM を編集します。ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。
2. グループを追加：*グループ*を選択し、*追加*を選択します。
3. グループ名を入力し、リストからユーザを選択します。
4. 既存のグループ ポリシーを選択するか新規に追加します。あとで追加することもできます。

CLI

1. S3グループを作成します（ `vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]`） `-policies`オプションは、オブジェクトストアにバケットが1つしかない構成では省略できます。グループ名はバケットポリシーに追加できます。 `-policies`オプションは、オブジェクトストレージサーバポリシーの作成後に `vserver object-store-server group modify`コマンドで追加できます。

ONTAP S3キーを再生成し、保持期間を変更する

アクセス キーとシークレット キーは、S3クライアント アクセスを有効にするユーザの作成時に自動的に生成されます。キーの有効期限が切れた場合や、キーが侵害された場合には、ユーザのキーを再生成できます。

アクセスキーの生成については、"S3ユーザの作成"を参照してください。

System Manager

1. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
2. *設定*タブで、*S3*タイルの をクリックします。
3. **Users** タブで、アクセスキーがないこと、またはユーザーのキーの有効期限が切れていることを確認します。
4. キーを再生成する必要がある場合は、ユーザーの横にあるをクリックし、*キーの再生成*をクリックします。
5. デフォルトでは、生成されたキーの有効期限は無期限です。9.14.1以降では、キーの保持期間を変更できます。この期間が過ぎると、キーは自動的に期限切れになります。保持期間を日、時間、分、または秒単位で入力します。
6. *保存*をクリックします。キーが再生成されます。キーの保持期間の変更は直ちに有効になります。
7. アクセス キーとシークレット キーをダウンロードまたは保存します。これらは、S3クライアントからのアクセスに必要になります。

CLI

1. `vserver object-store-server user regenerate-keys`コマンドを実行して、ユーザーのアクセスキーとシークレットキーを再生成します。
2. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できるようになりました。保持期間が過ぎると、キーは自動的に期限切れになります。保持期間は次の形式で追加できます： `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`例えば、1日2時間3分4秒の保持期間を入力する場合は、値を `P1DT2H3M4S`と入力します。

```
vserver object-store-server user regenerate-keys -vserver svm_name
-user user -key-time-to-live 0
```

3. アクセス キーとシークレット キーを保存します。これらは、S3クライアントからのアクセスに必要になります。

アクセス ポリシー ステートメントの作成と変更

ONTAP S3バケットとオブジェクトストアサーバのポリシーについて学ぶ

S3リソースへのユーザとグループのアクセスは、バケットとオブジェクト ストア サーバのポリシーで制御されます。ユーザやグループの数が少ない場合はバケット レベルでアクセスを制御すれば十分ですが、ユーザやグループが多数の場合はオブジェクト ストア サーバ レベルでアクセスを制御した方が簡単です。

デフォルトの**ONTAP S3**バケットポリシーにアクセスルールを追加する

デフォルトのバケット ポリシーにアクセス ルールを追加できます。デフォルト ポリシーのアクセス制御対象は対応するバケットであるため、バケットが1つだけの場合はデフォルト ポリシーが最も適しています。

開始する前に

S3サーバとバケットを含むS3対応のStorage VMがすでに存在している必要があります。

権限を付与するには、事前にユーザまたはグループを作成しておく必要があります。

タスク概要

新しいユーザーやグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。 `vserver object-store-server bucket policy`の詳細については、"ONTAPコマンド リファレンス"をご覧ください。

ユーザとグループの権限は、バケットの作成時、または必要に応じてあとから付与することができます。バケットの容量やQoSポリシー グループの割り当ても変更できます。

ONTAP 9.9.1 以降、ONTAP S3 サーバで AWS クライアントオブジェクトのタグ付け機能をサポートする予定の場合は、 `GetObjectTagging`、 `PutObjectTagging`、および `DeleteObjectTagging`のアクションをバケットまたはグループポリシーを使用して許可する必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

手順

1. バケットを編集するには、「ストレージ > バケット」をクリックし、対象のバケットをクリックして「編集」をクリックします。権限を追加または変更する際には、以下のパラメータを指定できます：
   - プリンシパル：アクセスが許可されるユーザーまたはグループ。
   - 効果：ユーザーまたはグループへのアクセスを許可または拒否します。
   - アクション：特定のユーザーまたはグループに対してバケット内で許可されるアクション。
   - リソース：アクセスが許可または拒否されるバケット内のオブジェクトのパスと名前。

     デフォルトの ***bucketname*** と ***bucketname/**** は、バケット内のすべてのオブジェクトへのアクセスを許可します。また、単一のオブジェクトへのアクセスを許可することもできます。たとえば、***bucketname/*_readme.txt*** などです。

   - 条件（オプション）：アクセス試行時に評価される条件式。例えば、アクセスを許可または拒否するIPアドレスのリストを指定できます。

> ONTAP 9.14.1以降では、*Resources*フィールドでバケットポリシーの変数を指定できます。これらの変数はプレースホルダであり、ポリシーの評価時にコンテキスト値に置き換えられます。例えば、 `${aws:username}`がポリシーの変数として指定されている場合、この変数はリクエストコンテキストのユーザー名に置き換えられ、そのユーザーに対して設定されたポリシーアクションを実行できます。

CLI

手順

1. バケット ポリシーにステートメントを追加します。

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

次のパラメータでアクセス権限を定義します。

`-effect`	アクセスを許可するか拒否するかを指定します。
`-action`	`*`すべてのアクションを意味するように指定することも、次の 1 つ以上のリストを指定することもできます： `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,`および `ListMultipartUploadParts`。

`-principal`	S3ユーザまたはグループのリストを指定します。 • 指定できるユーザまたはグループの数は最大10個までです。 • S3グループを指定する場合は、次の形式にする必要があります `group/group_name`. • `*`を指定すると、パブリックアクセス（アクセスキーとシークレットキーなしでのアクセス）を意味します。 • プリンシパルが指定されていない場合は、ストレージVM内のすべてのS3ユーザーにアクセスが許可されます。
`-resource`	バケットとそれに含まれるオブジェクト。ワイルドカード文字 `*`と `?`を使用して、リソースを指定するための正規表現を作成できます。リソースに対して、ポリシー内で変数を指定できます。これらのポリシー変数はプレースホルダであり、ポリシーが評価される際にコンテキスト値に置き換えられます。

`-sid`オプションを使用して、コメントとしてテキスト文字列をオプションで指定できます。

例

次の例では、Storage VM svm1.example.comのbucket1に対するオブジェクト ストア サーバ バケット ポリシーのステートメントを作成し、オブジェクト ストア サーバ ユーザuser1にreadmeフォルダへのアクセスを許可するように指定しています。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

次の例では、Storage VM svm1.example.comのbucket1に対するオブジェクト ストア サーバ バケット ポリシーのステートメントを作成し、オブジェクト ストア サーバ グループgroup1にすべてのオブジェクトへのアクセスを許可するように指定しています。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

ONTAP 9.14.1以降では、バケットポリシーに変数を指定できます。次の例では、ストレージVM `svm1`と `bucket1`のサーババケットポリシーステートメントを作成し、 `${aws:username}`をポリシーリソースの変数として指定します。ポリシーが評価されると、ポリシー変数はリクエストコンテキストのユーザー名に置き換えられ、そのユーザーに対して設定されたポリシーアクションを実行できます。たとえ

ば、次のポリシーステートメントが評価されると、 `${aws:username}`はS3操作を実行するユーザーに置き換えられます。ユーザー `user1`が操作を実行すると、そのユーザーには `bucket1`として `bucket1/user1/*`へのアクセスが許可されます。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

ONTAP S3オブジェクトストアサーバポリシーを作成または変更する

オブジェクト ストア内のバケットに適用できるポリシーを作成できます。オブジェクト ストア サーバ ポリシーはユーザのグループに関連付けることができるため、複数のバケットへのリソース アクセスの管理が簡単になります。

開始する前に

S3サーバとバケットを含むS3対応のSVMがすでに存在している必要があります。

タスク概要

オブジェクト ストレージ サーバ グループにデフォルトまたはカスタムのポリシーを指定することで、SVMレベルでアクセス ポリシーを有効にすることができます。ポリシーは、グループ定義で指定するまで有効になりません。

> オブジェクト ストレージ サーバ ポリシーを使用する場合、プリンシパル（ユーザとグループ）はポリシーではなくグループ定義に指定します。

ONTAP S3リソースへのアクセスに使用するデフォルトの読み取り専用ポリシーは3つあります。

- FullAccess
- NoS3Access
- ReadOnlyAccess

新しいカスタムポリシーを作成し、新しいユーザーやグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。"ONTAPコマンド リファレンス"の `vserver object-store-server policy`の詳細をご覧ください。

ONTAP 9.9.1 以降、ONTAP S3 サーバで AWS クライアントオブジェクトのタグ付け機能をサポートする予定の場合は、 `GetObjectTagging`、 `PutObjectTagging`、および `DeleteObjectTagging`のアクションをバケットまたはグループポリシーを使用して許可する必要があります。

実行する手順は、System ManagerとCLIのどちらのインターフェイスを使用するかによって異なります。

System Manager

System Manager を使用してオブジェクト ストア サーバー ポリシーを作成または変更する

手順

1. ストレージ VM を編集します。ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。
2. ユーザーを追加するには：*ポリシー*をクリックし、*追加*をクリックします。
   a. ポリシー名を入力し、リストからグループを選択します。
   b. 既存のデフォルト ポリシーを選択するか、新しいポリシーを追加します。

      グループ ポリシーを追加または変更する際には次のパラメータを指定できます。

      - Group：アクセスを付与するグループ。
      - Effect：1つ以上のグループにアクセスを許可するか拒否するか。
      - Actions：特定のグループに許可する1つ以上のバケット内での処理。
      - リソース：アクセスが許可または拒否される1つ以上のバケット内のオブジェクトのパスと名前。例：
        - * はストレージ VM 内のすべてのバケットへのアクセスを許可します。
        - **bucketname** と **bucketname/*** は、特定のバケット内のすべてのオブジェクトへのアクセスを許可します。
        - **bucketname/readme.txt** は、特定のバケット内のオブジェクトへのアクセスを許可します。
   c. 必要に応じて、既存のポリシーにステートメントを追加します。

CLI

CLI を使用してオブジェクト ストア サーバー ポリシーを作成または変更する

手順

1. オブジェクト ストレージ サーバ ポリシーを作成します。

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. ポリシーのステートメントを作成します。

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   次のパラメータでアクセス権限を定義します。

`-effect`	アクセスを許可するか拒否するかを指定します。

`-action`	`*`すべてのアクションを意味するように指定することも、次の 1 つ以上のリストを指定することもできます： `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads,`および `ListMultipartUploadParts`。
`-resource`	バケットとそれに含まれるオブジェクト。ワイルドカード文字 `*`と `?`を使用して、リソースを指定するための正規表現を作成できます。

`-sid`オプションを使用して、コメントとしてテキスト文字列をオプションで指定できます。

デフォルトでは、新しいステートメントはステートメントリストの末尾に追加され、順番に処理されます。後からステートメントを追加または変更する場合は、ステートメントの `-index`設定を変更して処理順序を変更できます。

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ONTAP S3アクセス用の外部ディレクトリサービスを設定する

ONTAP 9.14.1以降では、外部ディレクトリのサービスがONTAP S3オブジェクト ストレージに統合されています。この統合により、外部ディレクトリ サービスによるユーザとアクセスの管理が簡単になります。

外部ディレクトリサービスに属するユーザーグループに、ONTAPオブジェクトストレージ環境へのアクセス権限を付与できます。Lightweight Directory Access Protocol（LDAP）は、Active Directoryなどのディレクトリサービスと通信するためのインターフェースであり、IDおよびアクセス管理（IAM）用のデータベースとサービスを提供します。アクセス権限を付与するには、ONTAP S3環境でLDAPグループを設定する必要があります。アクセス権限を設定すると、グループメンバーにONTAP S3バケットへの権限が付与されます。LDAPの詳細については、"ONTAP NFS SVMでのLDAPネームサービスの使用について学習します"を参照してください。

また、Active Directoryユーザ グループを高速バインド モードに設定することで、ユーザ クレデンシャルを検証し、サードパーティおよびオープンソースのS3アプリケーションをLDAP接続を介して認証するようにもできます。

開始する前に

LDAPグループを設定し、グループ アクセスの高速バインド モードを有効にする場合は、事前に以下を確認してください。

1. S3サーバを含むS3対応Storage VMが作成されました。"S3用SVMの作成"を参照してください。
2. ストレージVMにバケットが作成されました。"バケットの作成"を参照してください。
3. ストレージVMにDNSが設定されています。"DNSサービスを設定する"を参照してください。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がストレージVMにインストールされています。"SVMに自己署名ルートCA証明書をインストールする"を参照してください。
5. LDAPクライアントは、SVM上でTLSを有効にして設定されています。"ONTAP NFSアクセス用のLDAPクライアント構成を作成する"および"LDAPクライアント設定をONTAP NFS SVMに関連付けて情報を取得する"を参照してください。

LDAPのS3アクセスを設定する

1. SVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAPコマンドリファレンスのhttps://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^]コマンドの詳細を参照してください。

2. アクセスを許可するLDAPグループに `principal`を設定したオブジェクトストアバケットポリシーステートメントを作成します：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

例：次の例では、 `buck1`のバケットポリシーステートメントを作成します。このポリシーは、LDAPグループ `group1`にリソース（バケットとそのオブジェクト） `buck1`へのアクセスを許可します。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. LDAPグループのユーザー `group1`がS3クライアントからS3操作を実行できることを確認します。

1. SVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

ONTAPコマンドリファレンスのhttps://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^]コマンドの詳細を参照してください。

2. S3バケットにアクセスするLDAPユーザーに、バケットポリシーで定義された権限が付与されていることを確認してください。詳細については、"バケット ポリシーの変更"をご覧ください。
3. LDAPグループのユーザが次の処理を実行できることを確認します。
   a. S3クライアントのアクセスキーを次の形式で設定します（ `"NTAPFASTBIND" + base64-encode(user-name:password)`例（ `"NTAPFASTBIND"+ base64-encode(ldapuser:password)、結果は次のようになります `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

> S3クライアントからシークレット キーの入力を求められることがあります。シークレット キーがない場合は、16文字以上のパスワードを入力できます。

   b. ユーザが権限を持っているS3クライアントから基本的なS3処理を実行します。

Base64認証情報

ONTAP S3のデフォルト設定では、HTTPは使用されず、HTTPSとトランスポート層セキュリティ（TLS）接続のみが使用されます。ONTAPは自己署名証明書を生成できますが、サードパーティの認証局（CA）が発行した証明書を使用することを推奨します。CA証明書を使用すると、クライアントアプリケーションとONTAPオブジェクトストアサーバの間に信頼関係が確立されます。

Base64を使用してエンコードされた認証情報は簡単にデコードされることに注意してください。HTTPSを使用すると、中間者攻撃によるパケットスニファーによるエンコードされた認証情報の傍受を防ぐことができます。

事前署名済みURLを作成する際は、認証にLDAPファストバインドモードを使用しないでください。認証は、事前署名済みURLに含まれるBase64アクセスキーのみに基づいて行われます。ユーザ名とパスワードは、Base64アクセスキーをデコードしたすべてのユーザに公開されます。

認証方法は**nsswitch**で**LDAP**が有効になっている例

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに転送します。ユーザが独自のキーを生成できるようにする場合は、curlを使用するためのHTTP権限をユーザのロールに追加する必要があります。この権限は、S3 API権限に追加されます。

Active Directoryまたは**SMB**サーバの**S3**アクセスを設定する

バケットポリシーステートメントで指定されたNASグループ、またはNASグループに属するユーザーにUIDとGIDが設定されていない場合、これらの属性が見つからないため検索は失敗します。Active DirectoryはUIDではなくSIDを使用します。SIDエントリをUIDにマッピングできない場合は、必要なデータをONTAPに取り込む必要があります。

これを行うには、"vserver active-directory create"を使用して、SVMがActive Directoryで認証し、必要なユーザおよびグループ情報を取得できるようにします。

または、"vserver cifs create"を使用して、Active Directoryドメインに SMB サーバを作成します。

ネームサーバーとオブジェクトストアで異なるドメイン名を使用している場合、検索エラーが発生する可能性があります。検索エラーを回避するには、NetAppではUPN形式のリソース認証に信頼できるドメインを使用することをお勧めします： `nasgroup/group@trusted_domain.com`信頼できるドメインとは、SMBサーバーの信頼済みドメインリストに追加されているドメインです。SMBサーバーリストで"優先する信頼済みドメインの追加、削除、変更"追加する方法については、こちらをご覧ください。

認証方法がドメインで、信頼されたドメインが **Active Directory** に構成されている場合にキーを生成します

UPN形式で指定されたユーザーで `s3/services/<svm_uuid>/users`エンドポイントを使用します。例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに転送します。ユーザが独自のキーを生成できるようにする場合は、curlを使用するためのHTTP権限をユーザのロールに追加する必要があります。この権限は、S3 API権限に追加されます。

認証方法がドメインで、信頼できるドメインがない場合にキーを生成する

このアクションは、LDAPが無効になっている場合、または非POSIXユーザがUIDとGIDを設定していない場合に可能です。例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

APIをSVMのデータLIFではなく、クラスタ管理LIFに誘導してください。ユーザーが独自のキーを生成できるようにするには、curlを使用するためのHTTP権限をロールに追加する必要があります。この権限は、S3 API権限に加えて付与されます。信頼できるドメインがない場合にのみ、ユーザー名にオプションのドメイン値（@fqdn）を追加する必要があります。

LDAPまたはドメインユーザーが独自の**ONTAP S3**アクセスキーを生成できるようにする

ONTAP 9.14.1以降では、ONTAP管理者がカスタム ロールを作成し、それをローカル グループ、ドメイン グループ、またはLightweight Directory Access Protocol（LDAP）グループに割り当てることができます。このようにすると、各グループに所属するユーザがS3クライアント アクセス用に自身のアクセス キーとシークレット キーを生成できるようになります。

カスタムロールを作成し、アクセスキー生成用のAPIを呼び出すユーザーに割り当てることができるように、ストレージVMでいくつかの設定手順を実行する必要があります。

LDAPが無効になっている場合は、"ONTAP S3アクセス用の外部ディレクトリサービスを設定する"ユーザーがアクセスキーを生成できるようにすることができます。

開始する前に

以下を確認してください。

1. S3サーバを含むS3対応Storage VMが作成されました。"S3用SVMの作成"を参照してください。
2. ストレージVMにバケットが作成されました。"バケットの作成"を参照してください。
3. ストレージVMにDNSが設定されています。"DNSサービスを設定する"を参照してください。
4. LDAPサーバの自己署名ルート認証局（CA）証明書がストレージVMにインストールされています。"SVMに自己署名ルートCA証明書をインストールする"を参照してください。
5. Storage VMでTLSが有効になっているLDAPクライアントが設定されています。"ONTAP NFSアクセス用のLDAPクライアント構成を作成する"を参照してください。
6. クライアント構成をVserverに関連付けます。"LDAPクライアント設定をONTAP NFS SVMに関連付ける"を参照してください。 `vserver services name-service ldap create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。
7. データストレージVMを使用している場合は、VM上に管理ネットワークインターフェース（LIF）と、LIFのサービスポリシーを作成します。 `network interface create`と `network interface service-policy create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

アクセス キー生成のためのユーザの設定

例 **3.** 手順

LDAPユーザ

1. ストレージVMのグループとパスワードの_ネームサービスデータベース_としてLDAPを指定します：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

`vserver services name-service ns-switch modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-services-name-service-ns-switch-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

2. S3ユーザREST APIエンドポイントへのアクセス権を持つカスタムロールを作成します：
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`この例では、 `s3-role`ロールがストレージVM `svm-1`上のユーザーに対して生成され、読み取り、作成、更新のすべてのアクセス権が付与されます。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

`security login rest-role create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-rest-role-create.html["ONTAPコマンド リファレンス"^]を参照してください。

3. `security login`コマンドを使用してLDAPユーザーグループを作成し、S3ユーザーREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。"ONTAPコマンド リファレンス"の `security login create`の詳細をご覧ください。

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

この例では、LDAPグループ `ldap-group-1`が `svm-1`に作成され、カスタムロール `s3role`がAPIエンドポイントにアクセスするために追加され、高速バインドモードでのLDAPアクセスが有効になります。

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

詳細については、"ONTAP NFS SVMのnsswitch認証にLDAP高速バインドを使用する"を参照してください。

`security login create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。

LDAPグループにカスタムロールを追加すると、そのグループ内のユーザーにONTAP `/api/protocols/s3/services/{svm.uuid}/users`エンドポイントへの限定的なアクセスが許可されます。APIを呼び出すことで、LDAPグループのユーザーはS3クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます。キーは自分自身のみ生成でき、他のユーザー用には生成できません。

ドメイン ユーザ

1. S3ユーザREST APIエンドポイントへのアクセス権を持つカスタム ロールを作成します。

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

この例では、 `s3-role`ロールがストレージVM `svm-1`上のユーザーに対して生成され、読み取り、作成、更新のすべてのアクセス権が付与されます。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

`security login rest-role create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-rest-role-create.html["ONTAPコマンド リファレンス
"^]を参照してください。

1. `security login`コマンドを使用してドメインユーザーグループを作成し、S3ユーザーREST APIエンドポイントにアクセスするための新しいカスタムロールを追加します。"ONTAPコマンド リファレンス"の `security login create`の詳細をご覧ください。

```
security login create -vserver <vserver-name> -user-or-group-name
domain\<group-name> -application http -authentication-method domain
-role <custom-role-name>
```

この例では、ドメイングループ `domain\group1`が `svm-1`に作成され、カスタムロール `s3role`がAPIエンドポイントにアクセスするためにそのグループに追加されます。

```
security login create -user-or-group-name domain\group1 -application
http -authentication-method domain -role s3role -vserver svm-1
```

`security login create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

ドメイングループにカスタムロールを追加すると、そのグループ内のユーザーに ONTAP /api/protocols/s3/services/{svm.uuid}/users エンドポイントへの限定的なアクセスが許可されます。API を呼び出すことで、ドメイングループのユーザーは S3 クライアントにアクセスするための独自のアクセスキーとシークレットキーを生成できます。キーは自分自身のみ生成でき、他のユーザー用には生成できません。

S3ユーザまたはLDAPユーザによる独自のアクセス キーの生成

ONTAP 9.14.1以降では、独自のキーを生成できるロールが割り当てられているユーザは、S3クライアントにアクセスするための独自のアクセス キーとシークレット キーを生成できます。次のONTAP REST APIエンドポイントを使用すると、自分専用のキーを生成できます。

S3ユーザを作成してキーを生成

このREST API呼び出しでは、以下のメソッドとエンドポイントを使用します。このエンドポイントの詳細については、リファレンス "APIのドキュメント"をご覧ください。

HTTPメソッド	パス
POST	/api/protocols/s3/services/{svm.uuid}/users

ドメインユーザーの場合は、S3ユーザー名に次の形式を使用します： user@fqdn。ここで、 `fqdn`はドメインの完全修飾ドメイン名です。

Curlの例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3ユーザのキーを再生成

S3ユーザーが既に存在する場合は、アクセスキーとシークレットキーを再生成できます。このREST API呼び出しでは、以下のメソッドとエンドポイントを使用します。

HTTPメソッド	パス
PATCH	/api/protocols/s3/services/{svm.uuid}/users/{name}

Curlの例

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON出力の例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

S3オブジェクト ストレージへのクライアント アクセスの有効化

リモートの**FabricPool**階層化用**ONTAP S3**アクセスの有効化

ONTAP S3をリモートのFabricPool大容量（クラウド）階層として使用するには、ONTAP S3管理者がリモートのONTAPクラスタ管理者にS3サーバの設定に関する情報を提供する必要があります。

タスク概要

FabricPoolクラウド階層を設定するには、次のS3サーバ情報が必要です。

- サーバ名（FQDN）
- バケット名
- CA証明書
- アクセス キー
- パスワード（シークレット アクセス キー）

さらに、次のネットワーク設定が必要です。

- 管理SVMに設定されたDNSサーバに、リモートのONTAP S3サーバのホスト名に関するエントリとしてS3サーバのFQDN名とサーバ上の各LIFのIPアドレスが必要です。
- ローカル クラスタにクラスタ間LIFを設定する必要があります。ただしクラスタのピアリングは必要ありません。

ONTAP S3をクラウド階層として設定する方法については、FabricPoolのドキュメントを参照してください。

"FabricPoolを使用したストレージ階層の管理"

ローカルの**FabricPool**階層化用の**ONTAP S3**アクセスの有効化

ONTAP S3をローカルのFabricPool大容量階層として使用するには、作成したバケットに基づいてオブジェクト ストアを定義し、そのオブジェクト ストアを高パフォーマンス階層のアグリゲートに接続してFabricPoolを作成する必要があります。

開始する前に

ONTAP S3サーバー名とバケット名が必要であり、S3サーバーはクラスタLIF（ `-vserver Cluster`パラメータ付き）を使用して作成されている必要があります。

タスク概要

オブジェクト ストアの設定には、S3サーバとバケットの名前や認証要件など、ローカルの大容量階層に関する情報が保存されます。

作成したオブジェクト ストア設定を、別のオブジェクト ストアやバケットに関連付けないでください。ローカル階層用に複数のバケットを作成できますが、1つのバケットに複数のオブジェクト ストアを作成することはできません。

ローカルの大容量階層にはFabricPoolライセンスは必要ありません。

手順

1. ローカルの大容量階層用のオブジェクト ストアを作成します。

```
storage aggregate object-store config create -object-store-name store_name
-ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

   - `-container-name`は、作成したS3バケットです。
   - この `-access-key`パラメータは ONTAP S3 サーバへの要求を承認します。
   - `-secret-password`パラメータ（シークレットアクセスキー）は、ONTAP S3サーバへのリクエストを認証します。
   - `-is-certificate-validation-enabled`パラメータを `false`に設定すると、ONTAP S3の証明書チェックを無効にすることができます。

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipspace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. オブジェクト ストアの設定情報を表示して確認します。

   `storage aggregate object-store config show`

3. オプション："Inactive Data Reportingによるボリューム内のアクセス頻度の低いデータ量の確認"。

   ボリューム内のアクセス頻度の低いデータの量を確認すると、どのアグリゲートをFabricPoolのローカル階層化に使用するかを決定するのに役立ちます。

4. オブジェクト ストアをアグリゲートに接続します。

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   `allow-flexgroup *true*`オプションを使用して、FlexGroupボリューム構成要素を含むアグリゲートをアタッチできます。

```
cluster1::> storage aggregate object-store attach
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. オブジェクト ストアの情報を表示し、接続したオブジェクト ストアが使用可能になっていることを確認します。

   `storage aggregate object-store show`

```
cluster1::> storage aggregate object-store show

Aggregate    Object Store Name    Availability State
---------    -----------------    ------------------
aggr1        MyLocalObjStore      available
```

関連情報

- "storage aggregate object-store attach"
- "storage aggregate object-store config create"
- "storage aggregate object-store config show"
- "storage aggregate object-store show"

S3クライアント アプリケーションからONTAP S3サーバにアクセスするには、ONTAP S3管理者がS3ユーザに設定情報を提供する必要があります。

開始する前に

S3クライアント アプリケーションは、ONTAP S3サーバとの認証にAWSの次のバージョンの署名を使用する必要があります。

- 署名バージョン4、ONTAP 9.8以降
- 署名バージョン2、ONTAP 9.11.1以降

これ以外の署名バージョンはONTAP S3ではサポートされません。

ONTAP S3管理者がS3ユーザを作成し、バケット ポリシーまたはオブジェクト ストレージ サーバ ポリシーで個々のユーザまたはグループ メンバーとしてアクセス権限を付与しておく必要があります。

S3クライアント アプリケーションがONTAP S3サーバ名を解決できるように、ONTAP S3管理者がS3サーバのサーバ名（FQDN）とLIFのIPアドレスを提供する必要があります。

タスク概要

ONTAP S3バケットにアクセスするには、S3クライアント アプリケーションのユーザがONTAP S3管理者から受け取った情報を入力します。

ONTAP 9.9.1以降では、ONTAP S3サーバで次のAWSクライアント機能がサポートされます。

- ユーザ定義のオブジェクト メタデータ

  PUT（またはPOST）を使用してオブジェクトを作成するときに、一連のキーと値のペアをメタデータとして割り当てることができます。オブジェクトに対してGET / HEAD処理が実行されると、システムのメタデータとともにユーザ定義のメタデータが返されます。

- オブジェクトのタグ付け

  オブジェクトの分類用に、キーと値のペアをタグとして割り当てることができます。メタデータとは異なり、タグはオブジェクトの作成とは別にREST APIを使用して作成および読み取られ、オブジェクトの作成時または作成後の任意の時点で実装されます。

> クライアントがタグ付け情報を取得および配置できるようにするには、`GetObjectTagging`、 `PutObjectTagging`、および `DeleteObjectTagging`のアクションをバケットまたはグループポリシーを使用して許可する必要があります。

詳細については、AWS S3のドキュメントを参照してください。

手順

1. S3サーバ名とCA証明書を入力して、S3クライアント アプリケーションをONTAP S3サーバで認証します。
2. 次の情報を入力して、S3クライアント アプリケーションのユーザを認証します。
   - S3サーバ名（FQDN）とバケット名

- ユーザのアクセス キーとシークレット キー

ONTAP S3 ストレージサービスレベル

ONTAPには、対応する最小パフォーマンス要因にマッピングされた定義済みのストレージサービスが含まれています。

クラスタまたは SVM で使用できる実際のストレージサービスのセットは、SVM 内のアグリゲートを構成するストレージのタイプによって決まります。

次の表は、最小パフォーマンス係数が定義済みストレージサービスにどのようにマッピングされるかを示しています：

ストレージサービス	予想**IOPS**（**SLA**）	ピーク**IOPS**（**SLO**）	最小ボリューム**IOPS**	推定レイテンシ	予想される **IOPS** は強制されますか？
価値	128/TB	512/TB	75	17ms	AFF：はい それ以外の場合：いいえ
パフォーマンス	2048/TB	4096/TB	500	2ms	はい
Extreme	6144/TB	12288/TB	1000	1ms	はい

次の表は、メディアまたはノードの種類ごとに利用可能なストレージ サービス レベルを定義しています：

メディアまたはノード	利用可能なストレージ サービス レベル
ディスク	価値
仮想マシン ディスク	価値
ハイブリッド	価値
容量最適化 Flash	価値
ソリッドステートドライブ（SSD）- 非AFF	価値
パフォーマンス最適化フラッシュ - SSD（AFF）	Extreme、Performance、Value

ONTAP S3バケットのクロスオリジンリソース共有（CORS）を設定する

ONTAP 9.16.1以降では、クライアントWebアプリケーションが複数のドメインからONTAPバケットにアクセスできるように、Cross-Origin Resource Sharing（CORS）

を設定できます。これにより、Webブラウザを使用したバケット オブジェクトへのセキュアなアクセスが実現されます。

CORSはHTTPを基盤としたフレームワークで、あるWebページで定義されたスクリプトが別のドメインのサーバ上のリソースにアクセスできるようにします。このフレームワークは、Webセキュリティの初期の基盤である_同一生成元ポリシー_を安全に回避するために使用されます。主要な概念と用語については以下で説明します。

キャッシュ元

オリジンによって、リソースの場所とIDが正確に定義されます。以下の値の組み合わせで表されます。

- URIスキーム（プロトコル）
- ホスト名（ドメイン名またはIPアドレス）
- ポート番号

以下はオリジンの簡単な例です： `https://www.mycompany.com:8001`。オリジンを CORS で使用すると、リクエスト元のクライアントが識別されます。

同一オリジン ポリシー

同一オリジン ポリシー（SOP）は、ブラウザ ベースのスクリプトに適用されるセキュリティ上の概念と制限です。このポリシーにより、あるWebページから最初に読み込まれたスクリプトが、別のページのデータにアクセスできるようになります。ただし、両方のページが同じオリジンにあることが条件になります。この制限により、悪意のあるスクリプトが別のオリジンにあるページのデータにアクセスするのを防げます。

CORSの一般的なユースケース

CORSには、一般的なユースケースがいくつかあります。ほとんどのケースで、AJAXリクエスト、フォント / スタイルシート / スクリプトの読み込み、クロスドメイン認証など、明確に定義されたクロス ドメイン アクセスのインスタンスが関係します。CORSは、シングルページ アプリケーション（SPA）の一部として実装することもできます。

HTTPヘッダー

CORSは、HTTPリクエストとレスポンスに挿入されるヘッダーを使用して実装されます。例えば、アクセス制御を実装し、メソッドやヘッダーを含む許可される操作を示すレスポンスヘッダーがいくつかあります。HTTPリクエストに_Origin_ヘッダーが存在する場合、そのリクエストはクロスドメインリクエストとして定義されます。origin値は、CORSサーバーが有効なCORS設定を見つけるために使用されます。

HTTPプリフライト要求

これは、特定のメソッドやヘッダーなど、サーバがCORSをサポートしているかどうかを最初に確認するために使用されるオプションの要求です。応答に基づいて、CORS要求を完了できるかどうかが決まります。

ONTAPバケット

バケットは、明確に定義されたネームスペースに基づいて格納、アクセスされるオブジェクトのコンテナです。以下の2種類のONTAPバケットがあります。

- NASバケット：NASプロトコルとS3プロトコルでアクセス可能
- S3バケット：S3プロトコルでのみアクセス可能

ONTAPでのCORSの実装

ONTAP 9.16.1以降のリリースでは、CORSがデフォルトで有効になっています。CORSは、アクティブにするSVMごとに設定する必要があります。

> ONTAPクラスタでCORSを無効にする管理オプションはありません。ただし、ルールを定義しないか、既存のルールをすべて削除することで、CORSを実質的に無効にできます。

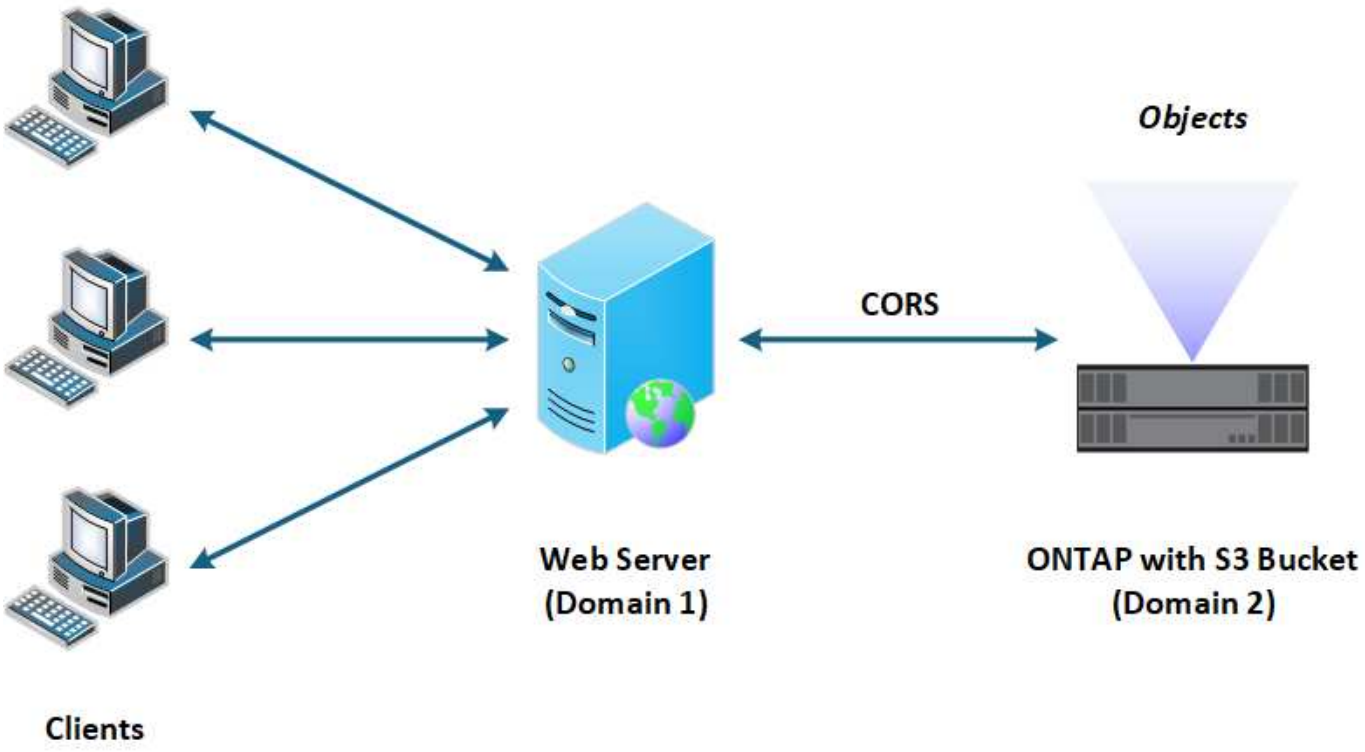
想定されるユースケース

ONTAP CORSの実装では、クロス ドメイン リソース アクセスのために、以下のようないくつかのトポロジが有効になります。

- ONTAP S3バケット（同一または異なるSVMまたはクラスタ内）
- ONTAP NASバケット（同一または異なるSVMまたはクラスタ内）
- ONTAP S3バケットとNASバケット（同一または異なるSVMまたはクラスタ内）
- ONTAPバケットと外部ベンダー バケット
- 異なるタイムゾーンのバケット

概要図

下の図は、CORSによってONTAP S3バケットへのアクセスが可能になる仕組みを示しています。



CORSルールの定義

機能をアクティブ化して使用するには、ONTAPでCORSルールを定義する必要があります。

設定の操作

ONTAPでは、以下の3つの基本的なルール設定の操作がサポートされています。

- 表示
- 作成
- 削除

ONTAPで定義されるCORSルールには、SVMとバケットや、許可されるオリジン、メソッド、ヘッダーなど、いくつかのプロパティがあります。

管理オプション

ONTAPクラスタでのCORSの管理には、いくつかのオプションがあります。

ONTAPコマンドライン インターフェイス

CORSはコマンドラインインターフェイスを使用して設定できます。詳細については、CLIを使用したCORSの管理を参照してください。

ONTAP REST API

ONTAP REST APIを使用してCORSを設定できます。CORS機能をサポートする新しいエンドポイントは追加されていません。代わりに、以下の既存のエンドポイントを使用できます。

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

詳細については、 "ONTAP自動化ドキュメント"をご覧ください。

S3 API

S3 APIを使用してONTAPバケットでのCORSの設定を作成、削除できます。S3クライアント管理者には、以下のことに関する十分な権限が必要です。

- アクセス キーまたはシークレット キーのクレデンシャル
- s3api経由のアクセスを許可するようにバケットに設定されたポリシー

アップグレードとリバート

CORSを使用してONTAP S3バケットにアクセスする予定がある場合は、いくつかの管理上の問題に注意する必要があります。

アップグレード

CORS機能は、すべてのノードが9.16.1にアップグレードされている場合にサポートされます。混在モードのクラスタでは、有効なクラスタ バージョン（ECV）が9.16.1以降の場合にのみ、CORS機能を使用できます。

リバート

ユーザ側の観点では、クラスタのリバートを続行する前に、すべてのCORS設定を削除する必要があります。内部的には、処理により、すべてのCORSデータベースが削除されます。これらのデータ構造をクリアしてリバートするコマンドの実行を求めるメッセージが表示されます。

CLIを使用したCORSの管理

ONTAP CLIを使用してCORSルールを管理できます。主な操作については以下で説明します。CORSコマンドを実行するには、ONTAPの*admin*権限レベルが必要です。

作成

CORSルールは `vserver object-store-server bucket cors-rule create`コマンドを使って定義できます。 `vserver object-store-server bucket cors-rule create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

パラメータ

ルールの作成に使用するパラメータを以下にまとめています。

パラメータ	概要
`vserver`	ルールが作成されるオブジェクトストアサーババケットをホストするSVM（vserver）の名前を指定します。

パラメータ	概要
bucket	ルールが作成されるオブジェクトストアサーバーのバケットの名前。
index	ルールが作成されるオブジェクトストアサーババケットのインデックスを示すオプションのパラメータ。
rule id	オブジェクトストアサーバーバケットルールの一意の識別子。
allowed-origins	クロスオリジンリクエストの発信が許可されるオリジンのリスト。
allowed-methods	クロスオリジンリクエストで許可されるHTTPメソッドのリスト。
allowed-headers	クロスオリジンリクエストで許可されるHTTPヘッダーのリスト。
expose-headers	顧客がアプリケーションからアクセスできるCORS応答で送信される追加ヘッダーのリスト。
max-age-in-seconds	ブラウザが特定のリソースのプリフライト応答をキャッシュする時間を指定するオプションパラメータ。

例

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

表示

コマンド `vserver object-store-server bucket cors-rule show`を使用すると、現在のルールとその内容のリストを表示できます。"ONTAPコマンド リファレンス"の `vserver object-store-server bucket cors-rule show`の詳細をご覧ください。

パラメータ `-instance`を含めると、各ルールに表示されるデータが拡張されます。必要なフィールドを指定することもできます。

例

```
server object-store-server bucket cors-rule show -instance
```

削除

CORSルールのインスタンスを削除するには、deleteコマンドを使用します。ルールの `index`値が必要なので、この操作は2つのステップで実行されます：

1. `show`コマンドを発行してルールを表示し、そのインデックスを取得します。

2. インデックス値を使用してdeleteコマンドを実行します。

例

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

変更

既存のCORSルールを変更するCLIコマンドはありません。ルールを変更するには、以下の手順を実行する必要があります。

1. 既存のルールを削除します。
2. 必要なオプションを指定して新しいルールを作成します。

SnapMirror S3によるバケットの保護

ONTAP SnapMirror S3について学ぶ

ONTAP 9.10.1以降では、SnapMirrorのミラーリングとバックアップの機能を使用してONTAP S3オブジェクト ストアのバケットを保護できます。標準のSnapMirrorとは異なり、SnapMirror S3を使うと、AWS S3などのNetApp以外のデスティネーションへのミラーリングとバックアップができます。

SnapMirror S3では、ONTAP S3バケットから次のデスティネーションへのアクティブなミラーとバックアップをサポートしています。

ターゲット	アクティブなミラーとテイクオーバーのサポート	バックアップとリストアのサポート
ONTAP S3 • 同じSVM内のバケット • 同じクラスタ内の別のSVM内のバケット • 別のクラスタ内のSVM内のバケット	はい	はい
StorageGRID	いいえ	はい
AWS S3	いいえ	はい
Cloud Volumes ONTAP for Azure	はい	はい
Cloud Volumes ONTAP for AWS	はい	はい
Cloud Volumes ONTAP for Google Cloud	はい	はい

ONTAP S3サーバ上の既存のバケットを保護することも、新しく作成したバケットですぐにデータ保護を有効にすることもできます。

SnapMirror S3の要件

- ONTAPのバージョン

  ソースとデスティネーションのクラスタでONTAP 9.10.1以降が実行されている必要があります。

  SnapMirror S3はMetroCluster構成ではサポートされていません。

- ライセンス

  "ONTAP One"ソフトウェア スイートで利用可能な次のライセンスは、ONTAPソース システムとデスティネーション システムで次の項目へのアクセスを提供するために必要です：

  - ONTAP S3プロトコルおよびストレージ
  - SnapMirror S3：NetAppの他のオブジェクト ストア（ONTAP S3、StorageGRID、Cloud Volumes ONTAP）をターゲットにするため
  - SnapMirror S3からAWS S3（"ONTAP One互換性バンドル"で利用可能）を含むサードパーティのオブジェクト ストアへ
  - クラスタでONTAP 9.10.1を実行している場合は、"FabricPoolライセンス"が必要です。

- ONTAP S3
  - ソースとデスティネーションのSVMでONTAP S3サーバが実行されている必要があります。
  - TLSアクセス用のCA証明書はS3サーバをホストするシステムにインストールすることを推奨しますが、必須ではありません。
    - S3サーバの証明書への署名に使用されたCA証明書を、S3サーバをホストするクラスタの管理Storage VMにインストールする必要があります。
    - 自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。
    - ソースまたはデスティネーションのStorage VMがHTTPSをリスンしていない場合、CA証明書をインストールする必要はありません。
- ピアリング（ONTAP S3ターゲットの場合）
  - クラスタ間LIFが設定されている必要があります（リモートのONTAPターゲットの場合）。ソース クラスタとデスティネーション クラスタのクラスタ間LIFは、ソースとデスティネーションのS3サーバのデータLIFに接続できます。
  - ソースとデスティネーションのクラスタがピアリングされている必要があります（リモートのONTAPターゲットの場合）。
  - ソースとデスティネーションのStorage VMがピアリングされている必要があります（すべてのONTAPターゲットで必須）。
- SnapMirrorポリシー
  - すべてのSnapMirror S3関係にS3固有のSnapMirrorポリシーが必要ですが、複数の関係に同じポリシーを使用することができます。
  - 独自のポリシーを作成することも、次の値を含むデフォルトの **Continuous** ポリシーを受け入れることもできます：
    - スロットル（スループット / 帯域幅の上限）：無制限。
    - 回復ポイント目標の時間：1時間（3600秒）。

2つのS3バケットがSnapMirror関係にある場合、現バージョンのオブジェクトの有効期限を定めた（削除するための）ライフサイクル ポリシーが存在すると、パートナー バケットにも同様の処理がレプリケートされることに注意してください。これは、パートナー バケットが読み取り専用またはパッシブである場合も同様です。

- ルート ユーザ キー Storage VMルート ユーザ アクセス キーはSnapMirror S3関係に必要です。ONTAPではデフォルトで割り当てられません。SnapMirror S3関係を初めて作成する際は、ソースとデスティネーションの両方のStorage VMにキーが存在することを確認し、存在しない場合は再生成する必要があります。再生成が必要な場合は、アクセス キーとシークレット キーのペアを使用しているすべてのクライアントとすべてのSnapMirrorオブジェクト ストア設定が新しいキーで更新されていることを確認する必要があります。

S3サーバの設定については、次のトピックを参照してください。

- "Storage VMでのS3サーバの有効化"
- "ONTAP S3の設定プロセスについて"

クラスタおよびStorage VMのピアリングについては、次のトピックを参照してください。

- "Prepare for mirroring and vaulting（System Manager、手順1～6）"
- "Cluster and SVM peering（CLI）"

サポートされる**SnapMirror**関係

SnapMirror S3はファンアウトとカスケード関係をサポートしています。概要については、"ファンアウト構成およびカスケード構成のデータ保護"をご覧ください。

SnapMirror S3では、ファンイン構成（複数のソース バケットと1つのデスティネーション バケットの間のデータ保護関係）はサポートされません。SnapMirror S3では、複数のクラスタから単一のセカンダリ クラスタへの複数のバケットのミラーはサポートされますが、各ソース バケットに対応する独自のデスティネーション バケットがセカンダリ クラスタに必要です。

SnapMirror S3はMetroCluster環境ではサポートされていません。

S3バケットへのアクセスの制御

新しいバケットを作成する際、ユーザとグループを作成してアクセスを制御できます。

SnapMirror S3 はソース バケットからデスティネーション バケットにオブジェクトを複製しますが、ソース オブジェクト ストアからデスティネーション オブジェクト ストアにユーザー、グループ、およびポリシーを複製しません。

フェイルオーバー イベント中にクライアントがデスティネーション バケットにアクセスできるように、ユーザー、グループ ポリシー、権限、および同様のコンポーネントをデスティネーション オブジェクト ストアで構成する必要があります。

移行元ユーザーと移行先ユーザーは、デスティネーション クラスタでユーザーが作成されるときに移行元キーが手動で提供される場合、同じアクセス キーとシークレット キーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

詳細については、次のトピックを参照してください。

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"

S3 オブジェクトロックと**SnapMirror S3**によるバージョン管理を使用する

オブジェクト ロックとバージョン管理が有効になっているONTAPバケットでSnapMirror S3を使用できますが、いくつかの考慮事項があります：

- Object Lockが有効になっているソースバケットをレプリケートするには、デスティネーションバケットでもObject Lockが有効になっている必要があります。さらに、ソースとデスティネーションの両方でバージョン管理が有効になっている必要があります。これにより、両方のバケットのデフォルトの保持ポリシーが異なる場合に、削除がデスティネーションバケットにミラーリングされる問題を回避できます。
- S3 SnapMirrorはオブジェクトの過去のバージョンをレプリケートしません。オブジェクトの現在のバージョンのみがレプリケートされます。

オブジェクトロックされたオブジェクトが宛先バケットにミラーリングされると、元の保持期間が維持されます。ロックされていないオブジェクトが複製された場合は、宛先バケットのデフォルトの保持期間が適用されます。例：

- バケットAのデフォルトの保持期間は30日間、バケットBのデフォルトの保持期間は60日間です。バケットAからバケットBに複製されたオブジェクトは、バケットBのデフォルトの保持期間よりも短いにもかかわらず、30日間の保持期間を維持します。
- バケットAにはデフォルトの保持期間がなく、バケットBにはデフォルトの保持期間が60日間あります。ロック解除されたオブジェクトがバケットAからバケットBに複製されると、60日間の保持期間が適用されます。バケットAでオブジェクトが手動でロックされた場合、バケットBに複製される際に元の保持期間が維持されます。
- バケットAのデフォルトの保持期間は30日間ですが、バケットBにはデフォルトの保持期間がありません。バケットAからバケットBに複製されたオブジェクトは、30日間の保持期間を維持します。

リモート クラスタでのミラーとバックアップによる保護

リモート クラスタ上の新しい**ONTAP S3**バケットのミラー関係を作成します

新しい S3 バケットを作成すると、リモート クラスター上の SnapMirror S3 デスティネーションにすぐに保護できます。

タスク概要

このタスクはソースとデスティネーションの両方のシステムで実行する必要があります。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。

- ソースとデスティネーションのクラスタ間にピア関係が、ソースとデスティネーションのStorage VM間にピア関係がそれぞれ確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
   b. *設定*タブで、*S3*タイルの をクリックします。
   c. *ユーザー*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. 存在しない場合は、*root*の横にあるをクリックし、*キーの再生成*をクリックします。既にキーが存在する場合は、再生成しないでください。
2. ソースとデスティネーションの両方のStorage VMで、Storage VMを編集してユーザを追加し、グループにユーザを追加します。

   ストレージ > ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. ソースクラスタで、既存のものがなくデフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. *Protection > Overview*をクリックし、*Local Policy Settings*をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. SnapMirror保護を適用してバケットを作成します。
   a. *ストレージ > バケット*をクリックし、*追加*をクリックします。権限の確認は任意ですが、推奨されます。
   b. 名前を入力し、ストレージ VM を選択し、サイズを入力して、*その他のオプション*をクリックします。
   c. *権限*で*追加*をクリックします。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - デフォルト値 `(*bucketname, bucketname*/*)`または必要なその他の値を使用します。

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してく

ください。

d. *保護*で、*SnapMirrorを有効にする（ONTAPまたはCloud）*にチェックを入れます。次に、以下の値を入力します：

- デスティネーション
  - ターゲット：**ONTAP**システム
  - **CLUSTER**：リモート クラスターを選択します。
  - **STORAGE VM**：リモートクラスタ上のストレージVMを選択します。
  - **S3 SERVER CA CERTIFICATE**：*source* 証明書の内容をコピーして貼り付けます。
- ソース
  - **S3** サーバー **CA** 証明書： デスティネーション 証明書の内容をコピーして貼り付けます。

5. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
6. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
7. *保存*をクリックします。ソースストレージVMに新しいバケットが作成され、デスティネーションストレージVMに作成された新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. このSVMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のSVMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。

   ```
   vserver object-store-server user show
   ```

   rootユーザのアクセス キーがあることを確認します。キーがない場合は次のように入力します。

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   キーがすでにある場合は再生成しないでください。

2. ソースとデスティネーションの両方のSVMにバケットを作成します。

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーにアクセス ルールを追加します。

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   例

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. ソースSVMで、既存のものがなくデフォルトのポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成します：
   ```
   snapmirror policy create -vserver svm_name -policy policy_name -type
   continuous [-rpo integer] [-throttle throttle_type] [-comment text]
   [additional_options]
   ```

   パラメータ：

   - type `continuous` - SnapMirror S3関係の唯一のポリシー タイプ（必須）。
   - `-rpo` - 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` - スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. ソースとデスティネーションのクラスタの管理SVMに、CAサーバ証明書をインストールします。

   a. ソース クラスタで、デスティネーション S3サーバ証明書に署名したCA証明書をインストールします：
      ```
      security certificate install -type server-ca -vserver src_admin_svm
      -cert-name dest_server_certificate
      ```

   b. デスティネーション クラスタに、ソース S3 サーバー証明書に署名した CA 証明書をインストールします：
      ```
      security certificate install -type server-ca -vserver dest_admin_svm
      -cert-name src_server_certificate
      ```

外部CAベンダーが署名した証明書を使用する場合は、ソースとデスティネーションの管理SVMに同じ証明書をインストールします。

`security certificate install`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"^]をご覧ください。

6. ソース SVM で、SnapMirror S3 関係を作成します：

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

   例

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
   test-policy
   ```

7. ミラーリングがアクティブであることを確認します：
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

リモート クラスタ上の既存の **ONTAP S3** バケットのミラー関係を作成します

既存のS3バケットの保護は、たとえばONTAP 9.10.1よりも前のリリースからS3の設定をアップグレードした場合など、いつでも開始できます。

タスク概要

このタスクはソースとデスティネーションの両方のクラスタで実行する必要があります。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。
- ソースとデスティネーションのクラスタ間にピア関係が、ソースとデスティネーションのStorage VM間にピア関係がそれぞれ確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

手順

ミラー関係は、System ManagerまたはONTAP CLIを使用して作成できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. *ストレージ > ストレージVM*を選択し、ストレージVMを選択します。
   b. *設定*タブで、*S3*タイルの をクリックします。
   c. *ユーザー*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. ない場合は、**root** の横にある をクリックし、*キーの再生成*をクリックします。すでにキーが存在する場合は、キーを再生成しないでください。
2. 既存のユーザーとグループがソースとターゲットの両方のストレージVMに存在し、適切なアクセス権を持っていることを確認します。*ストレージ > ストレージVM*を選択し、ストレージVMを選択して*設定*タブを開きます。最後に*S3*タイルを見つけて を選択し、*ユーザー*タブ、*グループ*タブの順に選択して、ユーザーとグループのアクセス設定を表示します。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. ソースクラスタで、既存のものがなくデフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. *Protection > Overview*を選択し、*Local Policy Settings*をクリックします。
   b. *保護ポリシー*の横にある を選択し、*追加*をクリックします。
   c. ポリシーの名前と説明を入力します。
   d. ポリシーの対象として、クラスタとSVMのいずれかを選択します。
   e. SnapMirror S3 関係には 継続 を選択します。
   f. *Throttle*と*Recovery Point Objective*の値を入力します。
4. 既存のバケットのバケット アクセス ポリシーが引き続き要件を満たしていることを確認します。
   a. **Storage > Buckets** をクリックし、保護するバケットを選択します。
   b. *権限*タブで、 *編集*をクリックし、*権限*の下の*追加*をクリックします。
      - **Principal** と **Effect**：ユーザーグループの設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions**:次の値が表示されていることを確認します:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources**:デフォルト値 `(*bucketname, bucketname*/*)`または必要なその他の値を使用します。

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。
5. SnapMirror S3保護を使用して既存のバケットを保護します。
   a. ストレージ > バケット をクリックし、保護するバケットを選択します。

b. *Protect*をクリックし、次の値を入力します：

- デスティネーション
  - **TARGET**：ONTAPシステム
  - **CLUSTER**：リモート クラスターを選択します。
  - **STORAGE VM**：リモートクラスタ上のストレージVMを選択します。
  - **S3 SERVER CA CERTIFICATE**：*source* 証明書の内容をコピーして貼り付けます。
- ソース
  - **S3 SERVER CA CERTIFICATE**：_宛先_証明書の内容をコピーして貼り付けます。

6. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
7. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
8. *保存*をクリックします。既存のバケットが、宛先ストレージVMの新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. このSVMに対する最初のSnapMirror S3関係の場合、ソースSVMとデスティネーションSVMの両方にルートユーザーキーが存在することを確認し、存在しない場合は再生成してください：
   `vserver object-store-server user show` + ルートユーザーのアクセスキーが存在することを確認してください。存在しない場合は、以下を入力してください：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + キーが既に存在する場合は再生成しないでください。
2. デスティネーションSVMにミラー ターゲットにするバケットを作成します。

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーのアクセス ルールが正しいことを確認します。

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   ```

`-principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

例

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. ソースSVMで、既存のものがなくデフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous` – SnapMirror S3 関係の唯一のポリシータイプ（必須）。
   - `-rpo` – 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. ソースとデスティネーションのクラスタの管理SVMに、CA証明書をインストールします。

   a. ソース クラスタで、デスティネーション S3サーバ証明書に署名したCA証明書をインストールします：
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. デスティネーション クラスタに、ソース S3サーバ証明書に署名したCA証明書をインストールします：
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` + 外部CAベンダーによって署名された証明書を使用している場合は、ソースおよびデスティネーションの管理SVMに同じ証明書をインストールします。

   `security certificate install`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"^]をご覧ください。

6. ソース SVM で、SnapMirror S3 関係を作成します：

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

   例

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. ミラーリングがアクティブであることを確認します：
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

リモート クラスタ上のデスティネーション **ONTAP S3** バケットから引き継ぎます

ソース バケットのデータを使用できなくなった場合は、SnapMirror関係を解除してデスティネーション バケットを書き込み可能にし、データの提供を開始できます。

タスク概要

テイクオーバー処理が実行されると、ソース バケットが読み取り専用に変換され、元のデスティネーション バケットが読み取り / 書き込みに変換されて、SnapMirror S3関係が反転します。

無効になったソース バケットが再び使用できるようになると、SnapMirror S3は2つのバケットの内容を自動的に再同期します。Volume SnapMirrorの構成と違って、関係を明示的に再同期する必要はありません。

テイクオーバー処理はリモート クラスタから開始する必要があります。

SnapMirror S3 はソース バケットからデスティネーション バケットにオブジェクトを複製しますが、ソース オブジェクト ストアからデスティネーション オブジェクト ストアにユーザー、グループ、およびポリシーを複製しません。

フェイルオーバー イベント中にクライアントがデスティネーション バケットにアクセスできるように、ユーザー、グループ ポリシー、権限、および同様のコンポーネントをデスティネーション オブジェクト ストアで構成する必要があります。

移行元ユーザーと移行先ユーザーは、デスティネーション クラスタでユーザーが作成されるときに移行元キーが手動で提供される場合、同じアクセス キーとシークレット キーを使用できます。例：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

System Manager

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. *保護 > 関係*をクリックし、*SnapMirror S3*を選択します。
2. をクリックし、*フェイルオーバー*を選択して、*フェイルオーバー*をクリックします。

CLI

1. デスティネーション バケットのフェイルオーバー処理を開始します。
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー操作のステータスを確認します：
   `snapmirror show -fields status`

   例

   ```
   dest_cluster::> snapmirror failover start -destination-path
   dest_svm1:/bucket/test-bucket-mirror
   ```

関連情報

- "S3のユーザとグループの追加（System Manager）"
- "S3ユーザの作成（CLI）"
- "S3グループの作成と変更（CLI）"
- "SnapMirrorフェイルオーバーの開始"
- "snapmirror show"

リモート クラスタのデスティネーション **SVM** から **ONTAP S3** バケットをリストアする

ソース バケットのデータがなくなったり破損したりした場合、デスティネーション バケットからオブジェクトをリストアしてデータを再度取り込むことができます。

タスク概要

デスティネーション バケットは既存のバケットにも新しいバケットにもリストアできます。リストア処理のターゲット バケットには、デスティネーション バケットの使用済み論理スペースよりも多くのスペースが必要です。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はリモート クラスタから開始する必要があります。

System Manager

バックアップ データをリストアします。

1. *保護 > 関係*をクリックし、*SnapMirror S3*を選択します。
2. をクリックし、*復元*を選択します。
3. ソース*で、*既存のバケット（デフォルト）または*新しいバケット*を選択します。
   - 既存のバケット（デフォルト）に復元するには、次の操作を実行します：
     - 既存のバケットを検索するクラスタとStorage VMを選択します。
     - 既存のバケットを選択します。
     - デスティネーション S3 サーバー CA 証明書の内容をコピーして貼り付けます。
   - *新しいバケット*に復元するには、次の値を入力します：
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンス サービス レベル。詳細については、"ストレージ サービス レベル"を参照してください。
     - デスティネーション S3 サーバー CA 証明書の内容。
4. *Destination*の下に、*source* S3サーバーCA証明書の内容をコピーして貼り付けます。
5. 復元の進行状況を監視するには、*保護 > 関係*をクリックします。

ロックされたバケットのリストア

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックされたバケットをデスティネーションとして選択できます。

- 新しいバケットへの復元：オブジェクトロックが有効になっている場合、オブジェクトロックが有効になっているバケットを作成することで、バケットを復元できます。ロックされたバケットを復元すると、元のバケットのオブジェクトロックモードと保持期間が複製されます。新しいバケットに異なるロック保持期間を定義することもできます。この保持期間は、他のソースのロックされていないオブジェクトに適用されます。
- 既存のバケットへの復元：オブジェクトロックされたバケットは、既存のバケットでバージョニングと同様のオブジェクトロックモードが有効になっている限り、既存のバケットに復元できます。元のバケットの保持期間は維持されます。
- ロックされていないバケットの復元：バケットでオブジェクトロックが有効になっていない場合でも、ソース クラスタ上のオブジェクトロックが有効になっているバケットに復元できます。バケットを復元すると、ロックされていないすべてのオブジェクトがロックされ、デスティネーション バケットの保持モードと保有期間が適用されます。

CLI

1. 復元用の新しいデスティネーション バケットを作成します。詳細については、"新しいONTAP S3バケットのクラウドバックアップ関係を作成する"を参照してください。
2. デスティネーション バケットのリストア処理を開始します。
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

例

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

`snapmirror restore`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-restore.html["ONTAPコマンド リファレンス"^]を参照してください。

ローカル クラスタでのミラーとバックアップによる保護

ローカルクラスタ上の新しい **ONTAP S3** バケットのミラー関係を作成する

新しいS3バケットを作成すると、同じクラスター内のSnapMirror S3宛先にすぐに保護できます。データのミラーリングは、ソースと同じストレージVMまたは別のストレージVM内のバケットに行うことができます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。
- ソースとデスティネーションのStorage VM間にピア関係が確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
   b. *設定*タブで、S3 タイルの をクリックします。
   c. *Users*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. 存在しない場合は、*root*の横にあるをクリックし、*キーの再生成*をクリックします。既にキーが存在する場合は、再生成しないでください。
2. ストレージ VM を編集して、ソース ストレージ VM と宛先ストレージ VM の両方でユーザーを追加し、ユーザーをグループに追加します：ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. **Protection > Overview** をクリックし、**Local Policy Settings** をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. SnapMirror保護を適用してバケットを作成します。
   a. **Storage > Buckets** をクリックし、**Add** をクリックします。
   b. 名前を入力し、ストレージ VM を選択し、サイズを入力して、*その他のオプション*をクリックします。
   c. *権限*で、*追加*をクリックします。権限の確認は任意ですが、推奨されます。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - デフォルト `(bucketname, bucketname/*)` または必要な他の値を使用します

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。
   d. *保護*で、*SnapMirrorを有効にする（ONTAPまたはCloud）*にチェックを入れます。次に、以下の値を入力します：

- デスティネーション
  - **TARGET**：ONTAPシステム
  - **CLUSTER**：ローカル クラスターを選択します。
  - **STORAGE VM**：ローカルクラスタ上のストレージ VM を選択します。
  - **S3 SERVER CA CERTIFICATE**：ソース証明書の内容をコピーして貼り付けます。
- ソース
  - **S3 SERVER CA CERTIFICATE**：宛先証明書の内容をコピーして貼り付けます。

5. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
6. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
7. *保存*をクリックします。ソースストレージVMに新しいバケットが作成され、デスティネーションストレージVMに作成された新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. この SVM の最初のSnapMirror S3 関係である場合は、ソース SVM と宛先 SVM の両方にルート ユーザー キーが存在することを確認し、存在しない場合は再生成します：
   `vserver object-store-server user show`

   ルートユーザーのアクセスキーがあることを確認してください。ない場合は、以下を入力してください（
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   キーがすでにある場合は再生成しないでください。

2. ソースとデスティネーションの両方のSVMにバケットを作成します。

   `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーにアクセス ルールを追加します。

`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 既存のSnapMirror S3ポリシーがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous` – SnapMirror S3 関係の唯一のポリシータイプ（必須）。
   - `-rpo` – 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source* S3 サーバーの証明書に署名した CA 証明書を管理 SVM にインストールします：
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. 管理 SVM に、宛先 S3 サーバーの証明書に署名した CA 証明書をインストールします：
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate` + 外部 CA ベンダーによって署名された証明書を使用している場合は、この証明書を管理 SVM にインストールするだけで済みます。

   ```
   `security certificate install`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-
   cli/security-certificate-install.html["ONTAPコマンド リファレンス
   "^]をご覧ください。
   ```

6. SnapMirror S3 関係を作成します：
`snapmirror create -source-path src_svm_name:/bucket/bucket_name`

`-destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror -policy test-policy
```

7. ミラーリングがアクティブであることを確認します：
`snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

ローカル クラスタ上の既存の **ONTAP S3** バケットのミラー関係を作成します

同じクラスタ内の既存のS3バケットの保護は、たとえば、ONTAP 9.10.1よりも前のリリースからS3の設定をアップグレードした場合など、いつでも開始できます。データは、ソースとは別のStorage VMまたは同じStorage VMのバケットにミラーリングできます。

開始する前に

- ONTAPのバージョン、ライセンス、S3サーバの設定に関する要件を満たしている必要があります。
- ソースとデスティネーションのStorage VM間にピア関係が確立されている必要があります。
- ソースとデスティネーションのVMのCA証明書が必要です。自己署名CA証明書または外部CAベンダーが署名した証明書を使用できます。

System Manager

1. このStorage VMに対する最初のSnapMirror S3関係を作成する場合は、ソースとデスティネーションの両方のStorage VMに対するrootユーザのキーがあることを確認し、ない場合は再生成します。
   a. **Storage > Storage VMs** をクリックし、Storage VMを選択します。
   b. *設定*タブで、*S3*タイルの をクリックします。
   c. *ユーザー*タブで、rootユーザーのアクセスキーがあることを確認します。
   d. ない場合は、*root*の横にあるをクリックし、*Regenerate Key*をクリックします。既にキーが存在する場合は再生成しないでください。
2. 既存のユーザーとグループがソースとターゲットの両方のストレージVMに存在し、適切なアクセス権を持っていることを確認します：*ストレージ > ストレージVM*を選択し、ストレージVMを選択して*設定*タブを開きます。最後に*S3*タイルを見つけて を選択し、*ユーザー*タブ、*グループ*タブの順に選択して、ユーザーとグループのアクセス設定を表示します。

   詳細については、"S3のユーザとグループの追加"を参照してください。
3. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. *保護 > 概要*をクリックし、*ローカルポリシー設定*をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. 既存のバケットのバケット アクセス ポリシーが引き続き要件を満たしていることを確認します。
   a. **Storage > Buckets** をクリックし、保護するバケットを選択します。
   b. *権限*タブで *編集*をクリックし、*権限*の下の*追加*をクリックします。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Resources** - デフォルト値 `*(bucketname, bucketname/*)*`または必要なその他の値を使用します。

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。
5. SnapMirror S3を使用して既存のバケットを保護します。
   a. ストレージ > バケット をクリックし、保護するバケットを選択します。

b. *Protect*をクリックし、次の値を入力します：

- デスティネーション
  - **TARGET**：ONTAPシステム
  - **CLUSTER**：ローカル クラスターを選択します。
  - **STORAGE VM**：同じまたは別のストレージ VM を選択します。
  - **S3 SERVER CA CERTIFICATE**：*source* 証明書の内容をコピーして貼り付けます。
- ソース
  - **S3 SERVER CA CERTIFICATE**：_宛先_証明書の内容をコピーして貼り付けます。

6. 外部 CA ベンダーによって署名された証明書を使用している場合は、* 宛先で同じ証明書を使用する * をオンにします。
7. *宛先設定*をクリックすると、バケット名、容量、パフォーマンスサービスレベルのデフォルトの代わりに独自の値を入力することもできます。
8. *保存*をクリックします。既存のバケットが、宛先ストレージVMの新しいバケットにミラーリングされます。

ロックされたバケットのバックアップ

ONTAP 9.14.1以降では、ロックされたS3バケットをバックアップし、必要に応じてリストアできます。

新規または既存のバケットの保護設定を定義する際に、ソース クラスタとデスティネーション クラスタがONTAP 9.14.1以降を実行し、ソース バケットでオブジェクト ロックが有効になっている場合、デスティネーション バケットでオブジェクト ロックを有効にできます。ソース バケットのオブジェクト ロック モードとロック保持期間は、デスティネーション バケットにレプリケートされたオブジェクトに適用されます。また、*デスティネーション設定*セクションで、デスティネーション バケットに異なるロック保持期間を定義することもできます。この保持期間は、ソース バケットとS3インターフェースからレプリケートされた、ロックされていないオブジェクトにも適用されます。

バケットでオブジェクト ロックを有効にする方法については、"バケットの作成"を参照してください。

CLI

1. この SVM の最初のSnapMirror S3 関係である場合は、ソース SVM と宛先 SVM の両方にルート ユーザー キーが存在することを確認し、存在しない場合は再生成します：
   `vserver object-store-server user show`

   ルートユーザーのアクセスキーがあることを確認してください。ない場合は、以下を入力してください（
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   キーがすでにある場合は再生成しないでください。

2. デスティネーションSVMにミラー ターゲットにするバケットを作成します。

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. ソースとデスティネーションの両方のSVMで、デフォルトのバケット ポリシーのアクセス ルールが

正しいことを確認します。

`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

例

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo _integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：

   - `continuous` – SnapMirror S3 関係の唯一のポリシータイプ（必須）。
   - `-rpo` – 回復ポイント目標の時間を秒単位で指定します（オプション）。
   - `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

     例

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 管理SVMにCAサーバ証明書をインストールします。

   a. *source* S3 サーバーの証明書に署名した CA 証明書を管理 SVM にインストールします：`security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. 管理 SVM に、宛先 S3 サーバーの証明書に署名した CA 証明書をインストールします：`security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate` + 外部 CA ベンダーによって署名された証明書を使用している場合は、この証明書を管理 SVM にインストールするだけで済みます。

`security certificate install`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"^]をご覧ください。

6. SnapMirror S3 関係を作成します：
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   作成したポリシーを使用することも、デフォルトのポリシーをそのまま使用することもできます。

   例

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
   ```

7. ミラーリングがアクティブであることを確認します：
   `snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

ローカルクラスタ上のデスティネーション**ONTAP S3**バケットから引き継ぎます

ソース バケットのデータを使用できなくなった場合は、SnapMirror関係を解除してデスティネーション バケットを書き込み可能にし、データの提供を開始できます。

タスク概要

テイクオーバー処理が実行されると、ソース バケットが読み取り専用に変換され、元のデスティネーション バケットが読み取り / 書き込みに変換されて、SnapMirror S3関係が反転します。

無効になったソース バケットが再び使用できるようになると、SnapMirror S3は2つのバケットの内容を自動的に再同期します。標準のVolume SnapMirrorの構成と違って、関係を明示的に再同期する必要はありません。

デスティネーション バケットがリモート クラスタにある場合、テイクオーバー処理はリモート クラスタから開始する必要があります。

System Manager

使用できないバケットからフェイルオーバーし、データの提供を開始します。

1. *保護 > 関係*をクリックし、*SnapMirror S3*を選択します。
2. ⋮をクリックし、*フェイルオーバー*を選択して、*フェイルオーバー*をクリックします。

CLI

1. デスティネーション バケットのフェイルオーバー処理を開始します。
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. フェイルオーバー操作のステータスを確認します：
   `snapmirror show -fields status`

例

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

関連情報

- "SnapMirrorフェイルオーバーの開始"
- "snapmirror show"

ローカル クラスタのデスティネーション**SVM**から**ONTAP S3**バケットをリストアする

ソース バケットのデータがなくなったり破損したりした場合、デスティネーション バケットからオブジェクトをリストアしてデータを再度取り込むことができます。

タスク概要

デスティネーション バケットは既存のバケットにも新しいバケットにもリストアできます。リストア処理のターゲット バケットには、デスティネーション バケットの使用済み論理スペースよりも多くのスペースが必要です。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

リストア処理はローカル クラスタから開始する必要があります。

System Manager

バックアップ データをリストアします。

1. *Protection > Relationships*をクリックし、バケットを選択します。
2. ⋮をクリックし、*復元*を選択します。
3. ソース*で、*既存のバケット（デフォルト）または*新しいバケット*を選択します。
   - 既存のバケット（デフォルト）に復元するには、次の操作を実行します：
     - 既存のバケットを検索するクラスタとStorage VMを選択します。
     - 既存のバケットを選択します。
4. デスティネーションのS3サーバCA証明書の内容をコピーして貼り付けます。
   - *新しいバケット*に復元するには、次の値を入力します：
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンス サービス レベル。詳細については、"ストレージ サービス レベル"を参照してください。
     - デスティネーションのS3サーバCA証明書の内容。
5. *Destination*で、ソースS3サーバーCA証明書の内容をコピーして貼り付けます。
6. 保護 > 関係をクリックして、リストアの進行状況を監視します。

ロックされたバケットのリストア

ONTAP 9.14.1以降では、ロックされたバケットをバックアップし、必要に応じてリストアできます。

オブジェクトロックされたバケットは、新規または既存のバケットにリストアできます。次のシナリオでは、オブジェクトロックされたバケットをデスティネーションとして選択できます。

- 新しいバケットへの復元：オブジェクトロックが有効になっている場合、オブジェクトロックが有効になっているバケットを作成することで、バケットを復元できます。ロックされたバケットを復元すると、元のバケットのオブジェクトロックモードと保持期間が複製されます。新しいバケットに異なるロック保持期間を定義することもできます。この保持期間は、他のソースのロックされていないオブジェクトに適用されます。
- 既存のバケットへの復元：オブジェクトロックされたバケットは、既存のバケットでバージョニングと同様のオブジェクトロックモードが有効になっている限り、既存のバケットに復元できます。元のバケットの保持期間は維持されます。
- ロックされていないバケットの復元：バケットでオブジェクトロックが有効になっていない場合でも、ソース クラスタ上のオブジェクトロックが有効になっているバケットに復元できます。バケットを復元すると、ロックされていないすべてのオブジェクトがロックされ、デスティネーション バケットの保持モードと保有期間が適用されます。

CLI

1. オブジェクトを新しいバケットに復元する場合は、新しいバケットを作成してください。詳細については、"新しいONTAP S3バケットのクラウドバックアップ関係を作成する"をご覧ください。
2. デスティネーション バケットのリストア処理を開始します。
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name`

例

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

`snapmirror restore`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-restore.html["ONTAPコマンド リファレンス"^]を参照してください。

クラウド ターゲットでのバックアップによる保護

ONTAP SnapMirror S3クラウドターゲット関係の要件

ソースとターゲットの環境が、SnapMirror S3によるクラウド ターゲットへのバックアップ保護の要件を満たしていることを確認します。

データ バケットにアクセスするには、オブジェクト ストア プロバイダの有効なアカウント クレデンシャルが必要です。

クラスタをクラウド オブジェクト ストアに接続するためには、クラスタ間LIFとIPspaceがクラスタに設定されている必要があります。ローカル ストレージからクラウド オブジェクト ストアにデータをシームレスに転送するためには、各ノードにクラスタ間LIFを作成します。

StorageGRIDをターゲットにする場合は、次の情報を確認しておく必要があります。

- サーバ名：完全修飾ドメイン名（FQDN）またはIPアドレスで表されます。
- バケット名：バケットがすでに存在している必要があります。
- アクセス キー
- シークレット キー

さらに、StorageGRIDサーバ証明書の署名に使用するCA証明書を、`security certificate install`コマンドを使用してONTAP S3クラスタの管理ストレージVMにインストールする必要があります。詳細については、StorageGRIDを使用する場合は"CA証明書のインストール"を参照してください。

AWS S3をターゲットにする場合は、次の情報を確認しておく必要があります。

- サーバ名：完全修飾ドメイン名（FQDN）またはIPアドレスで表されます。
- バケット名：バケットがすでに存在している必要があります。
- アクセス キー
- シークレット キー

ONTAPクラスタの管理Storage VM用のDNSサーバが、FQDN（使用している場合）をIPアドレスに解決できる必要があります。

関連情報

- "security certificate install"

新しい**ONTAP S3**バケットのクラウドバックアップ関係を作成する

新しい S3 バケットを作成すると、SnapMirror S3 ターゲット バケットにすぐにバックアップできます。このターゲット バケットは、オブジェクト ストア プロバイダー（StorageGRID システムまたは Amazon S3 デプロイメント）上にあります。

開始する前に

- オブジェクト ストア プロバイダの有効なアカウント クレデンシャルと設定情報が必要です。
- ソース システムにクラスタ間ネットワーク インターフェイスとIPspaceが設定されている必要があります。
- • ソース ストレージ VM の DNS 構成は、ターゲットの FQDN を解決できる必要があります。

System Manager

1. Storage VMを編集してユーザを追加し、グループにユーザを追加します。
   a. ストレージ **>** ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、**S3** の下の をクリックします。

      詳細については、"S3のユーザとグループの追加"を参照してください。

2. ソース システムにクラウド オブジェクト ストアを追加します。
   a. *保護 > 概要*をクリックし、*クラウドオブジェクトストア*を選択します。
   b. *追加*をクリックし、*Amazon S3*または*StorageGRID*を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセス キー
      - シークレット キー
      - コンテナ（バケット）の名前
3. 既存のSnapMirror S3ポリシーがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. **Protection > Overview** をクリックし、**Local Policy Settings** をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシーの対象として、クラスタまたはSVMを選択します。
      - SnapMirror S3 関係には 継続 を選択します。
      - *Throttle*と*Recovery Point Objective*の値を入力します。
4. SnapMirror保護を適用してバケットを作成します。
   a. *Storage > Buckets*をクリックし、*Add*をクリックします。
   b. 名前を入力し、ストレージ VM を選択し、サイズを入力して、*その他のオプション*をクリックします。
   c. *権限*で、*追加*をクリックします。権限の確認は任意ですが、推奨されます。
      - **Principal** および **Effect**：ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions**：次の値が表示されていることを確認します。

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- リソース：デフォルト値 `_(bucketname, bucketname/*)`または必要なその他の値を使用します。

  これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。

d. *保護*で、*SnapMirrorを有効化（ONTAPまたはクラウド）*をチェックし、*クラウドストレージ*を選択してから、*クラウドオブジェクトストア*を選択します。

*保存*をクリックすると、ソースストレージVMに新しいバケットが作成され、クラウドオブジェクトストアにバックアップされます。

CLI

1. このSVMで最初のSnapMirror S3関係を作成する場合は、ソースSVMとデスティネーションSVMの両方にルートユーザキーが存在することを確認し、存在しない場合は再生成します：
   `vserver object-store-server user show` + ルートユーザのアクセスキーが存在することを確認します。存在しない場合は、次のように入力します：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + キーがすでに存在する場合は、再生成しないでください。
2. ソース SVM にバケットを作成します（
   `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. デフォルトのバケットポリシーにアクセスルールを追加します：
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 既存のSnapMirror S3ポリシーがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   パラメータ：* `type continuous` – SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo` – リカバリポイント目標の時間を秒単位で指定します（オプション）。* `-throttle` – スループッ

ト/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

例

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. ターゲットが StorageGRID システムの場合は、ソース クラスタの管理 SVM に StorageGRID CA サーバ証明書をインストールします。
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

```
`security certificate install`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-certificate-install.html["ONTAPコマンド リファレンス"^]をご覧ください。
```

6. SnapMirror S3宛先オブジェクトストアを定義します：
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

パラメータ：* `-object-store-name` – ローカル ONTAP システム上のオブジェクトストアターゲットの名前。* `-usage` – このワークフローには `data`を使用します。* `-provider-type` – `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server` – ターゲットサーバの FQDN または IP アドレス。* `-is-ssl-enabled` – SSL の有効化はオプションですが、推奨されます。+ `snapmirror object-store config create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. SnapMirror S3 関係を作成します：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path` - 前の手順で作成したオブジェクト ストア名と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトを受け入れることもできます。

例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. ミラーリングがアクティブであることを確認します：
`snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

既存の**ONTAP S3**バケットのクラウドバックアップ関係を作成する

既存のS3バケットのバックアップは、たとえばONTAP 9.10.1よりも前のリリースからS3の設定をアップグレードした場合など、いつでも開始できます。

開始する前に

- オブジェクト ストア プロバイダの有効なアカウント クレデンシャルと設定情報が必要です。
- ソース システムにクラスタ間ネットワーク インターフェイスとIPspaceが設定されている必要があります。
- ソースStorage VMのDNS設定でターゲットのFQDNを解決できる必要があります。

System Manager

1. ユーザーとグループが正しく定義されていることを確認します：ストレージ > ストレージ **VM** をクリックし、ストレージ VM をクリックして、設定 をクリックし、S3 の下の をクリックします。

   詳細については、"S3のユーザとグループの追加"を参照してください。

2. 既存のものがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   a. *Protection > Overview*をクリックし、*Local Policy Settings*をクリックします。
   b. *Protection Policies*の横にあるをクリックし、*Add*をクリックします。
   c. ポリシーの名前と説明を入力します。
   d. ポリシーの対象として、クラスタまたはSVMを選択します。
   e. SnapMirror S3 関係には 継続 を選択します。
   f. *スロットル*と*リカバリポイント目標値*を入力します。
3. ソース システムにクラウド オブジェクト ストアを追加します。
   a. *保護 > 概要*をクリックし、*クラウドオブジェクトストア*を選択します。
   b. 追加*をクリックし、**StorageGRID Webscale** の ***Amazon S3** または その他 を選択します。
   c. 次の値を入力します。
      - クラウド オブジェクト ストアの名前
      - URLの形式（パスまたは仮想ホスト）
      - Storage VM（S3対応）
      - オブジェクト ストアのサーバ名（FQDN）
      - オブジェクト ストアの証明書
      - アクセス キー
      - シークレット キー
      - コンテナ（バケット）の名前
4. 既存のバケットのバケット アクセス ポリシーが引き続き要件を満たしていることを確認します。
   a. ストレージ > バケット をクリックし、保護するバケットを選択します。
   b. *権限*タブで *編集*をクリックし、*権限*の下の*追加*をクリックします。
      - **Principal** と **Effect** - ユーザーグループ設定に対応する値を選択するか、デフォルトを受け入れます。
      - **Actions** - 次の値が表示されていることを確認します：`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Resources** - デフォルト値 `*(bucketname, bucketname/*)*` または必要なその他の値を使用します。

        これらのフィールドの詳細については、"バケットへのユーザ アクセスの管理"を参照してください。

5. SnapMirror S3を使用してバケットをバックアップします。
   a. ストレージ > バケット をクリックし、バックアップするバケットを選択します。
   b. *保護*をクリックし、*ターゲット*の下の*クラウドストレージ*を選択して、*クラウドオブジェクトストア*を選択します。

*保存*をクリックすると、既存のバケットがクラウドオブジェクトストアにバックアップされます。

CLI

1. デフォルトのバケットポリシーのアクセスルールが正しいことを確認します：
   `vserver object-store-server bucket policy add-statement -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-effect {allow|deny} -action` *`object_store_actions`* `-principal` *`user_and_group_names`* `-resource` *`object_store_resources`* `[-sid` *`text`*`] [-index` *`integer`*`]`

   例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. 既存のSnapMirror S3ポリシーがなく、デフォルトポリシーを使用したくない場合は、SnapMirror S3ポリシーを作成してください：
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   パラメータ：* `type continuous` – SnapMirror S3関係の唯一のポリシータイプ（必須）。* `-rpo` – リカバリポイント目標の時間を秒単位で指定します（オプション）。* `-throttle` – スループット/帯域幅の上限をキロバイト/秒単位で指定します（オプション）。

   例

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. ターゲットが StorageGRID システムの場合は、ソース クラスタの管理 SVM に StorageGRID CA 証明書をインストールします。
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   ```
   `security certificate install`
   の詳細については、link:https://docs.netapp.com/us-en/ontap-
   cli/security-certificate-install.html["ONTAPコマンド リファレンス
   "^]をご覧ください。
   ```

4. SnapMirror S3宛先オブジェクトストアを定義します：
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

パラメータ：* `-object-store-name` – ローカルONTAPシステム上のオブジェクトストアターゲットの名前。* `-usage` – このワークフローには `data`を使用します。* `-provider-type` – `AWS_S3`および `SGWS`（StorageGRID）ターゲットがサポートされています。* `-server` – ターゲットサーバのFQDNまたはIPアドレス。* `-is-ssl-enabled` – SSLの有効化はオプションですが、推奨されます。+ `snapmirror object-store config create`の詳細については、"ONTAPコマンド リファレンス"を参照してください。

例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. SnapMirror S3 関係を作成します：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

パラメータ：* `-destination-path` - 前の手順で作成したオブジェクト ストア名と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトを受け入れることもできます。

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. ミラーリングがアクティブであることを確認します：
`snapmirror show -policy-type continuous -fields status`

関連情報

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

クラウドターゲットから**ONTAP S3**バケットをリストアする

ソース バケットのデータがなくなったり破損したりした場合、デスティネーション バケットからリストアしてデータを再度取り込むことができます。

タスク概要

デスティネーション バケットは既存のバケットにも新しいバケットにもリストアできます。リストア処理の

ターゲット バケットには、デスティネーション バケットの使用済み論理スペースよりも多くのスペースが必要です。

既存のバケットを使用する場合は、リストア処理の開始時に空にする必要があります。リストアでは、バケットを特定の時点に「ロールバック」するのではなく、空のバケットに以前の内容を取り込みます。

System Manager

バックアップ データをリストアします。

1. *保護 > 関係*をクリックし、*SnapMirror S3*を選択します。
2. をクリックし、*復元*を選択します。
3. ソース*で、*既存のバケット（デフォルト）または*新しいバケット*を選択します。
   - 既存のバケット（デフォルト）に復元するには、次の操作を実行します：
     - 既存のバケットを検索するクラスタとStorage VMを選択します。
     - 既存のバケットを選択します。
     - デスティネーション S3 サーバー CA 証明書の内容をコピーして貼り付けます。
   - *新しいバケット*に復元するには、次の値を入力します：
     - 新しいバケットをホストするクラスタとStorage VM。
     - 新しいバケットの名前、容量、パフォーマンス サービス レベル。詳細については、"ストレージ サービス レベル"を参照してください。
     - デスティネーションのS3サーバCA証明書の内容。
4. *Destination*の下に、*source* S3サーバーCA証明書の内容をコピーして貼り付けます。
5. 復元の進行状況を監視するには、*保護 > 関係*をクリックします。

CLIの手順

1. 復元用の新しいデスティネーション バケットを作成します。詳細については、"バケット（クラウド ターゲット）のバックアップ関係を作成する"を参照してください。
2. デスティネーション バケットのリストア処理を開始します。
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   例

   次の例では、デスティネーション バケットを既存のバケットにリストアします。
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   `snapmirror restore`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/snapmirror-restore.html["ONTAPコマンド リファレンス"^]を参照してください。

ONTAP SnapMirror S3ポリシーを変更する

RPO とスロットル値を調整する場合は、S3 SnapMirrorポリシーを変更することがあります。

System Manager

1. *保護 > 関係*をクリックし、変更する関係の保護ポリシーを選択します。
2. ポリシー名の横にある ⋮ をクリックし、*編集*をクリックします。

CLI

SnapMirror S3ポリシーを変更します：

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

パラメータ：

- `-rpo`：回復ポイント目標の時間を秒単位で指定します。
- `-throttle`：スループット/帯域幅の上限をキロバイト/秒単位で指定します。

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

関連情報

- "snapmirror policy modify"

SnapshotによるS3データの保護

ONTAP S3スナップショットについて学ぶ

ONTAP 9.16.1以降では、ONTAP Snapshotテクノロジを使用して、ONTAP S3バケットの読み取り専用ポイントインタイム イメージを生成できます。

S3 Snapshot機能を使用すると、Snapshotを手動で作成したり、Snapshotポリシーを通じて自動的に生成したりできます。S3 Snapshotは、S3バケットとしてS3クライアントに提供されます。S3クライアントを介して、Snapshotのコンテンツの参照やリストアを行えます。

ONTAP 9.16.1では、S3バケット内の現在のバージョンのオブジェクトのみが、S3 Snapshotによってキャプチャされます。バージョン管理されたバケットの最新ではないバージョンは、S3 Snapshotにキャプチャされません。また、Snapshotの作成後にオブジェクト タグが変更された場合には、ポイントインタイムのオブジェクト タグは、Snapshotにキャプチャされません。

S3 スナップショットはクラスタの時刻に依存します。時刻を同期するには、クラスタ内の NTP サーバーを設定する必要があります。詳細については、"クラスター時間を管理する"を参照してください。

クォータとスペース使用量

クォータは、S3バケット内のオブジェクトの数と使用済み論理サイズを追跡します。S3 Snapshotが作成されると、S3 Snapshotにキャプチャされたオブジェクトは、Snapshotがファイルシステムから削除されるまで、バケットのオブジェクト数と使用済みサイズにカウントされます。

マルチパート オブジェクト

マルチパート オブジェクトについては、最終的なオブジェクトのみがSnapshotにキャプチャされます。部分的にアップロードされたマルチパート オブジェクトは、Snapshotにキャプチャされません。

バージョン管理されたバケットとバージョン管理されていないバケット上の**Snapshot**

Snapshotは、バージョン管理されたバケットとバージョン管理されていないバケットのどちらにも作成できます。Snapshotには、Snapshotがキャプチャされた時点での最新バージョンのオブジェクトのみが含まれます。

バージョン管理されたバケットと**Snapshot**

オブジェクトのバージョン管理が有効になっているバケットでは、Snapshot作成後の最新バージョンのオブジェクトのコンテンツがSnapshotに保持されます。バケット内の最新でないバージョンは除外されます。

次の例を考えてみましょう。オブジェクトのバージョニングが有効になっているバケットで、オブジェクト `obj1`のバージョンがv1、v2、v3、v4、v5であるとします。 `obj1`v3（キャプチャ時点の最新バージョン）から `snap1`スナップショットを作成しました。 `snap1`を参照すると、 `obj1`はv3で作成されたコンテンツを持つオブジェクトとして表示されます。以前のバージョンのコンテンツは返されません。

> 最新でないバージョンは、Snapshotが削除されるまでファイルシステムに保持されます。

バージョン管理されていないバケットと**Snapshot**

バージョン管理されていないバケットでは、Snapshot作成前の最新コミットのコンテンツがS3 Snapshotに保持されます。

次の例を考えてみましょう：オブジェクトのバージョン管理が利用できないバケットで、オブジェクト `obj1`が（t1、t2、t3、t4、t5）に複数回上書きされています。t3とt4の間にS3スナップショット `snap1`を作成しました。 `snap1`を参照すると、 `obj1`にはt3で作成されたコンテンツが表示されます。

オブジェクトの有効期限と**Snapshot**

ONTAP S3オブジェクトの有効期限とS3 Snapshot機能は、別々に機能します。ONTAPオブジェクトの有効期限は、S3バケットに定義されたライフサイクル管理ルールに従って各バージョンのオブジェクトを期限切れにする機能です。S3 Snapshotは、Snapshotが作成された時点のバケット オブジェクトの静的コピーです。

バケットでオブジェクトのバージョン管理が有効になっていて、そのバケットに定義された有効期限ルールに基づいて特定のバージョンのオブジェクトが削除された場合、そのバージョンが現在のバージョンとして1つ以上のS3 Snapshotにキャプチャされていれば、そのバージョンのコンテンツはファイルシステムに残ります。当該バージョンのオブジェクトは、そのSnapshotが削除された場合にのみファイルシステムに存在しなくなります。

同様に、バージョン管理が無効になっているバケットでは、有効期限ルールに基づいてオブジェクトが削除された場合でも、そのオブジェクトがいずれかのS3 Snapshotにキャプチャされているかぎり、オブジェクトはファイルシステムに保持されます。オブジェクトがキャプチャされているSnapshotが削除されると、オブジェクトはファイルシステムから完全に削除されます。

S3 オブジェクトの有効期限とライフサイクル管理の詳細については、"バケット ライフサイクル管理ルールの作成"を参照してください。

S3 Snapshotの制限事項

ONTAP 9.16.1では、以下の機能の除外とシナリオに注意してください。

- 1つのS3バケットで生成できるSnapshotは、最大1,023個です。
- クラスタをONTAP 9.16.1より前のバージョンのONTAPにリバートする前に、クラスタ内のすべてのバケットからS3 Snapshotとメタデータをすべて削除する必要があります。
- Snapshotがあるオブジェクトを含むS3バケットを削除する必要がある場合は、そのバケット内のすべてのオブジェクトに対応するSnapshotを、すべて削除しておく必要があります。
- S3 Snapshotは、以下の構成ではサポートされません。
  - SnapMirror関係にあるバケット
  - オブジェクトロックが有効になっているバケット
  - NetApp Console上
  - System Manager
  - ONTAP MetroCluster構成
- ローカルまたはリモートのFabricPool容量階層として使用されているバケットでは、S3スナップショットは推奨されません。

ONTAP S3 Snapshotを作成する

S3 Snapshotは手動で生成することも、Snapshotポリシーを設定して自動的に作成させることもできます。Snapshotはオブジェクトの静的コピーとして機能し、データのバックアップとリカバリで使用します。Snapshotの保持期間を決定するために、指定した間隔でSnapshotを自動的に作成するSnapshotポリシーを作成できます。

S3 Snapshotを使用すると、オブジェクトのバージョン管理が有効かどうかに関係なく、S3バケット内のオブジェクト データを保護できます。

Snapshotは、S3バケットでオブジェクトのバージョン管理が有効になっていない場合のデータ保護の確立に役立ちます。以前のバージョンのオブジェクトを使用できない場合に、ポイントインタイム レコードとして機能するSnapshotを使用してリストア処理を行えるからです。

タスク概要

- Snapshotには、以下の命名規則が適用されます（手動作成でも自動作成でも）。
  - S3 Snapshot名に指定できる文字数は最大30文字です。
  - S3 Snapshot名に使用できる文字は、小文字のアルファベット、数字、ドット（.）、ハイフン（-）のみです。
  - S3 Snapshot名の末尾の文字は、アルファベットか数字にする必要があります。
  - S3 Snapshot名に部分文字列を含めることはできません `s3snap`
- S3プロトコルの使用時には、バケット名の制限によってバケット名が63文字に制限されます。ONTAP S3

Snapshotは、S3プロトコルを介してバケットとして提供されるため、Snapshotバケット名にも同様の制限が適用されます。デフォルトでは、元のバケット名がベース バケット名として使用されます。

- どのSnapshotがどのバケットに属しているかを識別しやすくするために、Snapshotバケットはベースバケット名と、Snapshot名の先頭に付加される特殊な文字列 `-s3snap-`で構成されます。Snapshotバケット名は `<base_bucket_name>-s3snap-<snapshot_name>`という形式になります。

  たとえば、 `bucket-a`で `snap1`を作成するために次のコマンドを実行すると、 `bucket-a-s3snap-snap1`という名前のSnapshotバケットが作成されます。ベース バケットにアクセスする権限がある場合は、S3クライアント経由でこのバケットにアクセスできます。

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- 63文字を超えるSnapshotバケット名は作成できません。
- Snapshotの自動作成名には、ポリシー スケジュール名とタイムスタンプが含まれます。これは、従来のボリューム Snapshot の命名規則に似ています。たとえば、スケジュールされた Snapshot 名は `daily-2024-01-01-0015`や `hourly-2024-05-22-1105`になります。

S3 Snapshotの手動作成

ONTAP CLIを使用してS3 Snapshotを手動で作成できます。手順では、ローカル クラスタにのみSnapshotを作成します。

手順

1. S3 Snapshotを作成します。

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

次の例では、 `vs0`ストレージVMと `website-data`バケットに `pre-update`という名前のSnapshotを作成します：

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

バケットへの**S3 Snapshot**ポリシーの割り当て

S3バケット レベルでSnapshotポリシーを設定すると、スケジュールされたS3 SnapshotがONTAPによって自動的に作成されます。従来のSnapshotポリシーと同様に、S3 Snapshotにも最大5つのスケジュールを設定できます。

スナップショットポリシーでは通常、スナップショットを作成するスケジュール、各スケジュールで保持するコピーの数、およびスケジュールプレフィックスを指定します。例えば、ポリシーで毎日午前0：10にS3スナップショットを1つ作成し、最新の2つのコピーを保持し、それぞれに `daily-<timestamp>`という名前を付けることができます。

デフォルトのSnapshotポリシーでは、以下のSnapshotが保持されます。

- 時間単位のSnapshot×6
- 日単位のSnapshot×2
- 週単位のSnapshot×2

開始する前に

- Snapshotポリシーは、S3バケットに割り当てる前に作成しておく必要があります。

> S3 Snapshot用のポリシーは、他のONTAP Snapshotポリシーと同じルールに従います。ただし、いずれかのSnapshotスケジュールに保持期間が設定されているSnapshotポリシーを、S3バケットに割り当てることはできません。

スナップショットを自動生成するためのスナップショット ポリシーの作成の詳細については、"カスタム スナップショット ポリシーの設定の概要"を参照してください。

手順

1. Snapshotポリシーをバケットに割り当てます。

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

または

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> クラスタをONTAP 9.16.1より前のONTAPバージョンに戻す必要がある場合は、すべてのバケットの `snapshot-policy`の値が `none（または -）に設定されていることを確認します。

関連情報

"ONTAP S3スナップショットについて学ぶ"

ONTAP S3スナップショットの表示と復元

ONTAP 9.16.1以降では、S3クライアントからバケットのS3スナップショット データを表示および参照できます。ONTAP 9.18.1以降では、S3スナップショット バケットにONTAP CLIからネイティブにアクセスできるようになりました。さらに、S3スナップショットからS3クライアント上の単一のオブジェクト、オブジェクト セット、またはバケット全体を復元できます。

開始する前に

- ONTAP CLIでバケット スナップショットのリストア操作をネイティブに実行するには、クラスタ内のすべてのノードでONTAP 9.18.1以降が稼働している必要があります。ONTAP 9.18.1以降では、S3ブラウザ

は不要になりましたが、これらの操作は引き続きサポートされます。

- 特定のバケットに対して一度に実行できるスナップショット リストア操作は 1 つだけです。

タスク概要

ONTAP 9.16.1以降、ONTAP S3スナップショット機能は、手動およびスケジュールによるスナップショットの作成と削除、S3バケットのスナップショット ポリシー、S3クライアントベースのスナップショット参照など、ONTAP S3バケットの基本的なスナップショット機能を提供します。

ONTAP 9.18.1以降では、ネイティブのONTAPスナップショット リストアのサポートが追加され、ONTAP管理者はS3ブラウザを使用せずにポイントインタイム リストア機能を利用できるようになります。スナップショットには現在のバケット バージョンのみがキャプチャされます。バージョン履歴はキャプチャされず、S3スナップショット リストア操作ではリストアされません。

S3 Snapshotのリストアップと表示

S3 Snapshotの詳細を表示して比較し、エラーを特定できます。ONTAP CLIを使用すると、S3バケットに作成されたすべてのSnapshotをリストアップできます。

手順

1. S3 Snapshotをリストアップします。

```
vserver object-store-server bucket snapshot show
```

クラスタ上のすべてのバケットに対して作成されたS3スナップショットのスナップショット名、Storage VM、バケット、作成時刻、instance-uuidを表示できます。

2. バケット名を指定して、その特定のバケットに対して作成されたすべてのS3スナップショットの名前、作成時刻、instance-uuidを表示することもできます。

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

S3 Snapshotコンテンツの参照

環境内で障害や問題が発生した場合には、エラーを特定するために、S3バケットのSnapshotのコンテンツを参照できます。また、S3 Snapshotを参照して、リストアの対象にするエラーのないコンテンツを特定することもできます。

S3スナップショットは、S3クライアントにスナップショットバケットとして提供されます。スナップショットバケット名は `<base_bucket_name>-s3snap-<snapshot_name>`という形式です。 `ListBuckets`S3 API操作を使用して、ストレージVM内のすべてのスナップショットバケットを確認できます。

S3 スナップショット バケットはベース バケットのアクセス ポリシーを継承し、読み取り専用操作のみをサポートします。削除および書き込みベースの操作は禁止されています。ベース バケットへのアクセス権限がある場合は、S3 スナップショット バケットに対して `HeadObject`、 `GetObject`、 `GetObjectTagging`、 `ListObjects`、 `ListObjectVersions`、 `GetObjectAcl`、 `CopyObject`などの読み取り専用 S3 API 操作も実行できます。

`CopyObject`操作は、S3 スナップショット バケットがソース バケットのスナップショットである場合にのみサポートされ、スナップショットの保存先である場合はサポートされません。

これらの操作の詳細については、"ONTAP S3でサポートされる処理"を参照してください。

ONTAPを使用して**S3**スナップショットからバケットをリストアする

ONTAP 9.18.1以降では、ONTAP CLIを使用してONTAP S3スナップショットからバケット全体を復元できます。復元できるのは、選択したスナップショットが作成された時点で存在していたバケットのバージョンのみです。

手順

1. バケットを復元するために使用するスナップショットを特定します：

```
vserver object-store-server bucket snapshot show
```

2. バケットを復元します：

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

S3クライアントを使用して**S3**バケットのスナップショットからデータをリストアする

ONTAPでバケット全体を復元するだけでなく、S3cmdやS3 BrowserなどのS3クライアントを使用して、S3スナップショットから単一のオブジェクト、オブジェクトのセット、またはバケット全体を復元することもできます。

"バージョン管理されたスナップショットとバージョン管理されていないスナップショットの詳細をご確認ください。"

`aws s3 cp`コマンドを使用して、バケット全体、特定のプレフィックスを持つオブジェクト、または単一のオブジェクトを復元できます。

手順

1. S3ベース バケットのSnapshotを作成します。

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Snapshotを使用してベース バケットをリストアします。
   - バケット全体を復元します。スナップショット バケット名を `<base_bucket_name>-s3snap-<snapshot_name>`の形式で使用します。

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

- プレフィックスを持つディレクトリ内のオブジェクトを復元します： `dir1`

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

- `web.py`という名前の単一のオブジェクトを復元します：

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

ONTAP S3スナップショットを削除する

不要になったS3 Snapshotを削除して、バケット内のストレージ スペースを解放できます。S3 Snapshotを手動で削除したり、S3バケットに関連付けられたSnapshotポリシーを変更して、スケジュールで保持されるSnapshotの数を変更したりできます。

S3バケットのスナップショットポリシーは、従来のONTAPスナップショットポリシーと同じ削除ルールに従います。スナップショットポリシーの作成の詳細については、"Snapshotポリシーの作成"を参照してください。

タスク概要

- あるバージョンのオブジェクト（バージョン管理されたバケット内のもの）や、1つのオブジェクト（バージョン管理されていないバケットのもの）が複数のSnapshotにキャプチャされている場合、そのオブジェクトを保護している最後のSnapshotが削除されるまで、そのオブジェクトはファイル システムから削除されません。
- Snapshotがあるオブジェクトを含むS3バケットを削除するには、そのバケット内のすべてのオブジェクトのSnapshotをすべて削除しておく必要があります。
- クラスタをONTAP 9.16.1より前のONTAPバージョンに戻す必要がある場合は、すべてのバケットのS3スナップショットがすべて削除されていることを確認してください。また、 `vserver object-store-server bucket clear-snapshot-metadata`コマンドを実行してS3バケットのスナップショット メタデータを削除する必要がある場合もあります。詳細については、"S3 Snapshotメタデータのクリア"を参照してください。
- Snapshotをバッチで削除すると、複数のSnapshotにキャプチャされた多数のオブジェクトを削除できるため、個別にSnapshotを削除する場合よりも多くのスペースが効果的に解放されます。その結果、より多くのスペースをストレージ オブジェクト用に再利用できます。

手順

1. 特定のS3 Snapshotを削除するには、以下のコマンドを実行します。

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. バケット内のすべてのS3 Snapshotを削除するには、以下のコマンドを実行します。

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

S3 Snapshotメタデータのクリア

S3 Snapshotでは、Snapshotメタデータもバケット内で生成されます。Snapshotメタデータは、すべてのSnapshotがバケットから削除されても、バケット内に残ります。Snapshotメタデータがあると、以下の処理がブロックされます。

- ONTAP 9.16.1より前のバージョンのONTAPへのクラスタのリバート
- バケットでのSnapMirror S3の設定

これらの処理を実行する前に、バケットからすべてのSnapshotメタデータをクリアする必要があります。

開始する前に

メタデータのクリアを開始する前に、バケットからすべてのS3 Snapshotを削除しておく必要があります。

手順

1. バケットからSnapshotメタデータをクリアするには、このコマンドを実行します。

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

S3イベントの監査

ONTAP S3イベントの監査について学ぶ

ONTAP 9.10.1以降では、ONTAP S3環境のデータ イベントや管理イベントを監査できます。S3の監査機能は既存のNASの監査機能とほぼ同じであり、クラスタ内でS3とNASの監査を同時に使用できます。

SVMでS3の監査設定を作成して有効にすると、S3イベントがログ ファイルに記録されます。ログに記録できるイベントは次のとおりです。

リリース別のオブジェクト アクセス（データ）イベント

9.11.1：

- ListBucketVersions
- ListBucket（9.10.1のListObjectから名称変更）
- ListAllMyBuckets（9.10.1のListBucketsから名称変更）

9.10.1：

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListParts

リリース別の管理イベント

9.15.1：

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1：

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1：

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1：

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1：

- GetBucketVersioning
- PutBucketVersioning

9.10.1：

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

ログ形式はJavaScript Object Notation（JSON）です。

クラスタごとに監査可能なSVM数は、S3とNFSの監査設定を合わせて最大400個です。

次のライセンスが必要です。

- ONTAP S3プロトコルおよびストレージ向けのONTAP ONE（以前はCore Bundleに付属）

詳細については、"ONTAP監査プロセスの仕組み"を参照してください。

監査の保証

デフォルトでは、S3とNASの監査はどちらも保証されます。ONTAPでは、あるノードが利用できない場合でも、監査可能なバケット アクセス イベントはすべて記録されます。要求されたバケット処理は、その処理の監査レコードが永続的ストレージのステージング ボリュームに保存されるまで完了できません。スペース不足またはその他の問題が原因で監査レコードをステージング ファイルにコミットできない場合、クライアント処理は拒否されます。

監査のスペース要件

ONTAPの監査システムでは、監査レコードは最初に個々のノードのバイナリ ステージング ファイルに格納されます。定期的に統合され、ユーザが読解可能なイベント ログに変換されて、SVMの監査イベント ログ ディレクトリに格納されます。

ステージング ファイルは専用のステージング ボリュームに格納されます。このボリュームは、監査設定の作成時にONTAPによって作成されます。各アグリゲートに1つのステージング ボリュームがあります。

監査設定を作成するにあたっては、以下の項目について十分な使用可能スペースを確保する必要があります。

- 監査対象バケットを格納する、アグリゲート内のステージング ボリューム。
- 変換後のイベント ログの格納先ディレクトリを含むボリューム。

S3の監査設定を作成する際には、次のどちらかの方法を使用して、イベント ログの数、そして結果的にボリューム内の使用可能スペースを制御できます。

- 数値制限。 `-rotate-limit`パラメータは、保存する必要がある監査ファイルの最小数を制御します。
- 時間制限。 `-retention-duration`パラメータは、ファイルを保存できる最大期間を制御します。

どちらのパラメータも、設定値を超えると古い監査ファイルが削除されて新しい監査ファイル用のスペースが確保されます。どちらのパラメータも、0を指定するとすべてのファイルが保持されます。したがって、十分なスペースを確保するためには、どちらかのパラメータをゼロ以外の値に設定することを推奨します。

監査の保証により、ローテーションの制限に達する前に監査データに使用できるスペースがなくなると、新しい監査データを作成できず、クライアントはデータにアクセスできなくなります。そのため、このパラメータに指定する値と監査に割り当てるスペースを慎重に決定し、監査システムからの使用可能なスペースに関する警告に適切に対処する必要があります。

詳細については、"監査の基本概念"を参照してください。

ONTAP S3監査構成を計画する

S3の監査設定では、いくつかのパラメータを指定する必要があります（デフォルトを受け入れることもできます）。特に、ログ ローテーションのパラメータについては、十分な空きスペースを確保できるように検討が必要です。

`vserver object-store-server audit create`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/vserver-object-store-server-audit-create.html["ONTAPコマンド リファレンス
"^]をご覧ください。

一般パラメータ

監査設定の作成時に指定する必要がある2つの必須パラメータがあります。また、オプションのパラメータが3つあります。

情報の種類	オプション	必須
SVM 名 監査設定を作成するSVMの名前。 S3対応の既存のSVMを指定する必要があります。	`-vserver` *`svm_name`*	はい

ログの保存先パス 変換された監査ログを格納する場所を指定します。SVM上の既存のパスを指定する必要があります。 パスは864文字以内で、読み取り / 書き込みアクセス権が設定されている必要があります。 パスが有効でない場合、監査設定コマンドは失敗します。	`-destination text`	はい
監査対象イベントのカテゴリー 監査できるイベント カテゴリは次のとおりです。 • データGetObject、PutObject、DeleteObjectイベント • 管理 PutBucket および DeleteBucket イベント デフォルトでは、データ イベントのみが監査されます。	`-events {data|management}, …`	いいえ

監査ログ ファイルの数を制御するには、次のどちらかのパラメータを入力します。値を入力しないと、すべてのログ ファイルが保持されます。

情報の種類	オプション	必須
ログ ファイルのローテーション制限 最も古いログファイルをローテーションする前に保持する監査ログファイルの数を決定します。たとえば、値に5を入力すると、最後の5つのログファイルが保持されます。 値を0に設定すると、すべてのログ ファイルが保持されます。デフォルト値は0です。	`-rotate-limit integer`	いいえ
ログファイルの保存期間制限 ログ ファイルを削除するまでの保持期間を指定します。たとえば、「5d0h0m」という値を入力すると、5日以上経過したログが削除されます。 値を0に設定すると、すべてのログ ファイルが保持されます。デフォルト値は0です。	`-retention duration integer_time`	いいえ

監査ログのローテーション パラメータ

監査ログは、サイズまたはスケジュールに基づいてローテーションできます。デフォルトでは、サイズに基づいて監査ログがローテーションされます。

ログ サイズに基づいたログのローテーション

デフォルトのログローテーション方法とデフォルトのログサイズを使用する場合は、ログローテーションに関する特別なパラメータを設定する必要はありません。デフォルトのログサイズは100 MBです。

デフォルトのログ サイズを使用しない場合は、 `-rotate-size` パラメータを構成してカスタム ログ サイズを指定できます。

ログ サイズのみに基づいてローテーションをリセットする場合は、次のコマンドを使用して `-rotate-schedule-minute`パラメータの設定を解除します：

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

スケジュールに基づいたログのローテーション

スケジュールに基づいて監査ログをローテーションすることを選択した場合は、時間ベースのローテーション パラメータを任意の組み合わせで使用して、ログのローテーションをスケジュールできます。

- 時間ベースのローテーションを使用する場合、 `-rotate-schedule-minute`パラメータは必須です。
- それ以外の時間に基づくローテーション パラメータは、すべてオプションです。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- ローテーション スケジュールは、すべての時間関連値を使用して計算されます。たとえば、 `-rotate-schedule-minute`パラメータのみを指定した場合、監査ログ ファイルは、年間を通じてすべての月のすべての時間帯において、すべての曜日で指定された分に基づいてローテーションされます。
- 時間ベースのローテーション パラメータを 1 つまたは 2 つだけ指定すると（たとえば、 `-rotate-schedule-month`および `-rotate-schedule-minutes`）、指定した月のみ、すべての曜日、すべての時間帯で指定した分の値に基づいてログ ファイルがローテーションされます。

  たとえば、監査ログを1月、3月、8月のすべての月曜日、水曜日、土曜日の午前10：30にローテーションするように指定できます。

- `-rotate-schedule-dayofweek`と `-rotate-schedule-day`の両方に値を指定した場合、それらは独立して考慮されます。

  たとえば、 `-rotate-schedule-dayofweek`を金曜日、 `-rotate-schedule-day`を13と指定した場合、監査ログは13日の金曜日だけでなく、毎週金曜日と指定した月の13日にローテーションされます。

- スケジュールのみに基づいてローテーションをリセットする場合は、次のコマンドを使用して `-rotate-size parameter`の設定を解除します：

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

ログ サイズとスケジュールに基づいたログのローテーション

-rotate-size パラメータと時間ベースのローテーション パラメータを任意の組み合わせで設定することで、ログ サイズとスケジュールに基づいてログ ファイルをローテーションできます。例： `-rotate-size`が10 MBに

設定され、 `-rotate-schedule-minute`が15に設定されている場合、ログ ファイルのサイズが10 MBに達したとき、または毎時15分（どちらか早い方のイベント）にログ ファイルがローテーションされます。

この手順で説明されているコマンドの詳細については、"ONTAPコマンド リファレンス"を参照してください。

ONTAP S3監査設定を作成して有効にする

S3の監査を実装するには、S3対応SVMに永続的オブジェクト ストアの監査設定を作成し、その設定を有効にします。

開始する前に

- S3 対応の SVM があります。
- ローカル階層にステージング ボリューム用の十分なスペースがあることを確認します。

タスク概要

監査対象のS3バケットを含むSVMごとに監査設定が必要です。新規または既存のS3サーバーでS3監査を有効にできます。監査設定は、*vserver object-store-server audit delete*コマンドで削除されるまでS3環境に保持されます。

S3の監査設定は、監査対象として選択したSVM内のすべてのバケットに適用されます。監査を有効にしたSVMには、監査対象のバケットだけでなく、監査対象外のバケットも含めることができます。

S3監査では、ログサイズまたはスケジュールに基づいて自動的にログローテーションを行うように設定することをお勧めします。自動ログローテーションを設定しない場合は、デフォルトですべてのログファイルが保持されます。*vserver object-store-server audit rotate-log*コマンドを使用して、S3ログファイルを手動でローテーションすることもできます。

SVMがSVMディザスタ リカバリ ソースである場合、デスティネーション パスをルート ボリューム上に設定することはできません。

手順

1. ログ サイズまたはスケジュールに基づいて監査ログをローテーションする監査設定を作成します。

監査ログのローテーションの基準	入力する内容
ログ サイズ	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d`*`][_`*`integer_h`*`][_`*`integer_m`*`][_`*`integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`

監査ログのローテーションの基準	入力する内容
スケジュール	`vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute* `-rotate-schedule-minute`パラメータは、時間ベースの監査ログのローテーションを構成する場合に必須です。

2. S3の監査を有効にします。

   `vserver object-store-server audit enable -vserver` *svm_name*

例

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査設定を作成します。ログは/audit_logディレクトリに格納されます。ログ ファイル サイズの上限は200MBです。ログのサイズが200MB以上になると、ログがローテーションされます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

次の例は、サイズに基づくローテーションを使用してすべてのS3イベント（デフォルト）を監査する監査設定を作成します。ログ ファイルの最大サイズは100MB（デフォルト）で、5日経過すると削除されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

以下の例では、時間ベースのローテーションを使用してS3管理イベントと集約型アクセスポリシーのステージングイベントを監査する監査設定を作成します。監査ログは毎月、毎日午後12：30にローテーションされます。ログローテーションの上限は5です。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

ONTAP S3監査用のバケットを選択する

監査が有効なSVMから監査対象のバケットを指定する必要があります。

開始する前に

- S3 監査が有効になっている SVM があります。

タスク概要

S3監査設定はSVMごとに有効化されますが、監査が有効になっているSVM内のバケットを選択する必要があります。SVMにバケットを追加し、その新しいバケットを監査対象とする場合は、この手順でバケットを選択する必要があります。また、S3監査が有効になっているSVM内に監査対象外のバケットを含めることもできます。

監査構成は、 `vserver object-store-server audit event-selector delete` コマンドによって削除されるまでバケットに対して保持されます。

手順

1. S3の監査対象にするバケットを選択します。

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`：監査するイベント アクセスのタイプを指定します： `read-only`、 `write-only`または `all`（デフォルトは `all`）。
   - `-permission`：監査するイベント権限のタイプを指定します： `allow-only`、 `deny-only`または `all`（デフォルトは `all`）。

例

次の例は、読み取り専用アクセスで許可されたイベントのみをログに記録するバケットの監査設定を作成します。

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

ONTAP S3監査設定を変更する

個々のバケット、またはSVM内で監査対象として選択されているすべてのバケットについて、監査設定を変更することができます。

監査設定を変更する対象	入力する内容
個々のバケット	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`]` [*`parameters to modify`*]
SVM内のすべてのバケット	`vserver object-store-server audit modify -vserver` *`svm_name`* [*`parameters to modify`*]

例

次の例は、書き込み専用のアクセス イベントのみを監査するように個々のバケットの監査設定を変更します。

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

次の例では、SVM 内のすべてのバケットの監査設定を変更して、ログ サイズの制限を 10MB に変更し、ローテーション前に 3 つのログ ファイルを保持するようにしています。

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3監査設定を表示する

監査設定が完成したら、監査が適切に設定されて有効になっていることを確認できます。クラスタ内のすべてのオブジェクト ストアの監査設定に関する情報を表示することもできます。

タスク概要

バケットとSVMの監査設定に関する情報を表示できます。

- バケット： `vserver object-store-server audit event-selector show`コマンドを使用する

  このコマンドをパラメータなしで実行すると、オブジェクト ストアの監査設定があるクラスタ内のすべてのSVMのバケットについて、次の情報が表示されます。

  - SVM名
  - バケット名
  - アクセスと権限の値
- SVM： `vserver object-store-server audit show`コマンドを使用する

  このコマンドをパラメータなしで実行すると、オブジェクト ストアの監査設定があるクラスタ内のすべてのSVMについて、次の情報が表示されます。

  - SVM名
  - 監査の状態
  - ターゲット ディレクトリ

    `-fields`パラメータを指定して、表示する監査構成情報を指定できます。

手順

S3の監査設定に関する情報を表示します。

変更対象	入力する内容
バケット	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVM	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

例

次の例は、単一のバケットの情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

次の例は、SVMのすべてのバケットの情報を表示します。

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

次の例は、すべてのSVMの名前、監査の状態、イベントの種類、ログ形式、およびターゲット ディレクトリを表示します。

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

次の例は、すべてのSVMの名前、および監査ログの詳細情報を表示します。

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                              Rotation
      Vserver     File Size Rotation Schedule           Limit
      ----------- --------- ------------------------- --------
      vs1         100MB     -                         0
```

次の例は、すべてのSVMに関するすべての監査設定情報をリスト形式で表示します。

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                           Log Format: json
                  Log File Size Limit: 100MB
         Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

著作権に関する情報

商標に関する情報