S3オブジェクトストレージの管理

ONTAP 9

NetApp
December 20, 2024

目次

S3オブジェクトストレージの管理

ONTAP 9でのS3サポートの詳細

ONTAP S3設定の詳細

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することができます。ONTAP System Managerなどの使い慣れた管理ツールを使用して、ONTAPの開発と運用用に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、ONTAPのStorage Efficiencyとセキュリティを活用できます。

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。System Managerを使用してS3を有効にしてバケットを作成すると、ONTAPでは設定を簡易化するためにベストプラクティスのデフォルトが選択されます。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。CLIからS3サーバとバケットを設定した場合でも、必要に応じてSystem Managerで管理できます。その逆も可能です。

System Managerを使用してS3バケットを作成すると、ONTAPによってデフォルトのパフォーマンスサービスレベルがシステムで使用可能な最も高いレベルに設定されます。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、事前に定義されたアダプティブQoSポリシーグループです。デフォルトのいずれかのサービスレベルの代わりに、カスタムのQoSポリシーグループを指定することも、ポリシーグループを指定しないこともできます。

事前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 * ：最高レベルのレイテンシと最高レベルのパフォーマンスを求められるアプリケーションに使用されます。
- * パフォーマンス * ：適度なパフォーマンスとレイテンシが求められるアプリケーションに使用します。
- * Value * ：スループットと容量がレイテンシよりも重視されるアプリケーションに使用します。
- * カスタム * ：カスタムの QoS ポリシーを指定するか、 QoS ポリシーなしで指定します。

[階層化に使用する *] 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、階層化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選択しようとします。

も参照してください"アダプティブQoSポリシーグループを使用する"。

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使用するローカル階層にこのバケットをプロビジョニングしようとします。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からローカル階層（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ことを検討してください。CLIから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を指定できるようにするには、CLIを使用する必要があります。

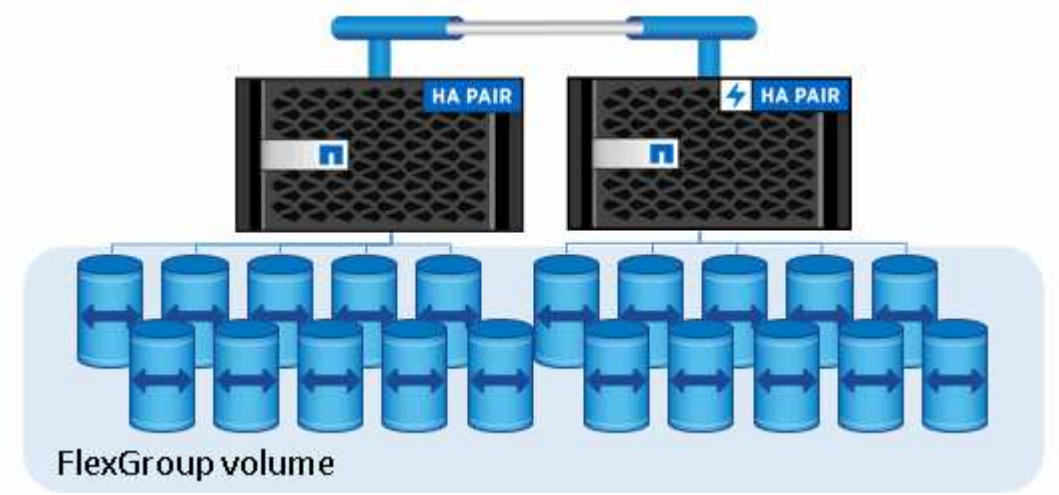
Cloud Volumes ONTAPでのS3バケットの設定

Cloud Volumes ONTAPからバケットを提供する場合は、使用するアグリゲートが1つのノードだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。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、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与える可能性があります。そのため、Cloud Volumes ONTAP環境ではを推奨しCLIからS3バケットを設定するます。

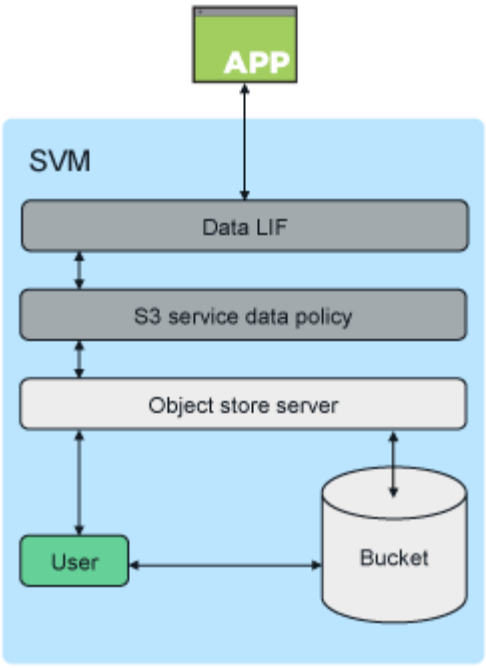
それ以外の場合、Cloud Volumes ONTAP上のS3サーバは、Cloud Volumes ONTAPでオンプレミス環境と同じように設定および維持されます。

FlexGroupボリュームを使用したONTAP S3アーキテクチャ

ONTAPのバケットの基盤となるアーキテクチャはです。は、複数のコンスティチュエントメンバーボリュームで構成される "FlexGroupボリューム"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、許可されたユーザとクライアントアプリケーションを通じて提供されます。



バケットがFabricPoolエンドポイントなどのS3アプリケーション専用に使用されている場合、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たS3プロトコルも有効にできます "マルチプロトコルNASボリューム" 。マルチプロトコルNASボリュームでS3プロトコルが有効になっている場合、クライアントアプリケーションはNFS、SMB、および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。

バケット制限

最小バケットサイズは95GBです。+最大バケットサイズは、FlexGroupの最大サイズである60PBに制限されています。

FlexGroupボリュームあたり1、000バケット、またはクラスタあたり12、000バケット（12個のFlexGroupボリュームを使用）の制限があります。

ONTAP 9.14.1以降での**FlexGroup**の自動サイジング

ONTAP 9.14.1以降では、デフォルトのFlexGroupサイズは基盤となるバケットのサイズに基づいて決まります。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張または縮小されます。

たとえば、初期のBucket_Aが100GBにプロビジョニングされている場合、FlexGroupは100GBにシンプロビジョニングされます。Bucket_B（300GB）とBucket_C（500GB）の2つのバケットを追加で作成すると、FlexGroupボリュームは900GBに拡張されます。

（100GBのBucket_A、300GBのBucket_B、500GBのBucket_C = 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以前で修正されたデフォルトの**FlexGroup**サイズ

バケットの拡張用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合計使用済み容量が、クラスタ上の使用可能なストレージアグリゲートに基づくFlexGroupの最大容量の33%未満である必要があります。この要件を満たすことができない場合、作成される新しいバケットは、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サイズは環境に基づいてデフォルトサイズに固定されていました。

- 1.6PB（ONTAP）
- ONTAP Selectで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ための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に縮小します。

たとえば、300TBの環境では、200TBのFlexGroupボリュームが自動的にプロビジョニングされます（1.6PB、800TB、400TBのFlexGroupボリュームは、環境にしては大きすぎます）。

ONTAP S3の主なユースケース

ONTAP S3サービスへのクライアントアクセスの主なユースケースは次のとおりです。

- FabricPoolを使用してアクセス頻度の低いデータをONTAP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。内のバケットへの階層化、または上のバケットへの階層化 "ローカルクラスタ"の "リモートクラスタ"両方がサポートされます。ONTAP S3への階層化により、使用頻度の低いデータに低コストのONTAPシステムを使用し、新しいフラッシュ容量にかかるコストを削減できます。追加のFabricPoolライセンスや新しいテクノロジを管理する必要はありません。
- 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たS3プロトコルも有効にできます "マルチプロトコルNASボリューム" 。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、およびSMB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るため、さまざまなユースケースが開かれます。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ことです。

> ONTAP S3は、既存のONTAPクラスタで追加のハードウェアや管理作業を行わずにS3機能を有効にする場合に適しています。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のあらゆる操作、高度なILM機能、またはONTAPベースのシステムでは達成できない容量を活用する必要があるネイティブのS3アプリケーションに推奨されます。詳細については、を参照して"StorageGRID のドキュメント"ください。

関連情報

"FlexGroupホリユウムノカンリ"

計画

ONTAPのバージョンとプラットフォームでS3オブジェクトストレージをサポート

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、ライセンスをインストールする必要があります。S3ライセンスはゼロコストライセンスですが、ONTAP 9.8にアップグレードするシステムにインストールする必要があります。S3ライセンスは、NetAppサポートサイトのからダウンロードできます "マスターライセンスキーページ" 。

新しいONTAP 9.8以降のシステムにはS3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は、Cloud Volumes ONTAPでオンプレミス環境と同じように設定および機能しますが、例外が1つあります。

- Cloud Volumes ONTAPでバケットを作成する場合は、CLIの手順を使用して、基盤となるFlexGroupボリュームが単一ノードのアグリゲートのみを使用するようにしてください。複数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、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響します。

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

NetApp ONTAP 対応の Amazon FSX

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によるS3のサポート

ONTAP 9 .14.1以降では、MetroCluster IP構成およびFC構成で、ミラーされたアグリゲート内のSVMでS3オブジェクトストレージサーバを有効にすることができます。

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にある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構成での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、を参照してください"ミラーされていないアグリゲートに関する考慮事項"。

ONTAP 9 .7でのS3のパブリックプレビュー

S3オブジェクトストレージは、ONTAP 9 .7で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の時点では更新されません。本番環境でS3オブジェクトストレージをサポートするのは、ONTAP 9 .8以降のリリースのみです。

9.7のパブリックプレビューで作成されたS3バケットは、ONTAP 9 .8以降で使用できますが、強化された機能は利用できません。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、機能サポート、セキュリティ、パフォーマンスを強化するために、バケットの内容を9.8のバケットに移行する必要があります。

ONTAP S3でサポートされる操作

ONTAP S3の操作は、以下に示す以外は標準のS3 REST APIでサポートされます。詳細については、を参照して"Amazon S3 APIリファレンス』を参照してください"ください。

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 9 .11.1
DeleteBucket	ONTAP 9 .11.1
DeleteBucketPolicy	ONTAP 9 12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1以降*有効期限アクションのみがサポートされています
GetBucketLocation	ONTAP 9 10.1
GetBucketPolicy	ONTAP 9 12.1
ヘッドバケット	ONTAP 9.8
ListBuckets	ONTAP 9.8
ListBucketVersioning	ONTAP 9 .11.1
ListObjectVersions	ONTAP 9 .11.1
PutBucket	• ONTAP 9 .11.1 • ONTAP 9.8 - ONTAP REST APIのみでサポート
PutBucketLifecycleConfiguration	ONTAP 9.13.1以降*有効期限アクションのみがサポートされています
PutBucketPolicy	ONTAP 9 12.1

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には、 `x-amz-meta-<key>.`

  例： `x-amz-meta-project: ontap_s3`。

- GetObjectとHeadObjectでは、ユーザ定義のメタデータが返されます。
- 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でオブジェクトのバージョン管理と次のONTAP APIによる関連操作がサポートされます。

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

オブジェクトの処理	**ONTAP**でのサポート開始
AbortMultipartUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
CopyObject	ONTAP 9 12.1
CreateMultipartUpload	ONTAP 9.8
deleteObject	ONTAP 9.8
オブジェクトの削除	ONTAP 9 .11.1
DeleteObjectTagging	ONTAP 9 .9.1
GetBucketVersioning	ONTAP 9 .11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetention	ONTAP 9 .14.1
GetObjectTagging	ONTAP 9 .9.1
ヘッドオブジェクト	ONTAP 9.8
ListMultipartUpload	ONTAP 9.8
ListObjects	ONTAP 9.8
ListObjectsV2	ONTAP 9.8
ListBucketVersions	ONTAP 9 .11.1
ListParts	ONTAP 9.8
PutBucketVersioning	ONTAP 9 .11.1
PutObject	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9 .14.1
PutObjectRetention	ONTAP 9 .14.1
PutObjectTagging	ONTAP 9 .9.1
パーツのアップロード	ONTAP 9.8
パーツコピーをアップロード	ONTAP 9 12.1

グループポリシー

これらの処理はS3に固有の処理ではなく、一般にIdentity and Management（IAM）プロセスに関連しています。ONTAPはこれらのコマンドをサポートしていますが、IAM REST APIは使用しません。

- ポリシーの作成
- AttachGroupポリシー

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**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（保持期間が定義されていないロック）はサポートされません。

- GetObjectLockConfigurationの略
- 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ています。

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9 12.1

ONTAP 9 .12.1では、バケットポリシーのサポートとオブジェクトのコピー機能が追加されています。

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- パーツコピーをアップロード

ONTAP 9 .11.1

ONTAP 9 .11.1では、バージョン管理、事前定義されたURL、チャンクアップロードがサポートされるようになりました。また、S3 APIを使用したバケットの作成や削除など、一般的なS3操作もサポートされるようになりました。

- ONTAP S3で、x-amz-content-sha256を使用したチャンクアップロードの署名要求がサポートされるようになりました。streaming-aws4-hmac-sha256-payload
- ONTAP S3では、クライアントアプリケーションが事前定義されたURLを使用してオブジェクトを共有したり、他のユーザがユーザクレデンシャルを必要とせずにオブジェクトをアップロードしたりできるようになりました。
- CreateBucket
- DeleteBucket
- GetBucketVersioning
- ListBucketVersions
- PutBucket
- PutBucketVersioning
- オブジェクトの削除
- ListObjectVersions

> 基盤となるFlexGroupは最初のバケットがにな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、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および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、「<key>」を使用したキーと値のペアが追加されました。例：「x-amz-meta-project：ONTAP _s3」。
- GetObjectとHeadObjectがユーザ定義のメタデータを返すようになりました。

タグはバケットでも使用できます。メタデータとは異なり、タグは次のコマンドを使用してオブジェクトから独立して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、次の表に記載されている場合を除き、ONTAPの他の機能と正常に連携します。

フィーチャー領域（ **Feature area** ）	サポート対象	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
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 • SnapMirrorクラウド • SVMディザスタリカバリ • SyncMirror
暗号化	• NetAppアグリゲート暗号化（NAE） • NetAppボリューム暗号化（NVE） • NetAppストレージ暗号化（NSE） • TLS/SSL	• SLAG
Storage Efficiency	• 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化 • 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
ストレージ仮想化	-	NetApp FlexArray仮想化

フィーチャー領域（ **Feature area** ）	サポート対象	サポート対象外
Quality of Service（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） • "バケットライフサイクル管理" （ONTAP 9.13.1以降）	• FlexCacheホリユウム • FPolicy • qtree • クォータ

NetAppがONTAP S3バケットに推奨するサードパーティソリューション

NetAppは、ONTAP S3で使用する以下のサードパーティソリューションを検証しました。お探しのソリューションがリストにない場合は、NetAppの営業担当者にお問い合わせください。

ONTAP S3で検証済みの他社製ソリューション

NetAppは、それぞれのパートナーと協力してこれらのソリューションをテストしました。

- Amazon SageMaker
- Apache Hadoop S3Aクライアント
- Apache Kafka
- Commvault（V11）
- コンフルエントカフカ
- レッドハットキー
- Rubrik
- スノーフレーク
- トリノ
- Veeam（V12）

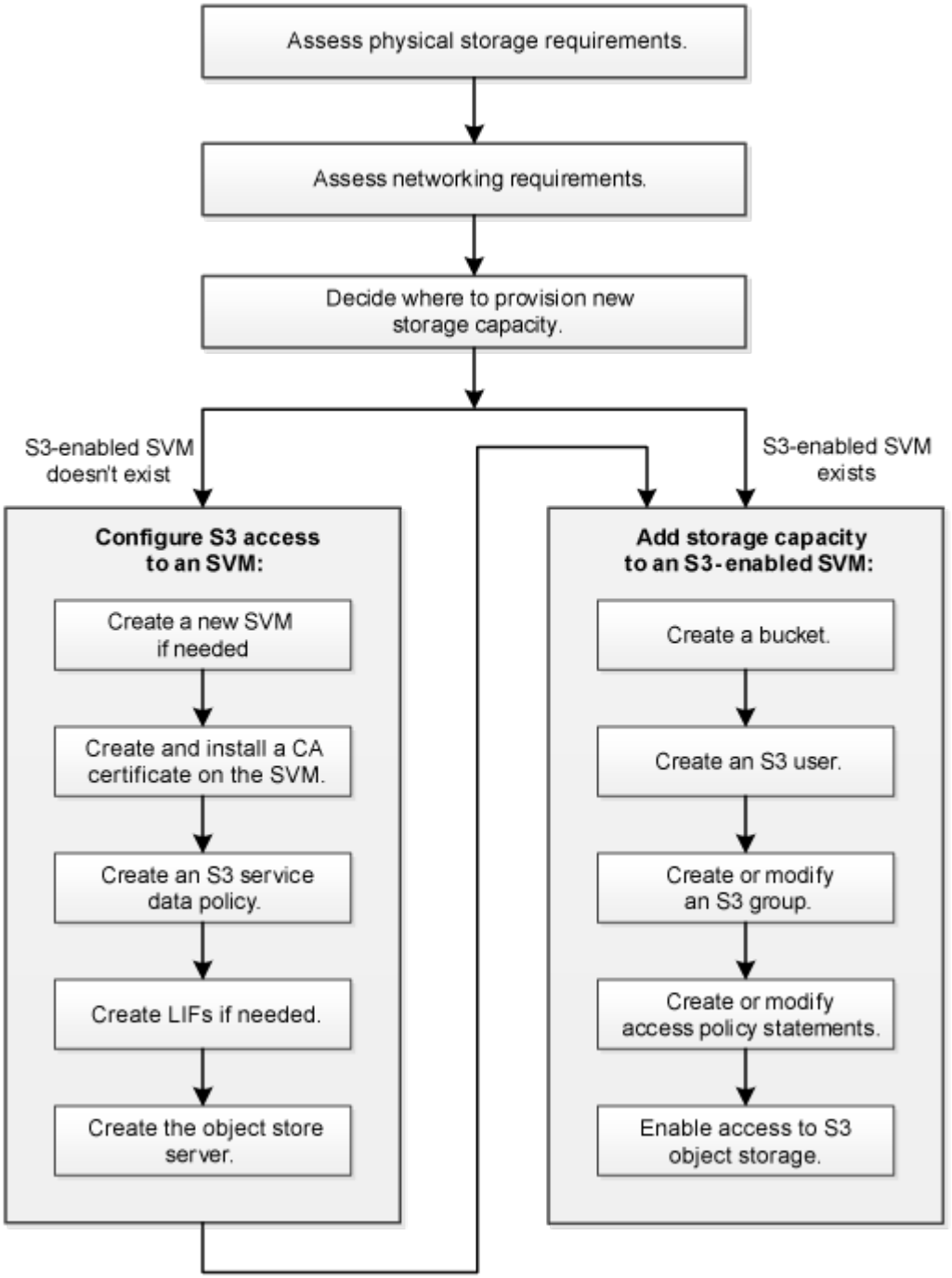
設定

S3の設定プロセスの概要

ONTAP S3の設定ワークフロー

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、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。

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



ONTAP S3の物理ストレージ要件の評価

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用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、必要なタイプと場所で新しいアグリゲートを作成できます。

タスクの内容

S3対応SVMにS3バケットを作成する場合、そのバケットはFlexGroupボリューム "自動作成" でサポートされます。使用するアグリゲートとFlexGroupコンポーネントをONTAP Selectで自動的に選択することも（デフォルト）、使用するアグリゲートとFlexGroupコンポーネントを自分で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する必要があります。詳細：

- "FlexGroupホリユウムノカンリ"
- "ネットアップテクニカルレポート 4571-A ：『 NetApp ONTAP FlexGroup Volume Top Best Practices 』"

Cloud Volumes ONTAPからバケットを提供する場合は、使用するアグリゲートが1つのノードだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。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、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与える可能性があります。詳細はこちらをご覧ください "Cloud Volumes ONTAP 用バケットの作成"。

ONTAP S3サーバを使用して、高パフォーマンス階層と同じクラスタにローカルのFabricPool大容量階層を作成できます。これは、 SSD ディスクが 1 つの HA ペアに接続されている状況で、別の HA ペアの HDD ディスクに階層化 _cold_data を設定する場合などに便利です。このユースケースでは、S3サーバとローカルの大容量階層を含むバケットを高パフォーマンス階層とは別のHAペアに配置する必要があります。ローカル階層化は、1ノードクラスタと2ノード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
   ```

   十分なスペースまたは必要なノードの場所を備えたアグリゲートがある場合は、その名前をS3構成用に記録します。

   ```
   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. 十分なスペースや必要なノードの場所を備えたアグリゲートがない場合は、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 `storage aggregate add-disks`か、コマンドを使用して新しいアグリゲートを作成 `storage aggregate create`します。

ONTAP S3のネットワーク要件の評価

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

タスクの内容

リモートのFabricPool容量（クラウド）階層とリモート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。クラスタピアリングは必要ありません。

ローカル FabricPool の大容量階層には、システム SVM （「 Cluster 」）を使用する必要がありますが、 LIF を設定する方法は 2 つあります。

- クラスタLIFを使用できます。

  このオプションでは、LIFをこれ以上設定する必要はありませんが、クラスタLIFのトラフィックが増加します。また、ローカル階層に他のクラスタからはアクセスできなくなります。

- データLIFとクラスタ間LIFを使用できます。

  このオプションでは、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. 使用可能な物理ポートと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も速いポートを使用してください。
   - 最大限のパフォーマンスを実現するには、データネットワーク内のすべてのコンポーネントのMTU設定を同じにする必要があります。

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、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3サブネットに属するIPアドレスのプールが含まれています。サブネットは、コマンドを使用して作成し `network subnet create`ます。

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、コマンドを使用してIPv6を有効にできます `network options ipv6 modify`。

新しい**ONTAP S3**ストレージ容量のプロビジョニング先を決定する

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のどちらのSVMに配置するかを決定する必要があります。この決定によって、ワークフローが決まります。

選択肢

- 新しいSVMまたはS3が有効になっていない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用のSVMの作成"

  "S3用のバケットを作成"

  S3はNFSやSMBを使用するSVMに共存できますが、次のいずれかに該当する場合は新しいSVMを作成します。

  - クラスタでS3を初めて有効にする場合。
  - クラスタ内の既存の SVM で S3 サポートを有効にするのが望ましくない場合。
  - クラスタ内に 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 サーバが必要な場合。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に最初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用のバケットを作成"

SVMへのS3アクセスの設定

ONTAP S3用の**SVM**の作成

S3はSVM内で他のプロトコルと共存できますが、ネームスペースやワークロードを分離

するために新しいSVMを作成することもできます。

タスクの内容

SVMからS3オブジェクトストレージのみを提供する場合は、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を設定することもできます。

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

例 **1.** 手順

System Manager

クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。S3サーバのFQDNの1文字目をバケット名にすることはできません。

インターフェイスロールデータのIPアドレスを入力する準備をしておく必要があります。

外部CA署名証明書を使用している場合は、この手順の実行中に入力するように求められます。また、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Storage VMを追加します。[* Storage（ストレージ）]>[Storage VMs]をクリックし、[* Add（追加）]をクリックします。

      既存のStorage VMがない新しいシステムの場合は、*ダッシュボード>プロトコルの設定*をクリックします。

   既存のStorage VMにS3サーバを追加する場合は、**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、 S3 *の下をクリックし ⚙ ます。

   a. Enable S3 * をクリックし、 S3 Server Name を入力します。

   b. 証明書のタイプを選択します。

      システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   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Storage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。

   - 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な場合は、[*ストレージ]、[Storage VMs]の順にクリックし、Storage 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になっていることを確認します。

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

   サポートされていない場合は、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>
```

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

3. 新しく作成したSVMの設定とステータスを確認します。

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

`Vserver Operational State`フィールドには状態が表示されている必要があり `running`ます。状態が表示された場合は `initializing`、ルートボリュームの作成などの中間処理が失敗したため、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でSVMが作成され、自動的に起動されて状態になっていることを示しています running。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あるため、ルートボリュームは作成時にエクスポートされません。デフォルトでは、vsadminユーザアカウントが作成され、状態がになってい `locked`ます。vsadminロールは、デフォルトのvsadminユーザアカウントに割り当てられます。

```
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クライアントからS3対応SVMへのHTTPSトラフィックを有効にするには、認証局（CA）証明書が必要です。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された関係が作成されます。ONTAPを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使用する前に、CA証明書をインストールしておく必要があります。

タスクの内容

HTTPのみを使用するようにS3サーバを設定したり、CA証明書を必要とせず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階層化では、CA証明書は必要ありません。

この手順では、ONTAP自己署名証明書を作成してインストールします。ONTAPで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からの署名済み証明書を使用することを推奨します。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。

"カンリシヤニンシヨウトRBAC"

その他の設定オプションについては、マニュアルページを参照して `security certificate`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`*

   オプションは `-type root-ca`、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。

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

   デフォルトの証明書サイズは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に保存しておきます。

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]`

   > `-common-name`署名要求のパラメータには、S3サーバ名（FQDN）を指定する必要があります。

   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。

   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するように求められます。

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`--ステップ1で入力したCAの共通名。
   - `-ca-serial`--ステップ1のCAシリアル番号。たとえば、CA証明書の名前が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限は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用に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
```

ONTAP S3サービスデータポリシーを作成

S3のデータサービスと管理サービスの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。

タスクの内容

データLIFとクラスタ間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。ローカル階層化のユースケースにクラスタ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、および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`ONTAP S3を有効にするために必要なサービスはサービスと `data-s3-server`サービスだけですが、必要に応じて他のサービスも含めることができます。

ONTAP S3用のデータ**LIF**の作成

新しいSVMを作成した場合は、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の管理 `up`ステータスがに設定されている必要があります。
- 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、そのサブネットがすでに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3サブネットに属するIPアドレスのプールが含まれています。コマンドを使用して作成し `network subnet create`ます。

- 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するLIF（data-s3-server）と管理処理に使用するLIF（management-https）を別 々 に配置することを推奨します。同じLIFで両方のサービスを有効にしないでください。
- 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必要があります。他のLIFのIPアドレスがDNSレコードに指定されている場合、ONTAP S3要求が他のサーバから処理され、予期しない応答やデータの損失が発生する可能性があります。

タスクの内容

- 同じネットワークポートにIPv4とIPv6の両方のLIFを作成できます。
- クラスタに多数のLIFがある場合は、コマンドを使用してクラスタでサポートされるLIFの容量を確認するか、コマンド（advanced権限レベル）を使用して各ノードでサポートされるLIFの容量を `network interface capacity details show`確認できます `network interface capacity show`。
- リモートのFabricPool容量（クラウド）階層化を有効にする場合は、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、LIFに対してコマンドを実行したときにLIFが戻るノードです `network interface revert`。

  オプションを使用して、LIFをホームノードおよびホームポートに自動的にリバートするかどうかを指定することもできます `-auto-revert`。

- `-home-port`は、LIFに対してコマンドを実行したときにLIFが戻る物理ポートまたは論理ポートです `network interface revert`。
- オプションと `-netmask`オプションでIPアドレスを指定することも、オプションでサブネットからの割り当てを有効にすることも `-subnet_name`できます `-address`。
- 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（サブネットを使用せずに）割り当てる場合、クライアントまたはドメインコントローラが別のIPサブネットにあるときに、ゲートウェイへのデフォルトルートの設定が必要になることがあります。 `network route create`のマニュアルページには、SVM内での静的ルートの作成に関する情報が記載されています。
- オプションには `-firewall-policy`、LIFのロールと同じデフォルトを使用し `data`ます。

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

  > ONTAP 9 10.1以降では、ファイアウォールポリシーが廃止され、LIFのサービスポリシーに全面的に置き換えられました。詳細については、を参照してください "LIFのファイアウォールポリシーを設定する"。

- `-auto-revert`起動時、管理データベースのステータスが変わったとき、ネットワーク接続が確立されたときなどの状況で、データLIFがホームノードに自動的にリバートされるかどうかを指定できます。デフォルトの設定はです `false`が、環境内のネットワーク管理ポリシーに応じてに設定できます `false`。
- オプションは、 `-service-policy`作成したデータサービスポリシーと管理サービスポリシー、およびその他の必要なポリシーを指定します。

2. オプションでIPv6アドレスを割り当てる場合 `-address`は、次の手順を実行します。

   a. コマンドを使用して `network ndp prefix show`、さまざまなインターフェイスで学習されたRAプレフィックスのリストを表示します。

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

   b. 形式を使用し `prefix:id`て、IPv6アドレスを手動で作成します。

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

   を生成するには `id`、ランダムな64ビット16進数を選択します。

3. 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 `network interface show`。
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	使用方法
IPv4アドレス	`network ping`
IPv6アドレス	`network ping6`

例

次のコマンドは、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 `my-S3-policy` 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。datalif1とdatalif3のデータLIFにはIPv4アドレスを設定し、datalif4にはIPv6アドレスを設定しています。

```
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.
```

ONTAP S3によるリモート**FabricPool**階層化用のクラスタ間**LIF**の作成

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は、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の管理 `up`ステータスがに設定されている必要があります。
- 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。

タスクの内容

クラスタ間LIFは、ローカルのファブリックプールの階層化や外部のS3アプリケーションへの提供には必要ありません。

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、のネットワークポートを示してい `cluster01`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
   ```

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
   ```

   次の例は、クラスタ間LIFと `cluster01_icl02`を作成し `cluster01_icl01`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
```

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、インタークラスタLIFおよび `cluster01_icl02`ポート上の `e0c`ポートがそのポートにフェイルオーバーする `e0d`ことを示しています `cluster01_icl01`。

```
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
```

ONTAP S3オブジェクトストアサーバの作成

ONTAPオブジェクトストアサーバは、ONTAP NASサーバやSANサーバが提供するファイルストレージやブロックストレージとは対照的に、S3オブジェクトとしてデータを管理します。

開始する前に

クライアントがS3アクセスに使用するFully Qualified Domain Name（FQDN；完全修飾ドメイン名）としてS3サーバ名を入力する準備をしておく必要があります。FQDNの1文字目をバケット名にすることはできません。仮想ホスト形式を使用してバケットにアクセスする場合は、サーバ名がとして使用されます `mydomain.com`。たとえば、 `bucketname.mydomain.com`です。

自己署名CA証明書（前の手順で作成）または外部CAベンダーによって署名され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階層化では、CA証明書は必要ありません。

タスクの内容

オブジェクトストアサーバを作成すると、UIDが0のrootユーザが作成されます。このrootユーザに対してアクセスキーやシークレットキーは生成されません。ONTAP管理者は、このユーザのアクセスキーとシークレットキーを設定するコマンドを実行する必要があります `object-store-server users regenerate-keys`。

> NetAppのベストプラクティスとして、このrootユーザは使用しないでください。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へのフルアクセスが付与されます。

その他の設定オプションおよび表示オプションについては、マニュアルページを参照して `vserver object-store-server`ください。

例 **2.** 手順

System Manager

この手順は、既存のStorage VMにS3サーバを追加する場合に使用します。新しいStorage VMにS3サーバを追加する方法については、を参照してください"S3用のストレージSVMを作成します"。

インターフェイスロールデータのIPアドレスを入力する準備をしておく必要があります。

1. 既存のStorage VMでS3を有効にします。
   a. Storage VMを選択します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**を選択して[設定]をクリックし、[S3]*の下をクリックします 。
   b. Enable S3 * をクリックし、 S3 Server Name を入力します。
   c. 証明書のタイプを選択します。

      システムで生成された証明書を選択した場合でも独自の証明書を選択した場合でも、クライアントアクセスに必要になります。

   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Storage VMの作成を確認した時点で証明書の情報が表示されます。[ダウンロード] をクリックし、クライアントアクセス用に保存します。
   - 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な場合は、 [* ストレージ] 、 [Storage VMs] の順にクリックし、 Storage 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。

   - ローカルの階層化を設定する場合は、SVM名にデータSVM名またはシステムSVM（クラスタ）名を指定できます。
   - 証明書名は、サーバCA証明書（中間またはルートCA証明書）ではなく、サーバ証明書（エンドユーザまたはリーフ証明書）の名前にする必要があります。
   - HTTPSはポート443ではデフォルトで有効になっています。ポート番号はオプションで変更できます `-secure-listener-port`。

     HTTPSを有効にすると、SSL/TLSと正しく統合するために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TLS 1.3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、サーバはポート80でリスンします。オプションを使用して有効にすることも、オプションを使用してポート番号を変更する `-listener-port`こともできます `-is-http-enabled`。

     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経由で送信されます。

2. S3が設定されていることを確認します。

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

例

このコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。

```
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にストレージ容量を追加する

ONTAP S3バケットを作成する

S3オブジェクトは_Buckets_に保持されます。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。

タスクの内容

- ONTAP 9 14.1以降では、S3 FlexGroupボリュームでバケットが作成されたときに、ボリュームの自動サイズ変更が有効になりました。これにより、既存および新規のFlexGroupボリュームでバケットを作成する際の過剰な容量割り当てが解消されます。FlexGroupボリュームのサイズは、次のガイドラインに基づいて、必要な最小サイズに変更されます。必要な最小サイズは、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、新しいバケットの作成時にS3 FlexGroupボリュームが作成されると、必要な最小サイズでFlexGroupボリュームが作成されます。
  - S3 FlexGroupボリュームがONTAP 9 .14.1より前に作成された場合は、ONTAP 9のあとに最初に作成または削除されたバケットが表示されます。14.1では、FlexGroupボリュームのサイズが必要な最小サイズに変更されます。
  - S3 FlexGroupボリュームがONTAP 9 .14.1より前に作成されたボリュームで、必要な最小サイズがすでに設定されている場合は、ONTAP 9 .14.1以降のバケットの作成または削除によってS3 FlexGroupボリュームのサイズが維持されます。

- 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 QoS ポリシーグループで、 *value*、*performion*、 _extreme デフォルトレベルがあります。デフォルトのストレージサービスレベルの代わりに、カスタムの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、を参照してください"ストレージサービスの定義"。パフォーマンス管理の詳細については、を参照してください"パフォーマンス管理"。ONTAP 9 8以降では、ストレージのプロビジョニング時にデフォルトでQoSが有効になります。プロビジョニングプロセス中またはあとで、QoSを無効にしたり、カスタムのQoSポリシーを選択したりできます。
- ローカル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の場合は、S3対応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にバケットを作成した場合、そのバケットはローカルの階層化にのみ使用できます。
- ONTAP 9 .14.1以降では、この機能を"MetroCluster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作成する"使用できます。
- CLIでバケットを作成する場合は、次の2つのプロビジョニングオプションがあります。
  - ONTAP Selectを基盤となるアグリゲートとFlexGroupコンポーネントにする（デフォルト）
    - ONTAPでは、アグリゲートが自動的に選択されることで、最初のバケットのFlexGroupボリュームが作成および設定されます。プラットフォームで使用可能な最も高いサービスレベルが自動的に選択されます。または、ストレージサービスレベルを指定できます。あとでStorage VMに追加するバケットには、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。その場合、ONTAPは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選択しようとします。
  - 使用するアグリゲートとFlexGroupコンポーネントを選択します（advanced権限のコマンドオプションが必要です）。バケットと包含FlexGroupボリュームを作成するアグリゲートを手動で選択し、各アグリゲートのコンスティチュエントの数を指定できます。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すると、そのバケット用に新しいFlexGroupが作成されます。
    - 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、を参照してください FlexGroupホリユウムノカンリ 。

      バケットの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、デフォルトまたはカスタムのQoSポリシーグループは適用されません。これは、コマンドを使用してあとで実行できます `vserver object-store-server bucket modify`。

    リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ vserver-object-store-server-show.html[`vserver object-store-server bucket modify`^]コマンドを参照してください。

注： Cloud Volumes ONTAP からバケットを処理する場合は、CLI手順 を使用してください。使用するノードが1つだけになるように、基盤となるアグリゲートを手動で選択することを強く推奨します。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、レイテンシの問題の影響を受けやすくなるため、パフォーマンスに影響を与え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]`

   ローカルでの階層化を設定する場合は、Storage VMの名前にデータStorage VMまたは（システムStorage VMの名前）を指定できます `Cluster`。

   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

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

   - 階層化

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

     基盤となる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。

   - パラメータは `-aggr-list`、FlexGroupボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

     リスト内の各エントリによって、指定した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。

   - パラメータは `-aggr-list-multiplier`、FlexGroupボリュームの作成時にパラメータで指定したアグリゲートを繰り返し実行する回数を指定します `-aggr-list`。

     パラメータのデフォルト値 `-aggr-list-multiplier`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. バケットの作成を確認します。

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

例

次の例では、Storage VM用のサイズの `1TB`バケットを作成し `vs1`、アグリゲートを指定しています。

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"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する。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] 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 * Save * 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。
        - グループポリシーがすでに有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。

          オブジェクトストレージへのアクセスが無制限になるため、S3 rootユーザを使用してONTAPオブジェクトストレージの管理と権限の共有を行わないでください。代わりに、管理Privilegesを割り当てたユーザまたはグループを作成します。

        - システムで使用可能な最高のサービス品質（パフォーマンス）レベル。
      - [保存]*をクリックして、これらのデフォルト値でバケットを作成します。

追加の権限と制限を設定する

バケットの設定時に*[その他のオプション]*をクリックすると、オブジェクトロック、ユーザ権限、パフォーマンスレベルを設定できます。設定はあとで変更することもできます。

S3 オブジェクトストアを FabricPool の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（階層化データのパフォーマンスが最適な低コストのメディアを使用）を選択することを検討してください。

後でリカバリするためにオブジェクトのバージョン管理を有効にする場合は、*バージョン管理を有効にする*を選択します。バケットでオブジェクトのロックを有効にすると、バージョン管理が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、を参照して "AmazonのS3バケットでのバージョン管理の使用"ください。

9.14.1以降では、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。このライセンスはに含まれてい"ONTAP One"ます。ONTAP Oneよりも前のリリースでは、SnapLockライセンスはSecurity and Compliance Bundleに含まれていました。Security and Compliance Bundleの提供は終了しましたが、引き続き有効です。現在は必須ではありませんが、既存のお客様は選択できます "ONTAP Oneへのアップグレード"。バケットでオブジェクトのロックを有効にする場

合は、を実行して "SnapLockライセンスがインストールされていることの確認"ください。SnapLockライセンスがインストールされていない場合は "インストール"、オブジェクトロックを有効にする前にライセンスが必要です。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ないように保護するには、*[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、すべてのバージョンまたは特定のバージョンのオブジェクトで有効にできます。また、クラスタノードのSnapLock Complianceクロックが初期化されている場合にのみ有効にできます。次の手順を実行します。

1. クラスタのいずれのノードでもSnapLockコンプライアンスクロックが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。クラスタノードの**SnapLock**コンプライアンスクロックを初期化するには、[SnapLockコンプライアンスクロックの初期化]*をクリックします。
2. オブジェクトに対して_ Write Once、Read Many（WORM）_権限を許可する時間ベースのロックを有効にするには、* Governance *モードを選択します。Governance_modeであっても、特定の権限を持つ管理者ユーザがオブジェクトを削除できます。
3. オブジェクトに対してより厳密な削除ルールと更新ルールを割り当てる場合は、*準拠*モードを選択します。このモードのオブジェクトロックでは、指定した保持期間が終了した時点でのみオブジェクトを期限切れにできます。保持期間を指定しないかぎり、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. 一定期間ロックを有効にする場合は、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、を参照してください "新しいバケットのミラーを作成"。

バケットへのアクセスを確認

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、次のように入力して、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バケットサイズを拡張または縮小する

必要に応じて、既存のバケットのサイズを増減できます。

手順

バケットサイズは、System ManagerまたはONTAP CLIを使用して管理できます。

System Manager

1. [Storage]>[Buckets]*を選択し、変更するバケットを探します。
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。

タスクの内容

- デフォルトでは、バケットはミラーされたアグリゲート上にプロビジョニングされます。
- MetroCluster環境でバケットを作成する場合も、で説明したのと同じプロビジョニングガイドラインが"バケットを作成する"適用されます。
- MetroCluster環境では、S3オブジェクトストレージの次の機能は*サポートされません*。
  - SnapMirror S3
  - S3バケットのライフサイクル管理
  - Compliance *モードでのS3オブジェクトのロック

    *ガバナンス*モードでのS3オブジェクトの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。

バケットを作成するプロセス

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]
   ```

   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応じて、オプションをまたは `false`に `true`設定し `-use-mirrored-aggregates`ます。

   > デフォルトでは、この `-use-mirrored-aggregates`オプションはに設定されて `true`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

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

     - 階層化

       オプションを含め `-used-as-capacity-tier true`ます。
   - 基盤となる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。
     - パラメータは `-aggr-list`、FlexGroupボリュームのコンスティチュエントに使用するアグリゲートのリストを指定します。

       リスト内の各エントリによって、指定した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。

   - パラメータは `-aggr-list-multiplier`、FlexGroupボリュームの作成時にパラメータで指定したアグリゲートを繰り返し実行する回数を指定します `-aggr-list`。

     パラメータのデフォルト値 `-aggr-list-multiplier`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. バケットの作成を確認します。

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

例

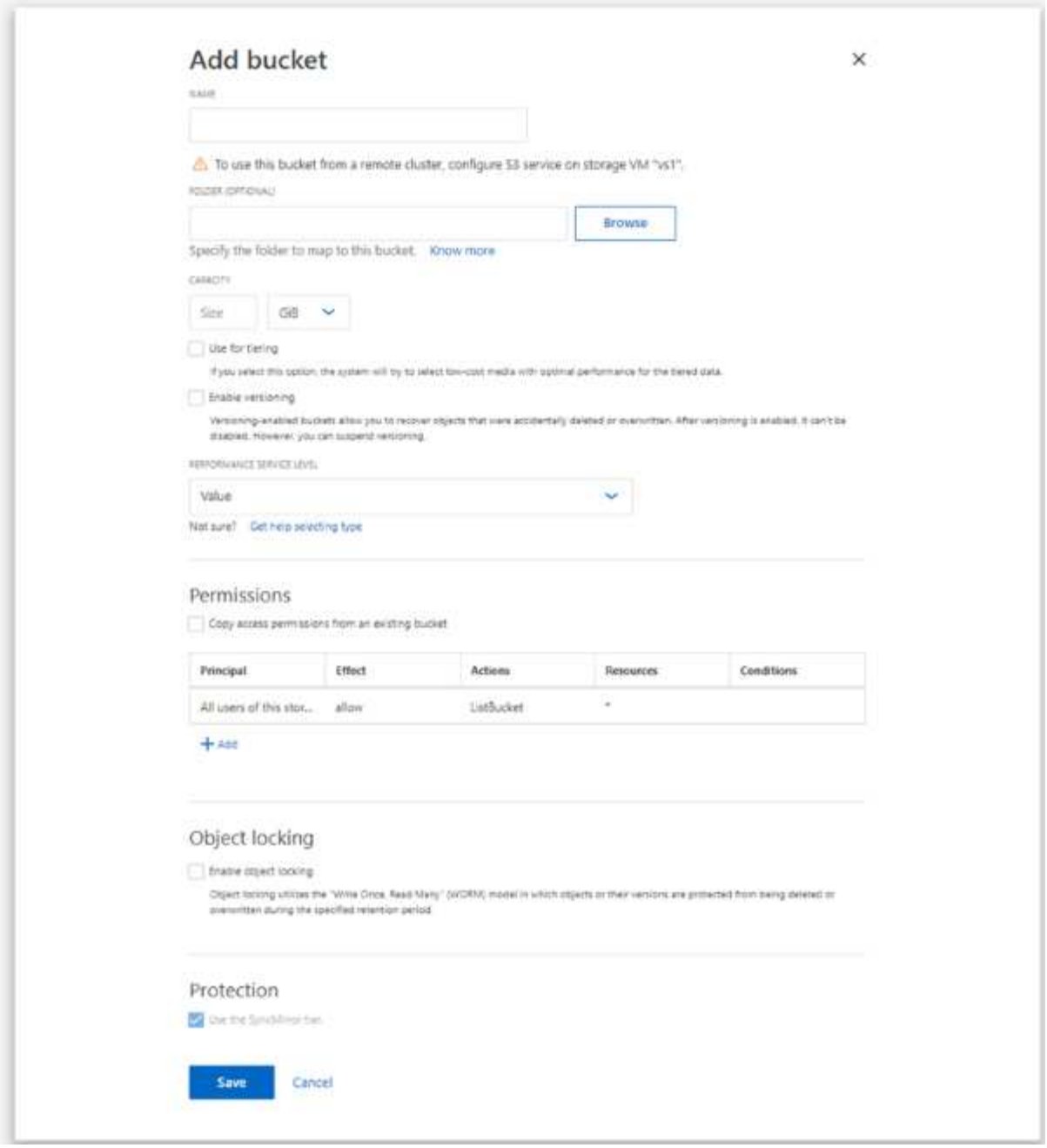
次の例では、ミラーされたアグリゲート上に1TBのSVM vs1のバケットを作成します。

```
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する。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] 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、バケットはミラーされたアグリゲート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[SyncMirror階層を使用する]*ボックスをオフにします（次の図を参照）。



- この時点で * Save * 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。
  - グループポリシーがすでに有効になっていないかぎり、バケットへのアクセスはユーザに許可されません。

> オブジェクトストレージへのアクセスが無制限になるため、S3 rootユーザを使用してONTAPオブジェクトストレージの管理と権限の共有を行わないでください。代わりに、管理Privilegesを割り当てたユーザまたはグループを作成します。

  - システムで使用可能な最高のサービス品質（パフォーマンス）レベル。
- バケットの設定時にユーザの権限やパフォーマンスレベルを設定するには、「 * More Options * 」をクリックします。あとで設定を変更することもできます。

- 権限を設定するために * More Options * を使用する前に、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 の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（階層化データのパフォーマンスが最適な低コストのメディアを使用）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ケーション（別のONTAPシステムまたは外部のサードパーティアプリケーション）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、S3バケット内のオブジェクトライフサイクルを管理するためのライフサイクル管理ルールを作成できます。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、それらのルールを使用してバケットオブジェクトを期限切れにすることができます。これにより、保持要件を満たし、S3オブジェクトストレージ全体を効率的に管理できます。

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。オブジェクトのロックについては、を参照してください"バケットを作成する"。

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。詳細については、を参照してください "S3用のSVMの作成" 。
- MetroCluster構成ではバケットライフサイクル管理ルールがサポートされないことに注意してください。

タスクの内容

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次の削除操作を適用できます。

- 現在のバージョンの削除-このアクションは、ルールで指定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ン管理が有効になっている場合は、S3によって、期限切れになったすべてのオブジェクトが使用できなくなります。バージョン管理が有効になっていない場合は、オブジェクトが永続的に削除されます。CLIアクションはです `Expiration`。
- Deletion of non-current versions - S3が最新でないオブジェクトを完全に削除できるタイミングを指定します。CLIアクションはです `NoncurrentVersionExpiration`。

最新でないバージョンは、現在のバージョンの作成時刻または変更時刻に基づいています。最新でないオブジェクトの削除を遅らせておくと、誤ってオブジェクトを削除または上書きした場合に役立ちます。たとえば、最新でないバージョンが最新でない状態になってから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日の午前10時30分（UTC）に、という名前のオブジェクト（バージョンID `111111`）を作成したとし `photo.gif`ます。2014年1月2日午前11時30分（UTC）に誤って（バージョンID） `111111`を削除する `photo.gif`と、新しいバージョンID（バージョンIDなど）を持つ削除マーカーが作成されます `4857693`。5日以内に元のバージョン（バージョンID `111111`）を復元してから、削除が永続的に行われるようになり `photo.gif`ます。2014年1月8日00:00 UTCに、有効期限のライフサイクルルールが実行され、非最新バージョンになってから5日後に（バージョンID `111111`）が完全に削除され `photo.gif`ます。

- 期限切れ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。バージョン管理が有効なバケットでは、削除マーカーが付いたオブジェクトがオブジェクトの現在のバージョンになります。オブジェクトは削除されず、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に現在のバージョンが関連付けられていない場合、これらのオブジェクトは期限切れになります。CLIアクションはです `Expiration`。
- [Deletion of incomplete multipart uploads]-マルチパートアップロードを実行中のままにする最大時間（日数）を設定します。その後、それらは削除されます。CLIアクションはです `AbortIncompleteMultipartUpload`。

実行する手順は、使用するインターフェイスによって異なります。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では、バケットライフサイクル管理ルールを作成するときに、有効期限アクションタイプごとに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、最初の作成後に変更できます。次の表に、アクションタイプごとに固有のフィールドを示します。

アクションタイプ	一意のフィールド
NonCurrentVersionExpiration	• `-non-curr-days`-最新でないバージョンが削除されるまでの日数 • `-new-non-curr-versions`-保持する最新の非最新バージョンの数
有効期限	• `-obj-age-days`-オブジェクトの現在のバージョンを削除できるまでの作成からの日数 • `-obj-exp-date`-オブジェクトが期限切れになる日付 • `-expired-obj-del-markers`-オブジェクト削除マーカーのクリーンアップ
AbortIncompleteMultipartUpload	• `-after-initiation-days`-アップロードが中止されるまでの開始日数

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のサブセットにのみ適用するには、管理者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。ルールの作成時にこれらの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。

以下の場合は、すべてのフィルタを最初に作成した後_except_に変更できます。+

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

手順

1. コマンドとexpirationアクションタイプの必須フィールドを使用し `vserver object-store-server bucket lifecycle-management-rule create`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オブジェクトを期限切れにできます。S3オブジェクトのライフサイクル管理ルールの追加、編集、削除ができます。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て、別のバケット内のオブジェクトに使用することもできます。アクティブなルールを無効にして、あとで有効にすることができます。

ライフサイクル管理ルールの追加

1. [ストレージ]>[バケット]*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、*[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. [ライフサイクルルールの追加]ページで、ルールの名前を追加します。
6. ルールの範囲を定義します。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. prefix：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。1つのルールに1つのプレフィックスを指定できます。有効なプレフィックスが指定されていない場合、ルールがバケット内のすべてのオブジェクトに適用されます。
   b. tags：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3つまで指定します。フィルタリングには有効なキーのみが使用されます。この値はオプションです。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間でスコープを制限できます。どちらか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. アクションを指定します。
   a. オブジェクトの現在のバージョンを期限切れにする：現在のオブジェクトが作成されてから一定の日数が経過した後、または特定の日付に、すべてのオブジェクトを永続的に使用不可にするルールを設定します。このオプションは、*期限切れのオブジェクト削除マーカーを削除*オプションが選択されている場合は使用できません。
   b. 最新でないバージョンを完全に削除：最新でないバージョンが削除されるまでの日数と、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、つまり現在のオブジェクトが関連付けられていない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を自動的に削除する*[現在のバージョンのオブジェクトを期限切れにする]*オプションを選択すると使用できなくなります。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も、このオプションは使用できません。

d. 未完了のマルチパートアップロードを削除：未完了の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。指定した保持期間内に実行中のマルチパートアップロードが失敗した場合は、完了していないマルチパートアップロードを削除できます。オブジェクトタグをフィルタリングに使用すると、このオプションは使用できなくなります。

e. [保存（ Save ）] 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. [ストレージ]>[バケット]*をクリックします。
2. 有効期限ルールをインポートするバケットを選択します。
3. アイコンをクリックし、*[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. ルールのインポート元の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

編集できるライフサイクル管理操作は、ルールに関連付けられているもののみです。ルールがオブジェクトタグでフィルタされている場合は、**[**期限切れのオブジェクト削除マーカーを削除する**]***オプションと[不完全なマルチパートアップロードを削除する]*オプションは使用できません。

ルールを削除すると、そのルールは以前に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. [ストレージ]>[バケット]*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、*[ライフサイクルルールの管理]*を選択します。
4. 必要なルールを選択します。一度に1つのルールを編集および無効にすることができます。一度に複数のルールを削除できます。
5. 、[削除]、または[無効化]*を選択し、手順を完了します。

ONTAP S3ユーザの作成

特定の権限を持つ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。

始める前に。

S3対応Storage VMがすでに存在している必要があります。

タスクの内容

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。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。

セキュリティを強化するため、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ユーザの作成時にのみ表示され、再度表示することはできません。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ります"を参照してください。

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rootユーザ（UID 0）が作成されます。rootユーザは、すべてのバケットにアクセスできる権限を持つユーザです。NetAppでは、ONTAP S3をrootユーザとして管理するのではなく、特定のPrivilegesでadminユーザロールを作成することを推奨しています。

CLI

1. S3ユーザを作成します。
   `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、キーが有効になる期間をパラメータで定義できます `-key-time-to-live`。保持期間を次の形式で追加して、アクセスキーの有効期限が切れるまでの期間を指定できます `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`。たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、と入力します `P1DT2H3M4S`。指定されていないかぎり、キーは無期限に有効です。

     次の例は、Storage VMに `vs0`という名前のユーザを作成し `sm_user1`、キーの保持期間を1週間に設定します。

```
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。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. Storage > Storage VM* をクリックします。ユーザを追加するStorage VMを選択し、*[設定]*を選択して[S3]の下をクリックします 。
2. ユーザを追加するには、*[ユーザ]>[追加]*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、ユーザに対して作成されるアクセス キーの保持期間を指定できます。キーが自動的に期限切れになるまでの保持期間を、日、時間、分、または秒単位で指定できます。デフォルトでは、キーが無期限に有効であることを示す値がに設定され `0`ます。
5. [保存（ Save ）] をクリックします。ユーザが作成され、そのユーザ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。S3クライアントからのアクセスに必要になります。

次のステップ

- S3グループを作成または変更する

バケットへのアクセスを制御するための**ONTAP S3**ユーザグループの作成または変更

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ことで、バケットへのアクセスを簡易化できます。

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。

タスクの内容

S3グループのユーザには1つのSVM内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ら、バケットポリシーのステートメントにグループ権限を指定すると、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ら、グループ定義でオブジェクトサーバポリシーの名前を指定します。これらのポリシーによって、グループメンバーのバケットとアクセスが決まります。

System Manager

1. Storage VMを編集します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。
2. グループを追加：* Groups を選択し、 Add *を選択します。
3. グループ名を入力し、ユーザのリストから選択します。
4. 既存のグループポリシーを選択するか、ここで追加するか、あとで追加することができます。

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`オブジェクトストアにバケットが1つしかない設定では、オプションは省略できます。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コマンドを使用して追加でき `vserver object-store-server group modify`ます。

ONTAP S3キーを再生成して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ための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、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、を参照してください"S3ユーザの作成"。

System Manager

1. Storage > Storage VM* をクリックし、 Storage VM を選択します。
2. [設定]タブで、* S3 *タイル内をクリックします 。
3. [ユーザ]タブで、アクセスキーがないか、ユーザ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（ Save ）] 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すぐに反映されます。
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。S3クライアントからのアクセスに必要になります。

CLI

1. コマンドを実行して、ユーザのアクセスキーとシークレットキーを再生成し `vserver object-store-server user regenerate-keys`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`たとえば、1日、2時間、3分、4秒の保持期間を入力する場合は、と入力します `P1DT2H3M4S`。

```
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。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または変更

ONTAP S3バケットとオブジェクトストアサーバのポリシーの詳細

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、ユーザやグループの数が多い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する方が簡単です。

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。アクセス制御の範囲は包含バケットであるため、バケットが1つの場合に最も適しています。

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。

タスクの内容

新しいユーザとグループの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。詳細については、のマニュアルページを参照して `vserver object-store-server bucket policy`ください。

ユーザ権限とグループ権限は、バケットの作成時に付与することも、あとで必要に応じて付与することもできます。バケット容量やQoSポリシーグループの割り当てを変更することもできます。

ONTAP 9 .9.1以降では、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場合は、バケットポリシーまたはグループポリシーを使用して、および `PutObjectTagging`の `DeleteObjectTagging`操作を `GetObjectTagging`許可する必要があります。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）によって異なります。

System Manager

手順

1. バケットを編集します。 * Storage > Bucket* をクリックし、目的のバケットをクリックして * Edit * をクリックします。権限を追加または変更するときは、次のパラメータを指定できます。
   - * Principal *：アクセス権を付与するユーザまたはグループ。
   - 影響：ユーザまたはグループへのアクセスを許可または拒否します。
   - * Actions *：特定のユーザまたはグループに対してバケットで許可されているアクション。
   - * Resources *：アクセスが許可または拒否されてい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** および * *bketname* / * _ * 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、 ** _bketname/** _readme.txt * と指定します。
   - * Conditions *（オプション）：アクセス試行時に評価される式。たとえば、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。たとえば、がポリシーの変数として指定されている場合 `${aws:username}`、この変数は要求コンテキストのユーザ名に置き換えられ、そのユーザ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指定するか、または次の1つ以上のリストを指定できます `*`。および `ListMultipartUploadParts。 GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,`

`-principal`	S3ユーザまたはグループのリスト。 • 最大10個のユーザまたはグループを指定できます。 • S3グループを指定する場合は、次の形式で指定する必要があります。`group/group_name`. • `*`には、パブリックアクセス（アクセスキーとシークレットキーを使用しないアクセス）を指定できます。 • プリンシパルを指定しない場合、Storage VM内のすべてのS3ユーザにアクセスが許可されます。
`-resource`	バケットとバケット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。リソースについては、ポリシー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、ポリシーの評価時にコンテキストに応じた値に置き換えられます。

オプションを使用して、テキスト文字列をコメントとして指定することもできます `-sid`。

例

次の例では、Storage VM svm1.example.comと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と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、バケットポリシーの変数を指定できます。次の例は、Storage VMとの`bucket1`サーババケットポリシーステートメントを作成し `svm1`、ポリシーリソースの変数としてを指定します `${aws:username}`。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると `${aws:username}`、はS3処理を実行するユーザに置き換えられます。ユーザ `user1`が操作を実行すると、そのユーザにはAS `bucket1/user1/*`へのアクセスが許可され `bucket1`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の作成または変更

オブジェクトストア内の1つ以上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、複数のバケットにわたるリソースアクセスの管理が簡易化されます。

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。

タスクの内容

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は、ポリシー自体ではなく、グループ定義でプリンシパル（ユーザとグループ）を指定します。

ONTAP S3リソースへのアクセスに関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。

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess

また、新しいカスタムポリシーを作成し、新しいユーザとグループの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。リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ index.html[`vserver object-store-server policy`^]コマンドを参照してください。

ONTAP 9 .9.1以降では、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場合は、バケットポリシーまたはグループポリシーを使用して、および `PutObjectTagging`の `DeleteObjectTagging`操作を `GetObjectTagging`許可する必要があります。

実行する手順は、使用するインターフェイス（System ManagerまたはCLI）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ポリシー*を作成または変更します

手順

1. Storage VMを編集します。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。
2. ユーザーの追加： [* 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、グループのリストから選択します。
   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ときは、次のパラメータを指定できます。

      - Group：アクセスが許可されているグループ。
      - 効果：1つ以上のグループへのアクセスを許可または拒否します。
      - actions：特定のグループに対して1つ以上のバケットで許可されるアクション。
      - Resources：1つ以上のバケット内でアクセスが許可または拒否されたオブジェクトのパスと名前。例：
        - * は、 Storage VM 内のすべてのバケットへのアクセスを許可します。
        - * bucketname * および * 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 * を指定すると、特定のバケット内のオブジェクトへのアクセスが許可されます。
   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ポリシー*を作成または変更します

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指定するか、または次の1つ以上のリストを指定できます `*`。および `ListMultipartUploadParts`。 `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`,`GetBucketAcl`, `GetObjectAcl`, `ListAllMyBuckets`, `ListBucketMultipartUploads`,
`-resource`	バケットとバケット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。

オプションを使用して、テキスト文字列をコメントとして指定することもできます `-sid`。

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のリストの最後に追加され、順番に処理されます。後でステートメントを追加または変更する場合は、ステートメントの設定を変更し `-index`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、を"ONTAPコマンド リファレンス"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の設定

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ました。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素化されます。

外部ディレクトリサービスに属するユーザグループに、ONTAPオブジェクトストレージ環境へのアクセスを提供できます。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イスで、IDおよびアクセス管理（IAM）のデータベースとサービスを提供します。アクセスを提供するには、ONTAP S3環境でLDAPグループを設定する必要があります。アクセスの設定が完了すると、グループ メンバーにONTAP S3バケットに対する権限が付与されます。LDAPの詳細については、を参照してください"LDAPノシヨウホウホウノカイヨウ"。

また、Active Directoryユーザグループを高速バインドモードに設定して、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接続を介して認証できるようにすることもできます。

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前に、次のことを確認してください。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照して "S3用のSVMの作成"
2. そのStorage VMにバケットが作成されている。を参照して "バケットを作成する"
3. Storage VMにDNSが設定されています。を参照して "DNSサービスの設定"
4. LDAPサーバの自己署名ルート認証局（CA）証明書がStorage VMにインストールされている。を参照して "自己署名ルートCA証明書をSVMにインストールする"

5. SVMでTLSを有効にしてLDAPクライアントが設定されている。およびを参照してください"LDAPクライアント設定を作成する""情報を取得するためのLDAPクライアント設定とSVMの関連付け"。

外部ディレクトリサービス用の**S3**アクセスの設定

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

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

リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^]コマンドを参照してください。

2. オブジェクトストアバケットポリシーのステートメントを作成し、アクセスを許可するLDAPグループを設定し `principal`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：次の例は、用のバケットポリシーステートメントを作成します `buck1`。このポリシーは、LDAPグループにリソース（バケットとそのオブジェクト）への `buck1`アクセスを許可し `group1`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グループのユーザがS3クライアントからS3処理を実行できることを確認します `group1`。

認証に**LDAP**高速バインドモードを使用する

1. グループのSVMの_name service database_ofとしてldapを指定し、ldapのパスワードを指定します。

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

リンクhttps://docs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。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ユーザの権限がバケットポリシーで定義されていることを確認します。詳細については、を参照してください "バケットポリシーを変更する"。
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クライアントで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）。
   `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. ユーザに権限が割り当てられているS3クライアントから基本的なS3処理を実行します。

UIDと**GID**を使用しないユーザに対する**Active Directory**のリソース認証

bucket-policyステートメントで指定されたnasgroupまたはnasgroupの一部であるユーザに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と検索が失敗します。

検索の失敗を避けるため、NetAppでは、信頼できるドメインをUPN形式で使用することを推奨しています。nasgroup / group@trusted_domain.com

LDAP高速バインドを使用しない場合に信頼できるドメインユーザのユーザアクセスキーを生成するには

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

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

LDAPユーザまたはドメインユーザが独自の**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管理者としてカスタムロールを作成し、ローカルグループ、ドメイングループ、またはLightweight Directory Access Protocol（LDAP）グループに付与して、それらのグループに属するユーザがS3クライアントアクセス用の独自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することができます。

カスタムロールを作成してアクセスキーを生成するAPIを呼び出すユーザに割り当てるには、Storage VMでいくつかの設定手順を実行する必要があります。

開始する前に

次の点を確認します。

1. S3サーバを含むS3対応Storage VMが作成されている。を参照して "S3用のSVMの作成"
2. そのStorage VMにバケットが作成されている。を参照して "バケットを作成する"
3. Storage VMにDNSが設定されています。を参照して "DNSサービスの設定"
4. LDAPサーバの自己署名ルート認証局（CA）証明書がStorage VMにインストールされている。を参照して "自己署名ルートCA証明書をSVMにインストールする"
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。を参照して "LDAPクライアント設定を作成する"
6. クライアント設定をSVMに関連付けます。を参照して "LDAPクライアント設定をSVMに関連付ける"リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI// vserver-services-name-service-ldap-create.html[`vserver services name-service ldap create`^]コマンドを参照してください。
7. データStorage VMを使用している場合は、管理ネットワークインターフェイス（LIF）とVM上に、LIFのサービスポリシーを作成します。^]および[`network interface service-policy create`^]コマンドの詳細については[`network interface create`、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

1. グループのStorage VMの_name service database_としてldapを指定し、ldapのパスワードを指定します。

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

   リンクhttps://docs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。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を含むカスタムロールを作成：`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`、Storage VM上のユーザに対してロールが生成され`svm-1`、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
```

   リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI/ security-login-rest-role-create.html[`security login rest-role create`^]コマンドを参照してください。

3. security loginコマンドを使用してLDAPユーザグループを作成し、S3ユーザ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。リンクhttps://docs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。NetApp .com /us-en/ ONTAP -CLI// security-login-create.html[security login create^]コマンドを参照してください。

```
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グループを `ldap-group-1`に作成し `svm-1`、APIエンドポイントにアクセスするためのカスタムロールを `s3role`追加し、高速バインドモードでLDAPアクセスを有効にします。

```
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、を参照してください "nsswitch認証にLDAP高速バインドを使用する"。

ドメインまたはLDAPグループにカスタムロールを追加すると、そのグループのユーザはONTAPエンドポイントへの制限付きアクセスが許可されます `/api/protocols/s3/services/{svm.uuid}/users`。APIを呼び出すことで、ドメインまたはLDAPグループのユーザは、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。キーを生成できるのは自分だけで、他のユーザーには生成できません。

S3ユーザまたはLDAPユーザとして、独自のアクセスキーを生成

ONTAP 9 14.1以降では、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（管理者が独自のキーを生成するロールをユーザに許可している場合）。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。

HTTPメソッドとエンドポイント

このREST API呼び出しでは、次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他のメソッドの詳細については、リファレンスを参照して "APIドキュメント"ください。

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

カールの例

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

JSON出力の例


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "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を有効にする

ONTAP S3アクセスによるリモート**FabricPool**階層化を有効にする

ONTAP S3をリモートFabricPoolの大容量（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。

タスクの内容

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用に設定されたDNSサーバに、リモートONTAP S3サーバのホスト名に関するエントリ（S3サー

バのFQDN名とサーバのLIFのIPアドレスを含む）が必要です。

- クラスタピアリングは不要ですが、ローカルクラスタにインタークラスタLIFが設定されている必要があります。

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**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サーバ名とバケット名を確認し、（パラメータを指定して）クラスタLIFを使用してS3サーバを作成しておく必要があります `-vserver Cluster`。

タスクの内容

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格納されます。

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またはバケットに再関連付けしないでください。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
```

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

```
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を使用して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"。

   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、FabricPoolのローカル階層化に使用するアグリゲート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`*

   オプションを使用すると、FlexGroupボリュームのコンスティチュエントを含むアグリゲートを接続できます `allow-flexgroup` **`true`**。

   ```
   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であ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
   ```

S3クライアントアプリケーションが**ONTAP S3**サーバにアクセスできるようにする

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、次のAWS署名バージョンを使用してONTAP S3サーバで認証できる必要があります。

- 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。

タスクの内容

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管理者から提供され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情報を取得および設定できるようにするには、 `GetObjectTagging` `DeleteObjectTagging`バケットポリシーまたはグループポリシーを使用して、およびを `PutObjectTagging`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で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事前定義された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 で実際に使用可能なストレージサービスは、 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。

次の表に、定義済みのストレージサービスと対応する最小パフォーマンス要因を示します。

ストレージサービス	想定 **IOPS** （ **SLA** ）	最大 **IOPS** （ **SLO** ）	最小ボリューム **IOPS**	推定レイテンシ	想定 **IOPS** の適用
値	128/TB	512/TB	75	17 ミリ秒	AFF の場合：はい それ以外の場合：いいえ
パフォーマンス	TBあたり2、048	4096/TB	500	2ミリ秒	○
最高レベル	TBあたり6、144	12288/TB	1000	1 ミリ秒	○

次の表に、メディアまたはノードのタイプごとに使用可能なストレージサービスレベルを示します。

メディアまたはノード	使用可能なストレージサービスレベル
ディスク	値
仮想マシンディスク	値
FlexArray LUN の略	値
ハイブリッド	値
大容量フラッシュ	値
ソリッドステートドライブ（ SSD ） - AFF 以外のドライブです	値
パフォーマンスが最適化されたフラッシュ - SSD （ AFF ）	卓越したパフォーマンス、価値

ONTAP S3バケット用のCross-Origin Resource Sharing（CORS）の設定

ONTAP 9 .16.1以降では、Cross-Origin Resource Sharing（CORS）を設定して、異なるドメインのクライアントWebアプリケーションがONTAPバケットにアクセスできるようにすることができます。これにより、Webブラウザを使用してバケットオブジェクトにセキュアにアクセスできるようになります。

CORSはHTTP上に構築されたフレームワークで、1つの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、ウェブセキュリティの初期の基盤である_same-origin policy_を安全にバイパスするために使用されます。主な概念と用語については、以下で説明します。

由来

原点は、リソースの場所とIDを正確に定義します。次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

ここに起源の簡単な例があります。 `https://www.mycompany.com:8001`オリジンがCORSとともに使用される場合、要求を行っているクライアントを識別します。

same-originポリシー

same-origin policy（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の概念と制限です。このポリシーでは、Webページから最初にロードされたスクリプトが、両方のページが同じオリジンにある限り、別のページのデータにアクセスできます。この制限により、悪意のあるスクリプトが別のオリジンのページ内のデータにアクセスするのを防ぐことができます。

一般的な**CORS**のユースケース

CORSにはいくつかの一般的なユースケースがあります。ほとんどの場合、AJAXリクエスト、フォント、スタイルシート、スクリプトのロード、クロスドメイン認証など、クロスドメインアクセスの明確に定義された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要求および応答に挿入されるヘッダーを使用して実装されます。たとえば、アクセス制御を実装し、メソッドやヘッダーなど、許可される操作を示す応答ヘッダーがいくつかあります。HTTP要求に_Origin_headerがあると、クロスドメイン要求として定義されます。オリジン値は、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のオプションの要求です。応答に基づいて、CORS要求を完了することも、完了しないこともできます。

ONTAPハケツト

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およびアクセスされるオブジェクトのコンテナです。ONTAPバケットには次の2種類があります。

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

ONTAPでの**CORS**の実装

CORSは、ONTAP 9 .16.1以降のリリースでは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、効果的に無効にすることができます。

想定されるユースケース

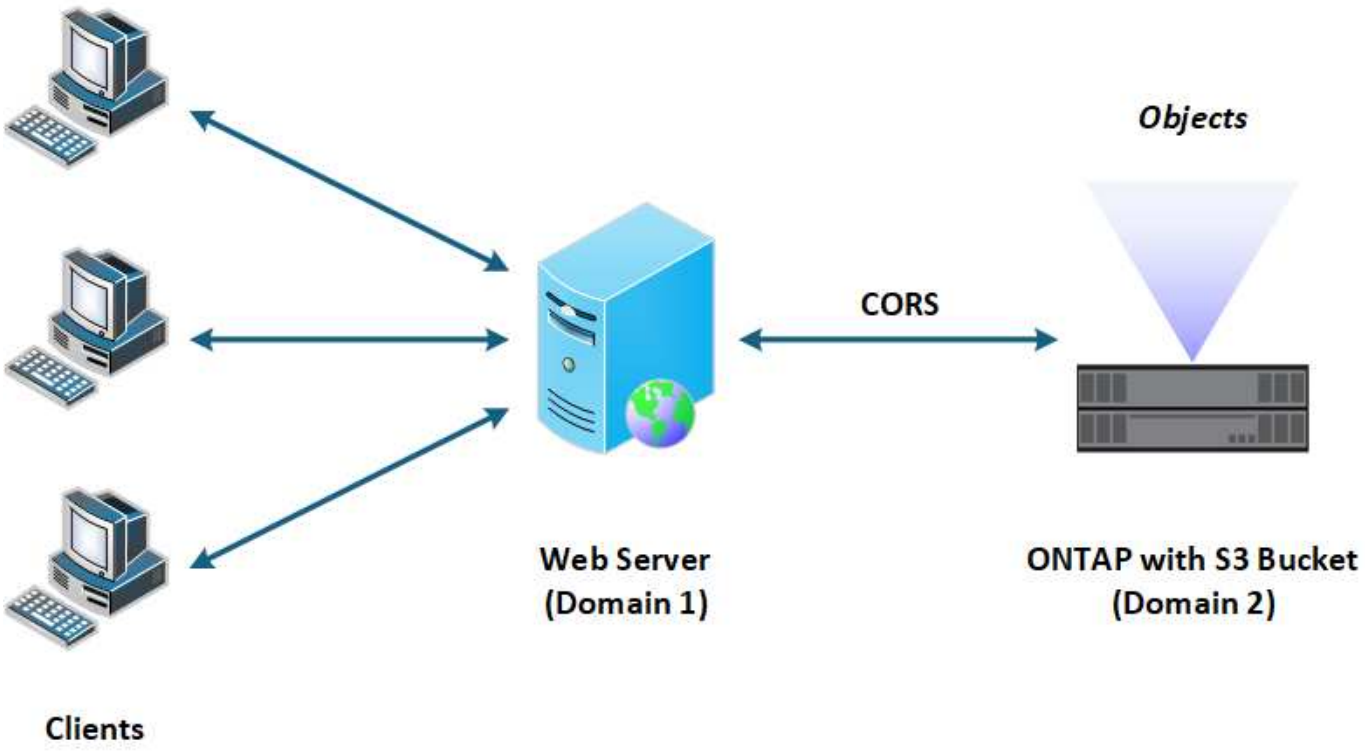
ONTAP CORSの実装では、クロスドメインリソースアクセスのために、次のようないくつかのトポロジが可

能になります。

- 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

次の図は、CORSによってONTAP S3バケットへのアクセスを有効にする方法の概要を示しています。



CORSルールの定義

この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。

設定アクション

ONTAPでは、次の3つの主要な設定ルールアクションがサポートされています。

- - 表示
- 作成
- 削除

ONTAPで定義されているCORSルールには、SVMとバケット、許可されているオリジン、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CORSを管理する場合は、いくつかのオプションを使用できます。

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、を参照してください CLIを使用したCORSの管理 。

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、次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、を "ONTAP自動化に関するドキュメント"参照してください。

S3 API

S3 APIを使用して、ONTAPバケットのCORS設定を作成および削除できます。S3クライアント管理者には、次のような十分なPrivileges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、すべてのノードを9.16.1にアップグレードするとサポートされます。混在モードのクラスタでは、この機能は有効なクラスタバージョン（ECV）が9.16.1以降の場合にのみ使用できます。

リバート

ユーザ側では、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、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元に戻すコマンドを実行するように求められます。

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。主な操作は以下のとおりです。CORSコマンドを発行するには、ONTAP * admin *権限レベルである必要があります。

作成

コマンドを使用して、CORSルールを定義できます `vserver object-store-server bucket cors-rule create`。

パラメータ

ルールの作成に使用するパラメータを次に示します。

パラメータ	説明
`vserver`	ルールを作成するオブジェクトストアサーババケットをホストするSVM（SVM）の名前を指定します。
`bucket`	ルールを作成するオブジェクトストアサーバのバケットの名前。
`index`	ルールを作成す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指定する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元を許可するオリジンのリスト。
`allowed-methods`	クロスオリジン要求で許可されるHTTPメソッドのリスト。
`allowed-headers`	クロスオリジン要求で許可されるHTTPメソッドのリスト。
`expose-headers`	お客様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レスポンスをキャッシュする時間を指定するオプションのパラメータ。

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 `vserver object-store-server bucket cors-rule show`。

パラメータを含める `-instance`と、各ルールに表示されるデータが展開されます。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。ルールの値が必要な `index`ため、この操作は次の2つのステップで実行されます。

1. コマンドを実行し `show`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を発行します。

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、次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でバケットを保護

SnapMirror S3の概要

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では、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可能です。

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階層とバックアップ階層がサポートされます。

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 • 同じクラスタの異なるSVMのバケット • 異なるクラスタのSVM内のバケット	○	○

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
StorageGRID	いいえ	○
AWS S3	いいえ	○
Cloud Volumes ONTAP for Azure	○	○
Cloud Volumes ONTAP for AWS	○	○
Cloud Volumes ONTAP for Google Cloud	○	○

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

  ソースクラスタとデスティネーションクラスタでONTAP 9 .10.1以降が実行されている必要があります。

- ライセンス

  のアクセスを提供するには、ONTAPソースシステムとデスティネーションシステムに次のライセンスがソフトウェアスイートに含まれている"ONTAP One"必要があります。

  - ONTAP S3プロトコルとストレージ
  - 他のNetAppオブジェクトストアターゲット（ONTAP S3、StorageGRID、Cloud Volumes ONTAP）をターゲットにするためのSnapMirror S3
  - AWS S3などのサードパーティのオブジェクトストアをターゲットとするSnapMirror S3（で使用可能"ONTAP One互換バンドル"）

- ONTAP S3
  - ONTAP S3サーバでソースとデスティネーションのSVMが実行されている必要があります。
  - TLSアクセス用のCA証明書を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したCA証明書が、S3サーバをホストするクラスタの管理Storage VMにインストールされている必要があります。
    - 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は、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ターゲット用）
  - クラスタ間LIFが設定されている（リモートONTAPターゲット用）必要があり、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が、ソースとデスティネーションのS3サーバのデータLIFに接続できるようになります。
  - ソースクラスタとデスティネーションクラスタがピア関係にある（リモート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がピア関係にある（すべてのONTAPターゲットに対して）。

- 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できます。
  - 独自のポリシーを作成するか、次の値を含むデフォルトの * Continuous * ポリシーをそのまま使用できます。
    - Throttle（スループット/帯域幅の上限）-無制限。
    - 目標復旧時点までの時間： 1 時間（ 3600 秒）

> ⓘ 2つのS3バケットがSnapMirror関係にある場合、オブジェクトの現在のバージョンが期限切れになる（削除される）ようにライフサイクルポリシーが設定されていると、同じ処理がパートナーバケットに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の場合でも同様です。

- rootユーザキーSnapMirror S3関係にはStorage VMのrootユーザアクセスキーが必要です。ONTAPではデフォルトで割り当てられません。SnapMirror S3関係の初回作成時には、キーがソースとデスティネーションの両方のStorage VMに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。それらのキーを再生成する必要がある場合は、アクセスキーとシークレットキーのペアを使用するすべてのクライアントおよびSnapMirrorオブジェクトストアの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S3サーバを有効にする"
- "ONTAP S3の設定プロセスの概要"

クラスタと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。

- "ミラーリングとバックアップの準備（System Manager、手順1~6）"
- "クラスタとSVMのピアリング（CLI）"

サポートされる**SnapMirror**関係

SnapMirror S3では、ファンアウト関係とカスケード関係がサポートされます。概要については、を参照してください"ファンアウト構成およびカスケード構成のデータ保護"。

SnapMirror S3は、ファンイン環境（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間のデータ保護関係）をサポートしていません。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ミラーをサポートできますが、各ソースバケットにセカンダリクラスタ上の専用のデスティネーションバケットが必要です。

S3バケットへのアクセスを制御

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

リモートクラスタでのミラーとバックアップの保護

新しいバケット（リモートクラスタ）のミラー関係を作成する

新しいS3バケットを作成したときに、リモートクラスタのSnapMirror S3デスティネーションでバケットをただちに保護することができます。

タスクの内容

タスクは、ソースシステムとデスティネーションシステムの両方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が完了している。
- ソースクラスタとデスティネーションクラスタの間にピア関係が確立され、ソースとデスティネーションのStorage VMの間にピア関係が確立されています。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。すでに存在するキーを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]>[Storage VM]をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. 既存のS3ポリシーがなく、デフォルトのポリシーを使用しない場合は、ソースクラスタでSnapMirror S3ポリシーを作成します。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] をクリックします。権限の検証はオプションですが、推奨されます。
   b. 名前を入力し、 Storage VM を選択してサイズを入力し、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-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-デフォルト値または必要なその他の値を使用します `(bucketname, bucketname/*)`。

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

管理"。

d. [**Protection**] で、 **[Enable SnapMirror (ONTAP or Cloud)**] をオンにします。次に、次の値を入力します。

- デスティネーション
  - * ターゲット： ONTAP システム *
  - * cluster * ：リモートクラスタを選択します。
  - * Storage VM * ：リモートクラスタの Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書： * destination_certificate の内容をコピーして貼り付けます。

5. チェック * 外部 CA ベンダーが署名し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します。
6. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存（ Save ）] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage 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でONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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
   ```

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

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

   すでに存在するキーを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. 既存のS3ポリシーがない場合やデフォルトポリシーを使用しない場合は、ソースSVMで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`-目標復旧時点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. ソースクラスタとデスティネーションクラスタの管理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、*destination_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で、*source_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

外部の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。

詳細については、のマニュアルページを参照して `security certificate install` 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`

既存のバケット（リモートクラスタ）のミラー関係を作成する

既存のS3バケットの保護はいつでも開始できます。たとえば、S3の設定をONTAP 9 10.1より前のリリースからアップグレードした場合などです。

タスクの内容

タスクはソースクラスタとデスティネーションクラスタの両方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が完了している。
- ソースクラスタとデスティネーションクラスタの間にピア関係が確立され、ソースとデスティネーションのStorage VMの間にピア関係が確立されています。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
   a. [ストレージ]>[Storage VM]*を選択し、Storage VMを選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。*すでに存在するキーを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に既存のユーザとグループが存在し、正しいアクセス権があることを確認します。**[ストレージ]>[Storage VM]***を選択し、**Storage VM**を選択して[設定]タブを選択します。最後に、 S3 タイルを探し 、を選択して Users タブを選択し、 Groups *タブを選択して、ユーザ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、を参照してください "S3ユーザとグループの追加" 。
3. 既存のS3ポリシーがなく、デフォルトのポリシーを使用しない場合は、ソースクラスタでSnapMirror S3ポリシーを作成します。
   a. [保護]>[概要]を選択し、[ローカルポリシー設定]*をクリックします。
   b. 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. ポリシースコープ（クラスタまたはSVM）を選択します。
   e. SnapMirror S3関係の場合は*[Continuous]*を選択します。
   f. スロットル値および * 目標復旧時点 * 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ニーズ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] の順にクリックし、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * 主な内容と効果 * ：ユーザーグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション：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:デフォルト値または必要なその他の値を使用し `(*bucketname, bucketname*/*)` ます。

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

b. [*Protect] をクリックして、次の値を入力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：リモートクラスタを選択します。
  - * Storage VM * ：リモートクラスタの Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書 * ： _destination_certificate の内容をコピーして貼り付けます。

6. チェック * 外部 CA ベンダーが署名し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します。
7. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存（ Save ）] をクリックします。既存のバケットがデスティネーションStorage 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でONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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`。+ rootユーザのアクセスキーがあることを確認します。存在しない場合は、「 `vserver object-store-server user regenerate-keys -vserver svm_name -user root`+ Do not regenerate the key if one already exists」と入力します。
2. ミラーターゲットとして使用するデスティネーションSVMに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、SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトのポリシーを使用しない場合）。

   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–目標復旧時点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. ソースクラスタとデスティネーションクラスタの管理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、*destination_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で、*source_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*。+外部のCAベンダーが署名した証明書を使用している場合は、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。

      詳細については、のマニュアルページを参照して security certificate install 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`

デスティネーションバケット（リモートクラスタ）からテイクオーバーしてデータを提供

ソースバケットのデータが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。

タスクの内容

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るため、SnapMirror S3関係が反転されます。

無効にしたソースバケットが再び使用可能になると、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環境の場合のように、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。

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、[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. フェイルオーバー処理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
```

デスティネーション**Storage VM**（リモートクラスタ）からバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、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することでデータを再取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、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大きくする必要があります。

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

バックアップした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 ⋮ 、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 既存のバケットを選択します。
     - destination_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
   - 新しいバケットへのリストアを実行するには、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、を参照してください "ストレージサービスレベル" 。
     - destination_S3 サーバ CA 証明書の内容。
4. 「 * Destination * 」の下にある _source_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護] 、 [関係] の順にクリックして、復元の進行状況を監視します。

ロックされたバケットの復元

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。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、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レプリケートされます。新しいバケットに対して別の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、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：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、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

CLI

1. リストア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、を参照してください "新しいバケット（クラウドターゲット）のバックアップ関係を作成"。
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
```

ローカルクラスタでのミラーとバックアップの保護

新しいバケット（ローカルクラスタ）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きに、同じクラスタ上のSnapMirror S3デスティネーションでバケットをただちに保護することができます。データは、ソースと同じStorage VMまたは別の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が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、[S3]タイル内をクリックし ます。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。すでに存在するキーを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ます。**[ストレージ]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

   詳細については、を参照してください "S3ユーザとグループの追加" 。
3. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   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. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] 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、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。権限の検証はオプションですが、推奨されます。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-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-デフォルト値または必要なその他の値を使用します。`(bucketname, bucketname/*)`

        これらのフィールドの詳細については、を参照してください"バケットへのユーザアクセスの管理"。
   d. [**Protection**] で、 **[Enable SnapMirror (ONTAP or Cloud)]** をオンにします。次に、次の値を入

力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：ローカルクラスタを選択します。
  - * Storage VM *：ローカルクラスタのStorage VMを選択します。
  - * S3 サーバ CA 証明書 * ：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 サーバ 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. チェック * 外部 CA ベンダーが署名し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します。
6. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
7. [保存（ Save ）] をクリックします。ソースStorage VMに新しいバケットが作成され、デスティネーションStorage 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でONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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
   ```
   rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。
   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```
   すでに存在するキーを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. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   `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`–目標復旧時点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. *destination_S3*サーバ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 dest_server_certificate。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

      詳細については、のマニュアルページを参照して `security certificate install` 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`

既存のバケット（ローカルクラスタ）のミラー関係を作成する

S3設定をONTAP 9 .10.1より前のリリースからアップグレードした場合など、同じクラスタ上の既存のS3バケットの保護はいつでも開始できます。データは、ソースと同じStorage VMまたは別の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が完了している。
- ソースとデスティネーションのStorage VMの間にピア関係が確立されている。
- CA証明書は、ソースVMとデスティネーションVMに必要です。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の最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のStorage VMにroot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。
   a. Storage > Storage VM* をクリックし、 Storage VM を選択します。
   b. [設定]タブで、* S3 *タイル内をクリックします 。
   c. [**Users**] タブで、 root ユーザのアクセスキーがあることを確認します。
   d. 表示されていない場合は、* root の横にあるをクリックし 、 Regenerate Key *をクリックします。キーがすでに存在する場合は再生成しない
2. ソースとデスティネーションの両方のStorage VMに既存のユーザとグループが存在し、正しいアクセス権があることを確認します。**[ストレージ]>[Storage VM]***を選択し、**Storage VM**を選択して、[設定]タブを選択します。最後に、 S3 タイルを探し 、を選択して Users タブを選択し、 Groups * タブを選択して、ユーザ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、を参照してください "S3ユーザとグループの追加" 。
3. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 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ニーズ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] の順にクリックし、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-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-デフォルト値または必要なその他の値を使用します *(bucketname, bucketname/*)*。

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

b. [*Protect] をクリックして、次の値を入力します。

- デスティネーション
  - * ターゲット * ： ONTAP システム
  - * cluster * ：ローカルクラスタを選択します。
  - * Storage VM * ：同じ Storage VM または別の Storage VM を選択します。
  - * S3 サーバ CA 証明書 * ： _source_certificate の内容をコピーして貼り付けます。
- ソース
  - * S3 サーバ CA 証明書 * ： _destination_certificate の内容をコピーして貼り付けます。

6. チェック * 外部 CA ベンダーが署名し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します。
7. [* Destination Settings] をクリックすると、バケット名、容量、およびパフォーマンスサービスレベルのデフォルト値の代わりに独自の値を入力することもできます。
8. [保存（ Save ）] をクリックします。既存のバケットがデスティネーションStorage 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でONTAP 9 .14.1以降を実行し、ソースバケットでオブジェクトのロックが有効になっている場合は、デスティネーションバケットでオブジェクトの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の保持期間が、デスティネーションバケットのレプリケートオブジェクトに適用されるようになります。また、*[Destination Settings]*セクションで、デスティネーションバケットに対して別の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インターフェイ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、を参照してください"バケットを作成する"。

CLI

1. このSVMに対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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`

   rootユーザのアクセスキーがあることを確認します。表示されない場合は、次のように入力します。
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   すでに存在するキーを再生成しないでください。

2. ミラーターゲットとして使用するデスティネーションSVMに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へのアクセスルール

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. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。

   `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`–目標復旧時点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. *destination_S3*サーバ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 dest_server_certificate。+外部のCAベンダーが署名した証明書を使用する場合は、管理SVMにこの証明書をインストールするだけです。

   詳細については、のマニュアルページを参照して `security certificate install` 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`

デスティネーションバケット（ローカルクラスタ）からテイクオーバーしてデータを提供

ソースバケットのデータが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。

タスクの内容

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るため、SnapMirror S3関係が反転されます。

無効にしたソースバケットが再び使用可能になると、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環境のように、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は、リモートクラスタからテイクオーバー処理を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、[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. フェイルオーバー処理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
```

デスティネーション**Storage VM**（ローカルクラスタ）からバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、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することでデータを再取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、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大きくする必要があります。

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. [* 保護] 、 [関係] の順にクリックし、バケットを選択します。
2. をクリックし ⋮ 、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 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。
   - 新しいバケットへのリストアを実行するには、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、を参照してください "ストレージサービスレベル" 。
     - デスティネーションS3サーバCA証明書の内容。
5. 「 * Destination * 」の下にあるソース S3 サーバ CA 証明書の内容をコピーして貼り付けます。
6. ［ * 保護 * ］ > ［ 関係 ］ の順にクリックして、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復元

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。

- 新しいバケットにリストア：オブジェクトのロックが有効になっている場合、オブジェクトのロックも有効になっているバケットを作成することで、バケットをリストアできます。ロックされたバケットをリストアすると、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レプリケートされます。新しいバケットに対して別の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、他のソースからのロックされていないオブジェクトに適用されます。
- 既存のバケットにリストア：オブジェクトロックバケットは、既存のバケットでバージョン管理および同様のオブジェクトロックモードが有効になっていれば、既存のバケットにリストアできます。元のバケットの保持期間が維持されます。
- ロックされていないバケットのリストア：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、ソースクラスタにあるオブジェクトロックが有効になっているバケットにリストアできます。バケットをリストアすると、ロックされていないオブジェクトがすべてロックされ、デスティネーションバケットの保持モードと保持期間がそれらのオブジェクトに適用されます。

CLI

1. オブジェクトを新しいバケットにリストアする場合は、新しいバケットを作成します。詳細については、を参照してください "新しいバケット（クラウドターゲット）のバックアップ関係を作成"。
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
```

クラウドターゲットを使用したバックアップ保護

クラウドのターゲットとなる関係の要件

ソースとターゲットの環境が、クラウドターゲットに対するSnapMirror S3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と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前に、クラスタ間LIFとIPspaceをクラスタに設定しておく必要があります。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できるように、各ノードにクラスタ間LIFを作成する必要があります。

StorageGRIDターゲットについて、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アドレスで指定）
- バケット名。既存のバケットを指定する必要があります。
- アクセスキー
- シークレットキー

また、StorageGRIDサーバ証明書への署名に使用したCA証明書が、を使用してONTAP S3クラスタの管理Storage VMにインストールされている必要があり `security certificate install command`ます。詳細については、「"CA 証明書をインストールしています"StorageGRIDを使用する場合」を参照してください。

AWS S3ターゲットについて、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アドレスで指定）
- バケット名。既存のバケットを指定する必要があります。
- アクセスキー
- シークレットキー

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

新しいバケット（クラウドターゲット）のバックアップ関係を作成

新しいS3バケットを作成すると、オブジェクトストアプロバイダ（StorageGRIDシステムまたはAmazon S3環境）の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。

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。
- •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. 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]>[Storage VM]をクリックし、**Storage VM**をクリックして[設定]をクリックし、 S3 * の下をクリックし ます。

      詳細については、を参照してください "S3ユーザとグループの追加" 。
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（ Protection ）] > [概要（ Overview ）] * をクリックし、 [クラウドオブジェクトストア（ Cloud Object Stores ）] を
   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）名
3. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[追加]*をクリックします。
      - ポリシーの名前と説明を入力します。
      - ポリシースコープ（クラスタまたはSVM）を選択します
      - SnapMirror S3関係の場合は*[Continuous]*を選択します。
      - スロットル値および * 目標復旧時点 * 値を入力します。
4. SnapMirror保護を設定してバケットを作成します。
   a. [* ストレージ] 、 [バケット] の順にクリックし、 [* 追加] 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、 * その他のオプション * をクリックします。
   c. [**Permissions**] で、 [**Add**] をクリックします。権限の検証はオプションですが、推奨されます。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-次の値が表示されていることを確認します。

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

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

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

d. [* 保護 *] で、 [* SnapMirror （ ONTAP またはクラウド）を有効にする *] をオンにし、 [* 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。

[Save] をクリックすると、ソース Storage 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に対する最初のSnapMirror S3関係である場合は、ソースとデスティネーションの両方のSVMにroot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`。+ rootユーザのアクセスキーがあることを確認します。存在しない場合は、「 `vserver object-store-server user regenerate-keys -vserver svm_name -user root`+ Do not regenerate the key if one already exists」と入力します。
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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   `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`–目標復旧時点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`

詳細については、のマニュアルページを参照して `security certificate install` ください。

6. SnapMirror S3デスティネーション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`–このワークフローで使用し `data`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。+詳細については、マニュアルページを参照して `snapmirror object-store config create`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の名前と固定値 `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 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
```

既存のバケット（クラウドターゲット）のバックアップ関係を作成する

既存のS3バケットのバックアップはいつでも開始できます。たとえば、S3の設定をONTAP 9 .10.1より前のリリースからアップグレードした場合などです。

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。
- 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]>[Storage VM]***をクリックし、**Storage VM**をクリックして[設定]*をクリックし、[S3]の下をクリックし ます。

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

2. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   a. [* 保護] 、 [概要 *] の順にクリックし、 [ローカルポリシーの設定 *] をクリックします。
   b. の横にあるをクリックし 、[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. ポリシースコープ（クラスタまたはSVM）を選択します
   e. SnapMirror S3関係の場合は*[Continuous]*を選択します。
   f. スロットル * とリカバリ・ポイントの目標値 * 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（ Protection ）] > [概要（ Overview ）] * をクリックし、 [クラウドオブジェクトストア（ Cloud Object Store ）] を選択
   b. [* 追加] をクリックし、 [* Amazon S3 * または * その他 * （ StorageGRID Webscale ）] 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）名
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ニーズを満たしていることを確認します。
   a. [* Storage * > * Buckets] をクリックして、保護するバケットを選択します。
   b. [権限]タブで*をクリックし 、[権限]の[追加]*をクリックします。
      - * Principal * および * Effect * - ユーザグループの設定に対応する値を選択するか、デフォルト値をそのまま使用します。
      - アクション-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-デフォルト値または必要なその他の値を使用します *(`bucketname`, `bucketname/*`)*。

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

5. SnapMirror S3を使用してバケットをバックアップします。
   a. [* Storage *] > [* Buckets] 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. [* Protect （保護）] をクリックし、 [* Target （ターゲット）] の下の [* Cloud Storage （クラウドストレージ）] を選択してから、 [* Cloud Object Store （クラウドオブジェクトストア）]

Save 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. SnapMirror S3ポリシーを作成します（既存のポリシーがなく、デフォルトポリシーを使用しない場合）。
   `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`–目標復旧時点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`

   詳細については、のマニュアルページを参照して `security certificate install` ください。

4. SnapMirror S3デスティネーション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`–このワークフローで使用し `data`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。+詳細については、マニュアルページを参照して `snapmirror object-store config create`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の名前と固定値 `objstore`。+ 作成したポリシーを使用することも、デフォルトをそのまま使用することもできます。

```
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`

クラウドターゲットからバケットをリストアする

ソースバケットのデータが失われたり破損したりした場合は、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取り込みできます。

タスクの内容

デスティネーションバケットは、既存のバケットまたは新しいバケットにリストアできます。リストア処理のターゲットバケットは、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大きくする必要があります。

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 ⋮ 、*[リストア]*を選択します。
3. 「 * ソース * 」で、「 * 既存バケット」（デフォルト）または「 * 新規バケット」を選択します。
   - 既存の Bucket * （デフォルト）にリストアするには、次の操作を実行します。
     - クラスタとStorage VMを選択して既存のバケットを検索します。
     - 既存のバケットを選択します。
     - destination_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
   - 新しいバケットへのリストアを実行するには、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、を参照してください "ストレージサービスレベル" 。
     - デスティネーションS3サーバCA証明書の内容。
4. 「 * Destination * 」の下にある _source_S3 サーバ CA 証明書の内容をコピーして貼り付けます。
5. [保護] 、 [関係] の順にクリックして、復元の進行状況を監視します。

CLIの手順

1. リストア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、を参照してください "バケットのバックアップ関係の作成（クラウドターゲット）"。
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
```

ミラーポリシーを変更する

S3ミラーポリシーの変更が必要になる場合があります。たとえば、RPOとスロットル値を調整する場合などです。

System Manager

これらの値を調整するには、既存の保護ポリシーを編集します。

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`–目標復旧時点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
```

SnapshotでS3データを保護

S3 Snapshotの概要

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のポイントインタイムイメージを生成できます。

S3のSnapshot機能を使用すると、Snapshotを手動で作成することも、Snapshotポリシーを使用して自動的に生成することもできます。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クライアントを使用して、Snapshotのコンテンツを参照し、リストアできます。

ONTAP 9 .16.1では、S3 SnapshotはS3バケット内のオブジェクトの現在のバージョンのみをキャプチャします。バージョン管理されたバケットの最新以外のバージョンは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、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 Snapshotはクラスタ時間に依存します。時刻を同期するには、クラスタ内のNTPサーバを設定する必要があります。詳細については、を参照してください "クラスタ時間を管理します。"。

クォータとスペース使用量

クォータは、S3バケットで使用されているオブジェクトの数と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、ファイルシステムからSnapshotが削除されるまで、バケットのオブジェクト数と使用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の場合、最後のオブジェクトのみがスナップショットにキャプチャされます。マルチパートオブジェクトの部分的なアップロードはSnapshotにキャプチャされません。

バージョン管理に対応しているバケットとバージョン管理に対応していないバケット上の**Snapshot**

バージョン管理に対応しているバケットとバージョン管理に対応していないバケットの両方にSnapshotを作成できます。スナップショットには、スナップショットがキャプチャされた時点での現在のオブジェクトバージョンのみが含まれます。

バージョン管理されたバケットとスナップショット

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の作成後に最新のオブジェクトバージョンのコンテンツが保持されます。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ン管理が有効になっているバケットで、オブジェクト `obj1` のバージョンは `v1`、`v2`、`v3`、`v4`、`v5` です。`v3`（キャプチャ時点の最新バージョン）から `obj1` スナップショットを作成した `snap1`。閲覧すると `snap1`、`obj1` はv3で作成されたコンテンツを含む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。

バージョン管理に対応していないバケットとスナップショット

バージョン管理に対応していないバケットでは、S3 SnapshotはSnapshotの作成前に最新のコミットの内容を保持します。

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を利用できないバケットで、でオブジェクトが `obj1` 数回上書きされています（`T1`、`T2`、`T3`、`T4`、`T5`）。`T3`と`T4`の間に`S3 Snapshot`を作成しました `snap1`。閲覧すると `snap1`、`obj1` `T3`で作成されたコンテンツと一緒に表示されます。

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、互いに独立して機能します。ONTAPオブジェクトの有効期限機能は、S3バケットに対して定義されたライフサイクル管理ルールに従ってオブジェクトバージョンの期限が切れます。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なコピーです。

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る場合、そのバケットに定義された有効期限ルールによってオブジェクトの特定のバージョンが削除されたときに、そのバージョンが1つ以上のS3 Snapshotに現在のバージョンとして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。そのオブジェクトバージョンは、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ても、そのオブジェクトが既存のS3 Snapshotにキャプチャされたままの場合、オブジェクトはファイルシステムに保持されます。オブジェクトをキャプチャしている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の管理については、を参照してください"バケットライフサイクル管理ルールを作成する"。

S3 Snapshotニカンスルセイケンシコウ

ONTAP 9 .16.1では、次の機能の除外とシナリオに注意してください。

- S3バケットに対して生成できるSnapshotは最大1023個です。
- クラスタをONTAP 9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。16.1
- Snapshotを含む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、次の構成ではサポートされません。
  - SnapMirror関係のバケット
  - オブジェクトロックが有効になっているバケット
  - NetApp BlueXP の場合
  - System Manager
  - ONTAP MetroClusterコウセイ

S3 Snapshotを作成する

S3 Snapshotを手動で生成することも、Snapshotポリシーを設定してS3 Snapshotを自動的に作成することもできます。Snapshotは、データのバックアップとリカバリに使用するオブジェクトの静的コピーとして機能します。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を有効にする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にデータ保護を確立する際に特に役立ちます。これは、以前のオブジェクトバージョンを使用できない場合にリストア処理で使用できるポイントインタイムレコードとして機能するためです。

タスクの内容

- スナップショットには、次の命名規則が適用されます（手動スナップショットと自動スナップショットの両方）。
  - S3 Snapshot名の最大文字数は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または数字にする必要があります
  - S3 Snapshot名にサブ文字列を含めることはできません `s3snap`
- S3プロトコルでは、バケットの命名制限によってバケット名は63文字に制限されます。ONTAP S3スナップショットはS3プロトコルで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。
- どのスナップショットがどのバケットに属しているかを簡単に識別できるように、スナップショットバケット名は、ベースバケット名と、スナップショット名の前に付加された特別な文字列で構成され

-s3snap-`ます。Snapshotバケット名の形式は、です `<base_bucket_name>-s3snap-<snapshot_name>`。

たとえば、次のコマンドを実行して `snap1`onを `bucket-a`作成すると、という名前のSnapshotバケットが作成され `bucket-a-s3snap-snap1`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クライアントから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バケット名を作成することはできません。
- 自動Snapshot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、トラディショナルボリュームSnapshotの命名規則に似ています。スケジュールされたSnapshotの名前は `daily-2024-01-01-0015`、など `hourly-2024-05-22-1105`です。

S3 Snapshotを手動で作成する

ONTAP CLIを使用して、S3 Snapshotを手動で作成できます。この手順では、ローカルクラスタにのみSnapshotが作成されます。

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>
```

次の例は `vs0`、Storage VMと `website-data`バケットにという名前のSnapshotを作成します `pre-update`。

```
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バケットレベルのSnapshotポリシーを設定すると、ONTAPによってスケジュールされたS3 Snapshotが自動的に作成されます。従来のSnapshotポリシーと同様に、S3 Snapshotに対して最大5つのスケジュールを設定できます。

Snapshotポリシーは、通常、Snapshot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のプレフィックスを指定します。たとえば、毎日午前12時10分にS3 Snapshotを1つ作成し、最新の2つのコピーを保持して、という名前を付けることができます `daily-<timestamp>`。

デフォルトのSnapshotポリシーで保持される内容は次のとおりです。

- 6時間ごとのスナップショット

- 2つの日単位のスナップショット
- 2つの週単位のスナップショット

開始する前に

- Snapshotポリシーを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のポリシーには、他のONTAP Snapshotポリシーと同じルールが適用されます。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。

Snapshotを自動生成するためのSnapshotポリシーの作成の詳細については、を参照してください"カスタムSnapshotポリシーの設定の概要"。

手順

1. バケットにSnapshotポリシーを割り当てます。

```
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より前のバージョンのONTAPにリバートする必要がある場合は、すべてのバケットのの値が（または -）に設定されている `none`ことを確認して `snapshot-policy`ください。

関連情報

"S3 Snapshotの概要"

S3 Snapshotの表示とリストア

ONTAP S3のSnapshot機能を使用すると、S3クライアントからバケットのS3 Snapshotのコンテンツを表示および参照できます。また、S3 SnapshotからS3クライアント上の単一のオブジェクト、一連のオブジェクト、またはバケット全体をリストアできます。

開始する前に

バケットのONTAP S3 Snapshotを表示、参照、およびリストアするには、Snapshotが作成されている必要があります。また、S3プロトコルクライアントからS3ベースバケットにアクセスできる必要があります。

S3 Snapshotのリストと表示

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を表示できます。

手順

1. S3 Snapshotを表示します。

```
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 Snapshotの名前、Storage VM、バケット、作成時間、およびの情報を確認できます `instance-uuid`。

2. バケット名を指定して、そのバケットに対して作成されたすべてのS3 Snapshotの名前、作成時間、およびそのバケットに対して作成されたすべてのS3 Snapshotを表示することもできます `instance-uuid`。

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

S3 Snapshotのコンテンツを参照する

環境で障害や問題が発生した場合は、S3バケットのSnapshotの内容を参照してエラーを特定できます。また、S3のSnapshotを参照して、リストア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 Snapshotは、S3クライアントにSnapshotバケットとして提供されます。Snapshotバケット名の形式は、です `<base_bucket_name>-s3snap-<snapshot_name>`。S3 API処理を使用して、Storage VM内のすべてのSnapshotバケットを表示できます `ListBuckets`。

S3 snapshot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、読み取り専用の処理のみをサポートします。ベースバケットにアクセスする権限がある場合は、S3 Snapshotバケットに対して読み取り専用のS3 API処理（ `HeadObject`、 `GetObject`、 `GetObjectTagging` `ListObjects`、、 `ListObjectVersions`、 `GetObjectAcl`、および `CopyObject`。

> S3 Snapshotバケットでこの `CopyObject`処理がサポートされるのは、ソースバケットのSnapshotコピーである場合のみです。Snapshotのストレージデスティネーション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、を参照してください"ONTAP S3でサポートされる操作"。

S3 Snapshotからコンテンツをリストア

S3クライアントでリストア処理を実行して、Snapshotバケットから元のバケットまたは別のバケットにコンテンツをコピーすることで、単一のオブジェクト、一連のオブジェクト、またはバケット全体をリカバリできます。スナップショットを参照して、コピーするスナップショットコンテンツを決定できます。

バケット全体、プレフィックスが付いたオブジェクト、または単一のオブジェクトをリストアするには、コマンドを使用し `aws s3 cp`ます。

手順

1. ベースS3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。
   - バケット全体をリストアします。Snapshotバケット名は、の形式で指定し `<base_bucket_name>-s3snap-<snapshot_name>`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
     s3://<base-bucket>  --recursive
     ```

   - ディレクトリ内のオブジェクトを次のプレフィックスでリストアし `dir1`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
     s3://<base_bucket_name>/dir1 --recursive
     ```

   - 次の名前の単一オブジェクトをリストアし `web.py`ます。

     ```
     aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
     s3://<base_bucket_name>/web.py
     ```

S3 Snapshotの削除

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ているSnapshotポリシーを変更して、スケジュールで保持するSnapshotの数を変更したりできます。

S3バケットのSnapshotポリシーは、従来のONTAP Snapshotポリシーと同じ削除ルールに従います。Snapshotポリシーの作成の詳細については、を参照してください"Snapshot ポリシーを作成します"。

タスクの内容

- オブジェクトのバージョン（バージョン管理されたバケット内）またはオブジェクト（バージョン管理されていないバケット内）が複数のSnapshotにキャプチャされた場合、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を含む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より前のバージョンのONTAPにリバートする必要がある場合は、すべてのバケットのS3 Snapshotをすべて削除しておく必要があります。コマンドを実行してS3バケットのSnapshotメタデータを削除することも必要になる場合があり `vserver object-store-server bucket clear-snapshot-metadata`ます。詳細については、を参照して "S3 Snapshotメタデータをクリア"ください。
- スナップショットをバッチで削除すると、複数のスナップショット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、スナップショットを個別に削除する場合よりも多くのスペースが解放されます。その結果、ストレージオブジェクト用により多くのスペースを再利用できます。

手順

1. 特定のS3 Snapshotを削除するには、次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S3 Snapshotをすべて削除するには、次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メタデータをクリア

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引き続きバケットに格納されます。Snapshotメタデータが存在すると、次の処理がブロックされます。

- ONTAP 9より前のONTAPバージョンにクラスタをリバートします。16.1
- 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Snapshotメタデータをすべて消去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メタデータを消去するには、次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

S3イベントの監査

ONTAP 9 .10.1以降では、ONTAP S3環境でデータイベントと管理イベントを監査できます。S3の監査機能は既存のNASの監査機能と同様で、S3とNASの監査機能はクラスタ内に共存できます。

SVMでS3監査の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。ログに記録するイベントを指定できます。

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からこの名前に変更）
- ListAllMyBuckets（9.10.1のListBucketsはこの名前に変更）

9.10.1：

- ヘッドオブジェクト
- GetObject
- PutObject
- deleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- リストアップロード
- 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
- パーツコピーをアップロード
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1：

- GetBucketVersioning
- PutBucketVersioning

9.10.1：

- ヘッドバケット
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

ログの形式はJavaScript Object Notation（JSON）です。

S3とNFSの監査設定の合計数は、クラスタあたり50 SVM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（旧Core Bundleに含まれていたもの）

詳細については、を参照してください "ONTAP監査プロセスの仕組み"。

監査の保証

デフォルトでは、S3とNASの監査が保証されます。ONTAPでは、あるノードを使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がすべて記録されることが保証されます。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。スペース不足や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でコミットできない場合は、クライアント処理が拒否されます。

カンサヨウノスヘエスヨウケン

ONTAP監査システムでは、監査レコードは最初に個 々 のノード上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。

監査の設定に十分な使用可能スペースがあることを計画する必要があります。

- 監査対象バケットを含むアグリゲート内のステージングボリューム。
- （変換されたイベントログが格納されるディレクトリを含むボリューム）。

S3監査の設定を作成するときに次の2つの方法のいずれかを使用して、イベントログの数とボリュームの利用可能なスペースを制御できます。

- 最大数値。パラメータは、 `-rotate-limit`保持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。パラメータは、ファイルを保持できる最大期間を制御します。 `-retention-duration`

どちらのパラメータでも、構成済みの監査ファイルを超えると、古い監査ファイルを削除して新しい監査ファイル用のスペースを確保できます。両方のパラメータの値は0で、すべてのファイルを維持する必要があることを示します。したがって、十分なスペースを確保するためには、いずれ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。

監査が保証されるため、ローテーション制限の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なくなり、クライアントがデータにアクセスできなくなります。したがって、この値と監査に割り当てられるスペースは慎重に選択する必要があり、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対応する必要があります。

詳細については、を参照してください "監査の基本概念"。

S3監査の設定を計画する

S3監査の設定にはいくつかのパラメータを指定するか、デフォルトを受け入れる必要があります。特に、適切な空きスペースを確保するのに役立つログローテーションパラメータを検討する必要があります。

*`vserver object-store-server audit create`構文の詳細については、*のマニュアルページを参照してください。

一般パラメータ

監査の設定を作成するときに指定する必要がある必須パラメータが2つあります。また、指定できるオプションのパラメータも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。 SVMがすでに存在し、S3に対して有効になっている必要があります。	`-vserver` *`svm_name`*	○

_ ログデスティネーションパス _ 変換された監査ログを格納する場所を指定します。SVM上にすでに存在しているパスを指定する必要があります。 パスは最大864文字で、読み取り/書き込み権限が必要です。 パスが無効な場合、監査設定コマンドは失敗します。	`-destination text`	○
_ 監査するイベントのカテゴリ _ 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、およびDeleteObjectイベント • 管理PutBucketイベントおよび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、次のいずれかのパラメータを入力します。値を入力しない場合は、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の上限 _ 保持する監査ログファイルの数を指定します。この数を超えると、最も古いログファイルがローテーションから除外されます。たとえば、値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0は、すべてのログファイルが保持されることを示します。デフォルト値は0です。	`-rotate-limit integer`	いいえ
ログファイル継続時間制限 ログファイルが削除されるまでの保持期間を指定します。たとえば、5d0h0mと入力すると、5日以上経過したログが削除されます。 値0は、すべてのログファイルが保持されることを示します。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のパラメータ

サイズまたはスケジュールに基づいて監査ログのローテーションを実行できます。デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。

ログサイズに基づく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式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の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100MBです。

デフォルトのログサイズを使用しない場合は、カスタムログサイズを指定するようにパラメータを設定できます `-rotate-size`。

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パラメータの設定を解除し `-rotate-schedule-minute`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く監査ログのローテーションを選択した場合は、時間に基づく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。

- 時間に基づく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。
- その他の時間ベースの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、時間に関連するすべての値を使用して計算されます。たとえば、パラメータのみを指定する `-rotate-schedule-minute`と、監査ログファイルのローテーションは、毎月のすべての曜日の毎時間、指定した分に行われます。
- 時間に基づくローテーションパラメータを1つか2つだけ指定した場合（、など `-rotate-schedule-month` `-rotate-schedule-minutes`）、ログファイルのローテーションは、指定した月にのみ、すべての曜日の毎時間、指定した分に行われます。

  たとえば、監査ログのローテーションを、1月、3月、8月の月曜日、水曜日、土曜日の午前10時30分に実行するように指定できます。

- との `-rotate-schedule-day`両方に値を指定すると `-rotate-schedule-dayofweek`、それらは独立して考慮されます。

  たとえば、にFridayを指定し、 `-rotate-schedule-day`に13を指定する `-rotate-schedule-dayofweek`と、監査ログのローテーションは、13日の金曜日だけでなく、毎週金曜日、および指定した月の13日にも実行されます。

- 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の設定を解除します `-rotate-size parameter`。

  ```
  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

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するように選択するには、-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の両方を任意の組み合わせで設定します。たとえば、が10MBに設定され、 `-rotate-schedule-minute`が15に設定されている場合 `-rotate-size`、ログファイルのサイズが10MBに達したとき、または1時間ごとの15分（いずれか早い方）にログファイルがローテーションされます。

S3監査の設定を作成して有効にする

S3監査を実装するには、まずS3対応のSVMで永続的なオブジェクトストアの監査設定を作成してから、設定を有効にします。

必要なもの

- S3対応のSVM。
- アグリゲートにステージングボリューム用の十分なスペースが必要です。

タスクの内容

監査の設定は、監査対象のS3バケットを含むSVMごとに必要です。新規または既存のS3サーバでS3監査を有効にすることができます。監査の設定は、 * vserver object-store-server audit delete * コマンドで削除されるまで S3 環境で維持されます。

S3監査の設定は、監査用に選択したSVM内のすべてのバケットに適用されます。監査が有効なSVMには、監査対象バケットと未監査バケットを含めることができます。

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がローテーションされるようにS3監査を設定することを推奨します。ログの自動ローテーションを設定しない場合、すべてのログファイルがデフォルトで保持されます。S3 ログファイルのローテーションは、 * vserver object-store-server audit rotate-log * コマンドを使用して手動で実行することもできます。

SVMがSVMディザスタリカバリのソースである場合、デスティネーションパスをルートボリュームに配置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のローテーションを行うには、監査の設定を作成します。

監査ログのローテーションの基準	入力するコマンド
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	入力するコマンド
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`時間に基づく監査ログのローテーションを設定する場合、パラメータは必須です。

2. S3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）を監査する監査の設定を作成します。ログは/audit_logディレクトリに格納されます。ログファイルのサイズの上限は200MBです。ログは、サイズが200MBに達すると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）を監査する監査の設定を作成します。ログファイルのサイズの上限は100MB（デフォルト）で、ログは5日間保持されてから削除されます。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

次の例は、時間に基づく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の設定を作成します。監査ログのローテーションは、毎月、すべての曜日の午後12時30分に実行されます。ログのローテーション回数の上限は5回です。

```
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
```

S3監査のバケットを選択

監査が有効なSVMでは、監査対象のバケットを指定する必要があります。

必要なもの

- S3監査が有効になっているSVM。

タスクの内容

S3 監査の設定は SVM 単位で有効になりますが、監査用に有効になっている 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、新しいバケットを監査する場合は、この手順でバケットを選択する必要があります。SVMの監査で未監査のバケットをS3監査用に有効にすることもできます。

監査の設定は、コマンドで削除するまでバケットの設定が維持され `vserver object-store-server audit event-selector delete`ます。

手順

S3監査のバケットを選択：

```
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`-監査対象のイベントアクセスのタイプ（、 `write-only`または） `all`を指定します `read-only`（デフォルトは `all`）。
- `-permission`-監査するイベント権限のタイプ（、 `deny-only`または） `all`を指定します。 `allow-only` `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
```

S3監査の設定を変更する

SVMでは、個 々 のバケットの監査パラメータや、監査対象として選択したすべてのバケットの監査の設定を変更できます。

監査設定を変更する対象	入力するコマンド
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
```

次の例は、 SVM 内のすべてのバケットの監査の設定を変更して、ログサイズの上限を 10MB に変更し、 3 つのログファイルを保持するように変更します。

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

S3監査の設定を表示します。

監査の設定が完了したら、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。また、クラスタ内のすべてのオブジェクトストアの監査の設定に関する情報を表示することもできます。

タスクの内容

バケットとSVMの監査の設定に関する情報を表示できます。

- バケット–コマンドを使用します。 `vserver object-store-server audit event-selector show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVM内のバケットに関する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–コマンドを使用します。 `vserver object-store-server audit show`

  パラメータを指定せずにコマンドを実行すると、オブジェクトストアの監査が設定されたクラスタ内のすべてのSVMに関する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

パラメータを指定すると、表示する監査設定情報を指定できます `-fields`。

手順

S3監査の設定に関する情報を表示します。

設定を変更する対象	入力するコマンド
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上のすべてのバケットに関する情報を表示します。

```
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、イベントタイプ、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の名前と監査ログに関する詳細を表示します。

```
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