Fsas Technologies

P3AG-6642-03Z0

ETERNUS AX series オールフラッシュアレイ，ETERNUS HX series ハイブリッドアレイ

ONTAP での S3 ベストプラクティス ONTAP 9.13.1

© 2022-2025 Fsas Technologies Inc.

目次

1. 概要 8

2. 主な使用例 9

2.1 Native S3 アプリケーション 9

2.2 FabricPool エンドポイント 9

3. 要件 10

3.1 プラットフォーム 10

3.2 データ LIF 10

3.3 クラスタ LIF 10

3.4 S3 ライセンス 11

3.4.1 インストール 11

4. アーキテクチャ 12

4.1 サービスポリシー 12

4.2 オブジェクトストアサーバー 13

4.3 バケット 13

4.3.1 既定のバケット設定 14

4.4 ユーザー 14

4.5 マルチプロトコル NAS ボリューム内の S3 15

5. Native S3 アプリケーションとリモートクラスタ階層化の構成 16

5.1 ONTAP System Manager 16

5.1.1 オブジェクトストアの設定 16

5.1.2 バケットの設定 17

5.1.3 その他のオプション 18

5.1.4 ユーザーとグループの追加 20

5.2 ONTAP CLI 21

5.2.1 サービスポリシーの作成 21

5.2.2 S3 を使用するデータ LIF の作成 21

5.2.3 CA 証明書のインストール 22

5.2.4 オブジェクトストアサーバーを作成する 22

5.2.5 ユーザーの作成 23

5.2.6 root ユーザー 23

5.2.7 バケットの作成 23

6. ローカルクラスタ階層化の構成 25
6.1 ONTAP System Manager 25
6.1.1 オブジェクトストアの設定 26
6.2 ONTAP CLI 27
6.2.1 クラスタ SVM 上でのオブジェクトストアサーバーの作成 27
6.2.2 データ SVM でバケットを作成する 28
6.2.3 ユーザーの作成 28
6.2.4 オブジェクトストアとバケットを使用してクラウド層を追加する 29
6.2.5 クラウド層をローカル層にアタッチする 29

7. マルチプロトコル NAS ボリュームでの S3 の構成 30
7.1 ONTAP System Manager 30
7.1.1 SVM で S3 を有効にする 30
7.1.2 バケットの作成 31
7.1.3 ネームマッピングの有効化 31
7.1.4 バケットアクセス権の追加 32
7.2 ONTAP CLI 33
7.2.1 S3 サービスポリシーの追加 33
7.2.2 データ LIF の検証 33
7.2.3 CA 証明書のインストール 34
7.2.4 オブジェクトストアサーバの作成 34
7.2.5 バケットの作成 34
7.2.6 ネームマッピングの有効化 35
7.2.7 バケットポリシーの作成 35

8. ライフサイクルルール 36
8.1 Expiration 36
8.1.1 例 36
8.2 Noncurrent Version Expiration 37
8.2.1 例 37
8.3 Abort Incomplete Multipart Upload 38
8.3.1 例 38

9. セキュリティ 39
9.1 ローカル層 39
9.2 Over the Wire 39
9.3 署名バージョン 4 39

10. S3 SnapMirror 40
10.1 Snapshot コピー 40
10.2 S3 SnapMirror を使用したバケットの保護 40

10.3 要件 40
10.3.1 デスティネーションターゲット 40
10.3.2 ライセンス 41
10.3.3 認証局 (CA) 証明書 41
10.3.4 クラスタピア関係 41
10.3.5 クラウドオブジェクトストア 41
10.4 保護ポリシー 41

11. サポートされている S3 アクション 43
11.1 バケット 43
11.2 オブジェクト 43
11.3 グループポリシー 44
11.4 ユーザー管理 44
11.5 マルチプロトコル NAS ボリュームで未サポートのアクションと機能 44

12. リリース済みの S3 アクション 45
12.1 ONTAP 9.13.1 45
12.2 ONTAP 9.12.1 45
12.3 ONTAP 9.11.1 45
12.4 ONTAP 9.10.1 46
12.5 ONTAP 9.9.1 46

13. 相互運用性 47

図目次

図 4.1 ONTAP における S3 オブジェクトストレージのコア要素 12
図 4.2 FlexGroup ボリューム 13
図 6.1 ローカルクラスタ階層化 25

表目次

表 13.1　相互運用性 47

はじめに

本書では、ONTAP ソフトウェアで Amazon Simple Storage Service (S3) を使用するためのベストプラクティスについて説明します。また、ONTAP を Native S3 アプリケーションのオブジェクトストアとして、または FabricPool の階層化先として使用するための機能と構成についても説明します。

第 3 版
2025 年 3 月

登録商標

本製品に関連する他社商標については、以下のサイトを参照してください。
https://www.fujitsu.com/jp/products/computing/storage/trademark/
本書では、本文中の™、® などの記号は省略しています。

本書の読み方

対象読者

本書は、ETERNUS AX/HX の設定、運用管理を行うシステム管理者、または保守を行うフィールドエンジニアを対象としています。必要に応じてお読みください。

関連マニュアル

ETERNUS AX/HX に関連する最新の情報は、以下のサイトで公開されています。
https://www.fujitsu.com/jp/products/computing/storage/manual/

本書の表記について

本文中の記号

本文中では、以下の記号を使用しています。

注意	お使いになるときに注意していただきたいことを記述しています。必ずお読みください。
備考	本文を補足する内容や、参考情報を記述しています。

1. 概要

ONTAP 9.8 以降の ONTAP ソフトウェアでは、Amazon Simple Storage Service (S3) をサポートしています。ONTAP は AWS S3 API アクションのサブセットをサポートし、ONTAP ベースのシステムである ETERNUS AX/HX でデータをオブジェクトとして扱うことを可能にしています。

2. 主な使用例

ONTAP での S3 の主な使用目的は、ONTAP ベースのシステム上のオブジェクトをサポートすることです。ONTAP 統合ストレージアーキテクチャでは、ファイル（NFS および SMB）、ブロック（FC および iSCSI）、およびオブジェクト（S3）がサポートされるようになりました。

2.1 Native S3 アプリケーション

ONTAP が S3 を使用したオブジェクトをサポートすることを必要とするお客様が増えています。大容量のアーカイブワークロードに適していますが、Native S3 アプリケーションに対する需要は急速に高まっており、以下のようなものがあります。

- 分析
- AI
- エッジツーコアインジェスト
- 機械学習

お客様は、ONTAP System Manager などの使い慣れた管理ツールを使用して、ONTAP での開発と運用のため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 の活用が可能になりました。これによって、ストレージの効率性とセキュリティが向上します。

ONTAP 9.12.1 以降では、NAS プロトコルを使用するようにあらかじめ構成されたマルチプロトコル NAS ボリュームでも、S3 プロトコルを有効にできます。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ようになり、用途が多様化します。最も一般的な使用例は、NAS クライアントでボリュームにデータを書き込み、S3 クライアントで同じデータを読み取って、分析、ビジネスインテリジェンス、機械学習、光学文字認識 (OCR) などの特殊なタスクを実行する場合です。

2.2 FabricPool エンドポイント

ONTAP 9.8 以降では、FabricPool で ONTAP のバケットへの階層化がサポートされるようになり、ONTAP から ONTAP への階層化が可能になりました。これは、既存の ETERNUS AX/HX インフラストラクチャをオブジェクトストアエンドポイントとして再利用したいお客様に最適なオプションです。

FabricPool は、以下の 2 つの方法で ONTAP への階層化をサポートします。

- **ローカルクラスタ階層化**
  非アクティブなデータは、クラスタ LIF を使用して、ローカルのクラスタにあるバケットに階層化されます。
- **リモートクラスタ階層化**
  FabricPool クライアント上のインタークラスタ LIF と ONTAP オブジェクトストアのデータ LIF を用いる従来の FabricPool クラウド層と同様に、非アクティブなデータはリモートクラスタ上にあるバケットに階層化されます。

300TB を超える使用頻度の低いデータを階層化する場合、最高クラスのオブジェクトストアソリューションである StorageGRID または FJcloud-o の使用を推奨します。ONTAP、StorageGRID、または FJcloud-o をクラウド層として使用する場合、FabricPool ライセンスは必要ありません。

3. 要件

3.1 プラットフォーム

- **ETERNUS AX series**
  S3 は、ONTAP 9.8 以降を使用するすべての ETERNUS AX プラットフォームでサポートされます。
- **ETERNUS HX series**
  S3 は、ONTAP 9.8 以降を使用するすべての ETERNUS HX プラットフォームでサポートされます。
- **Cloud Volumes ONTAP**
  - S3 は、ONTAP 9.9 以降を使用する Cloud Volumes ONTAP for Azure および FUJITSU Hybrid IT Service for Microsoft Azure の Cloud Volumes ONTAP でサポートされています。
  - S3 は、ONTAP 9.11 以降を使用する Cloud Volumes ONTAP for AWS および Amazon FSx for NetApp ONTAP でサポートされています。
  - S3 は、ONTAP 9.12 以降を使用する Cloud Volumes ONTAP for Google Cloud でサポートされています。

3.2 データ LIF

オブジェクトストアサーバーをホストするストレージ仮想マシン（SVM）には、S3 を使用してクライアントアプリケーションと通信するためのデータ LIF が必要です。リモートクラスタ階層化用に構成されている場合、FabricPool はクライアントで、オブジェクトストアはサーバーです。

3.3 クラスタ LIF

ローカルクラスタ階層化用に設定されている場合、ローカル層（ONTAP CLI ではストレージアグリゲートとも呼ばれます）はローカルバケットに割り当てられます。FabricPool は、クラスタ内トラフィックにクラスタ LIF を使用します。

注意

クラスタ LIF のリソースが飽和状態になると、パフォーマンスが低下する場合があります。これを回避するために、ローカルバケットへの階層化時に 4 ノード以上のクラスタを使用することをお勧めします。推奨するベストプラクティスは、ローカル層とローカルバケットにそれぞれ HA ペアを使用することです。単一 HA ペアでのローカルバケットへの階層化はお勧めしません。

3.4 S3 ライセンス

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 ライセンスは無料のライセンスですが、システムを ONTAP9.8 にアップグレードする必要があります。

新しい ONTAP 9.8 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。

S3 ライセンスは、以下のサイトからダウンロードできます。
https://storage-system.fujitsu.com/fjidauth/firmware/axhx/

3.4.1 インストール

S3 ライセンスをインストールするには、ONTAP CLI で以下のコマンドを実行します。

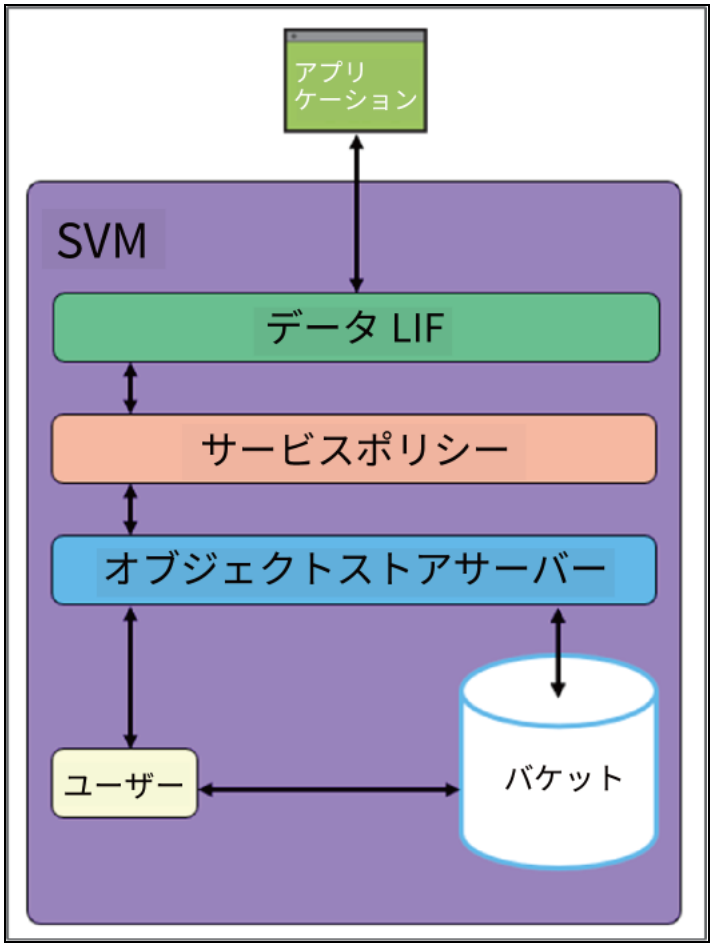
```
system license add <license_key>
```

4. アーキテクチャ

オブジェクトストレージは、ファイルやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理するアーキテクチャです。オブジェクトは単一のコンテナ（バケットなど）内に保持され、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。

オブジェクトストレージは、ファイルストレージやブロックストレージよりもパフォーマンスが劣る場合がありますが、非常にスケーラブルであり、数ペタバイトのデータを含むバケットも珍しくありません。

図 4.1　ONTAP における S3 オブジェクトストレージのコア要素



4.1 サービスポリシー

データサービスポリシーは SVM に割り当てられており、データ LIF がクライアントアプリケーションプロトコルをサポートするために必要なネットワークサービス一式を提供します。たとえば、data-nfs は NFS トラフィックのサポートに使用され、data-iscsi は iSCSI トラフィックのサポートに使用されます。

ONTAP 9.8 で新しく導入された data-s3-server サービスを使用すると、S3 を使用するクライアントアプリケーションのトラフィックをデータ LIF がサポートできるようになります。

備考

LIF を用いるアプリケーションを期待通りに動かすために、data-s3-server サービスに加えて、すべてのサービスポリシーに data-core サービスを必ず含めるようにしてください。

4.2 オブジェクトストアサーバー

SVM のオブジェクトストアサーバーは、ファイルやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。バケットおよびユーザーのアクセス許可レベルの管理も、オブジェクトストアサーバーレベルで行われます。

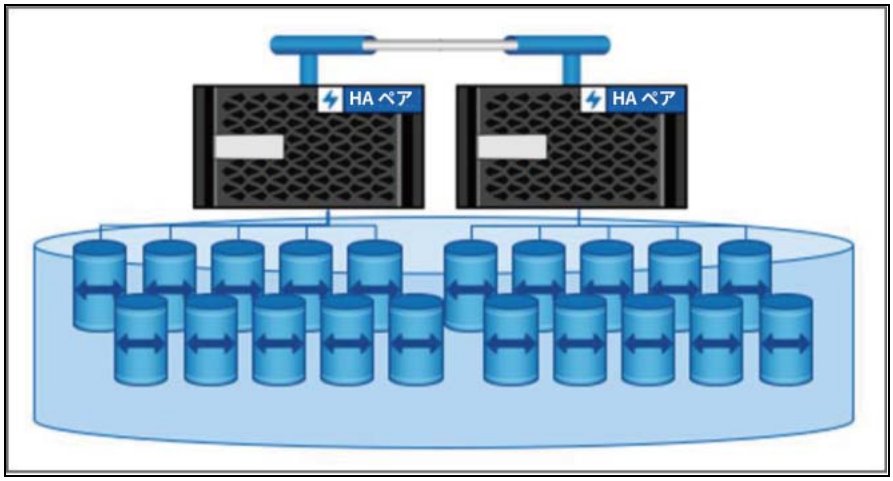
ONTAP S3 は、SVM ごとに 1 つのオブジェクトストアサーバーをサポートします。

4.3 バケット

ONTAP では、バケットの基盤となるアーキテクチャは、図 4.2 に示すように、FlexGroup ボリューム（複数のメンバーボリュームで構成されるが、1 つのボリュームとして管理される単一のネームスペース）です。バケット内の個々のオブジェクトは個々のメンバーボリュームに割り当てられ、ボリュームまたはノード間でストライプ化されません。一つのバケットを 96GB 未満でプロビジョニングすることはできません。

FlexGroup ボリュームの詳細については、マニュアルサイトの「ONTAP FlexGroup ボリューム技術概要」を参照してください。

図 4.2 FlexGroup ボリューム



バケットで使用される場合、FlexGroup ボリュームはボリューム自動拡張ではなく、エラスティックサイジングを使用します。FlexGroup ボリュームの最大容量は、基盤となるハードウェアの物理的な最大容量によってのみ制限され、10 ノードのクラスタで 20PB および 4000 億ファイルまでが検証済みです。

ONTAP S3 は最大 12,000 個のバケットをサポートしますが、単一の FlexGroup ボリュームに作成されるバケットは 1,000 個までです。

Amazon S3 の最大オブジェクトサイズは 5TB です。ONTAP S3 は、最大 16TB のオブジェクトをサポートします。Amazon が定義した最大オブジェクトサイズを超えることができないため、オブジェクトが 5TB を超えた場合、クライアントとの相互運用に問題が発生する場合があります。

備考

ONTAP 9.7（FlexGroup ボリュームごとに 1 つのバケット）と ONTAP 9.8 以降（FlexGroup ボリュームごとに複数のバケット）の間で根本的なアーキテクチャ変更を行うことはできません。新しいアーキテクチャの恩恵を受けるためには、既存のバケットから ONTAP 9.8 以降のバケットにデータを移行する必要があります。

4.3.1 既定のバケット設定

手動で設定されていないバケットでは、アグリゲート、FlexGroup、およびバケットのプロビジョニングにデフォルト設定が使用されます。

アグリゲート

バケットをサポートする FlexGroup ボリュームは、以下の優先順位を使用してアグリゲートにプロビジョニングされます。

- Flash Pool アグリゲート
- HDD アグリゲート
- SSD アグリゲート

FlexGroup ボリューム

デフォルトの FlexGroup サイズは大きく、ほとんどの環境で拡張領域が大きくなります。

- ONTAP で 1.6PB

クラスタにデフォルトサイズをプロビジョニングするための十分な容量がない場合、既存の環境でプロビジョニングできるようになるまで 50% ずつサイズを削減します。たとえば、300TB の環境では、FlexGroup ボリュームは 200TB で自動的にプロビジョニングされます。（1.6PB、800TB、400TB の FlexGroup ボリュームでは、環境に対して大きすぎるため。）

バケット

デフォルトのバケットサイズは以下のとおりです。

- ONTAP で 800GB

バケット拡張用の容量を提供するには、FlexGroup ボリューム上のすべてのバケットの合計容量が FlexGroup ボリューム容量の 33% 未満である必要があります。これが満たされない場合、作成中のバケットは新しく作成された FlexGroup ボリュームに自動的にプロビジョニングされます。

4.4 ユーザー

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー許可が必要です。特定のバケットまたは S3 アクションへのアクセスは、ユーザーレベルで許可、拒否、または条件付きにすることができます。

ONTAP S3 は、オブジェクトストアごとに 4,000 ユーザーをサポートします。

4.5 マルチプロトコル NAS ボリューム内の S3

S3 をマルチプロトコル NAS ボリューム (ONTAP 9.12.1 以降) で使用する場合、S3 は既存の NAS 階層にマッピングされます。たとえば、バケットはボリュームまたはボリューム内のディレクトリにマッピングされます。ファイル、ディレクトリ、ユーザー権限などの NAS セキュリティ設定は、NFS 設定と SMB 設定が相互にマッピングされるのと同じ方法で保存され、S3 ユーザーにマッピングされます。

オブジェクトはファイルにマッピングされ、ディレクトリ / ファイルに対応したフォルダ / オブジェクトを持つ、NAS 階層を基盤とした命名スキームに基づいて S3 クライアントに提供されます。

注意

基盤となるアーキテクチャはオブジェクトベースではなくファイルベースであるため、マルチプロトコル NAS ボリューム内の S3 では、ネイティブの S3 を使用する場合にはない NAS 関連の制限が課せられます。たとえば、ファイル名とディレクトリ名は最大で 255 文字と 1024 バイトのパスに制限されるため、対応するオブジェクト名も最大で 255 文字と 1024 バイトに制限されます。

5. Native S3 アプリケーションとリモートクラスタ階層化の構成

Native S3 アプリケーションや FabricPool クライアントなどの外部クライアントは、データ LIF を使用して ONTAP オブジェクトストアに接続します。ONTAP でオブジェクトストアを作成する最も簡単な方法は、ONTAP System Manager を使用することです。当社が推奨するベストプラクティスを使用すると、CLI を使用するときに複数のステップを必要とするプロセスを数クリックで実行できます。より多くのカスタム設定を行うには、CLI による設定が必要です。

5.1 ONTAP System Manager

ONTAP System Manager を使用してオブジェクトストア、バケット、および権限ユーザーを作成するには、以下の手順に従ってください。

5.1.1 オブジェクトストアの設定

オブジェクトストアを設定するには、以下の手順を実行します。

1. ONTAP System Manager を起動します。
2. [ストレージ] をクリックします。
3. [Storage VM] をクリックします。
4. [追加] をクリックします。

   新しい SVM は必要ありません。S3 機能は、SVM の Settings メニューを使用して既存の SVM に追加できます。
5. SVM に名前を付けます。
6. アクセスプロトコルとして [Enable S3] を選択します。

   [TLS を有効にする]（ポート 443）および [システムで生成された証明書を使用する] オプションは、デフォルトで選択されています。サードパーティの認証局が発行する署名付き証明書を使用することをお勧めします。
7. S3 サーバーに名前を付けます。

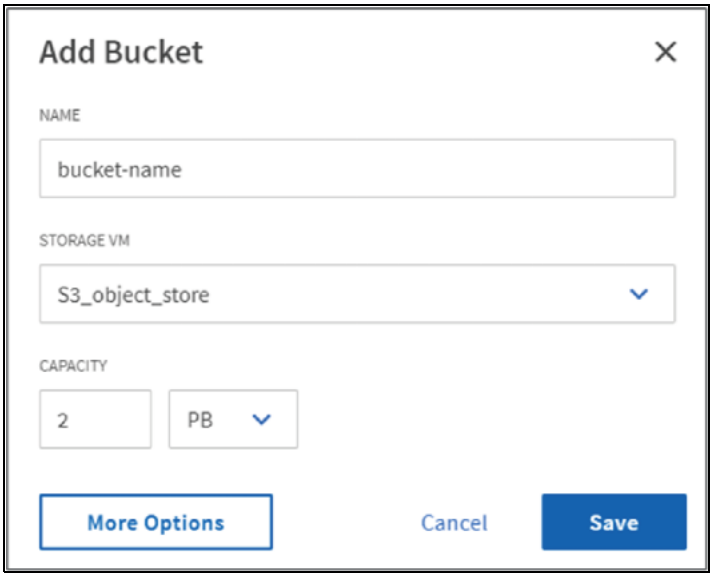
   備考

   サーバー名は、クライアントアプリケーションによって完全修飾ドメイン名 （FQDN）として使用されます。
8. ノードのネットワークインターフェースを入力します。

5.1.2 バケットの設定

バケットを設定するには、以下の手順を実行します。

1. ONTAP System Manager を起動します。
2. [ストレージ] をクリックします。
3. [バケット] をクリックします。
4. [追加] をクリックします。
5. バケットに名前を付けます。
6. バケットを割り当てる SVM/ オブジェクトストアを選択します。これは、前に作成した SVM/ オブジェクトストアと同じである必要があります。
7. [Save] をクリックします。



5.1.3 その他のオプション

階層化に使用

このオプションを選択すると、ONTAP System Manager は HDD > SSD > NVMe の順に最も安価なメディアにバケットを作成します。

パフォーマンスサービスレベル

バケットの適切な Quality of Service (QoS) を選択します。以下のオプションがあります。

- **Extreme**
  50,000 IOPS; 1562MBps
- **Performance**
  30,000 IOPS; 937MBps
- **Value**
  15,000 IOPS; 468MBps
- **Custom**
  既存の QoS ポリシーを使用するか、新しいポリシーを作成します。

> **備考**
>
> バケットが階層化に使用されている場合、パフォーマンスサービスレベルは選択できません。FabricPool は、QoS の最小値をサポートしません。

アクセス許可

既存のバケットからアクセス許可をコピーするか、アクセス許可を新規作成します。

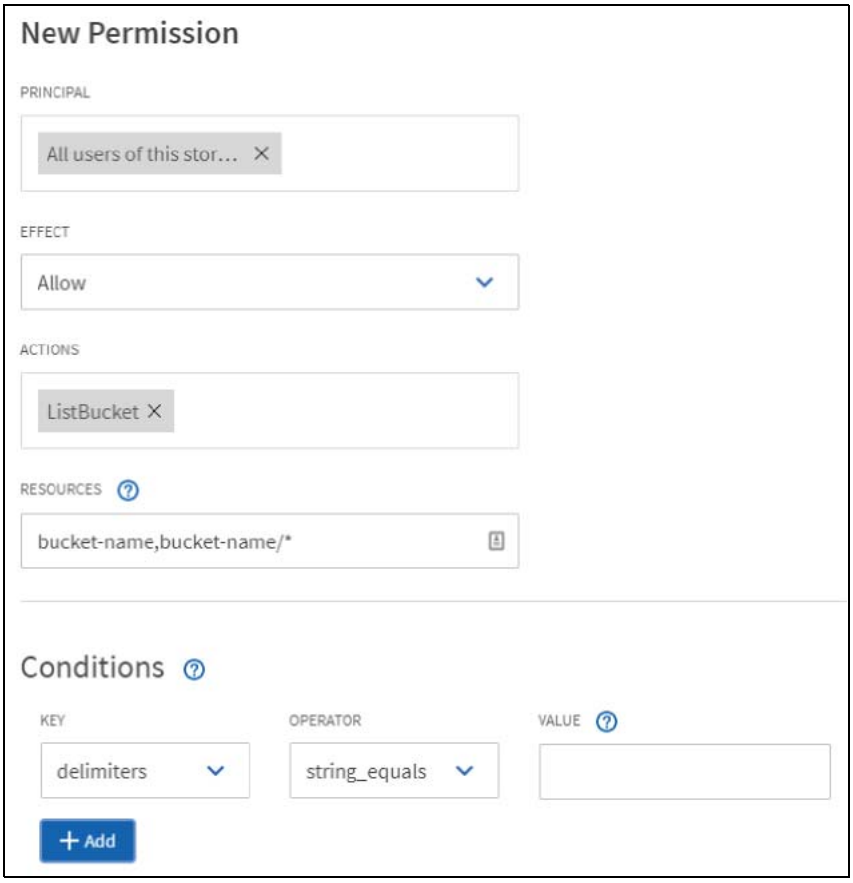
> **備考**
>
> ユーザーとグループは、アクセスを許可する前に設定する必要があります。「5.1.4 ユーザーとグループの追加」(P.20) を参照してください。

新しいアクセス許可を作成するには、以下の手順を実行します。

1. [Add Bucket] ページから、[Permissions] までスクロールダウンし、[Add] をクリックします。
2. プリンシパルユーザーを設定します。
   オプションには、SVM のすべてのユーザー（デフォルト）、すべてのパブリックユーザーと匿名ユーザー、および SVM に関連付けられた個々のユーザーが含まれます。
3. 効果を設定します。
   オプションには、[Allow]（デフォルト）と [Deny] があります。
4. アクションを設定します。
5. リソースを設定します。
   デフォルトでは "bucket-name" と "bucket-name/*" が使用されます。
6. 条件を設定します。

7 条件を追加します。

最大 10 個の条件文を追加できます。各条件ステートメントは、キー、演算子、および 1 つ以上の値で構成されます。



5.1.4 ユーザーとグループの追加

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー許可が必要です。アクセス許可を使用すると、特定のバケットまたは S3 アクションへのアクセスが、ユーザーレベルで許可、拒否、または条件付きにすることができます。

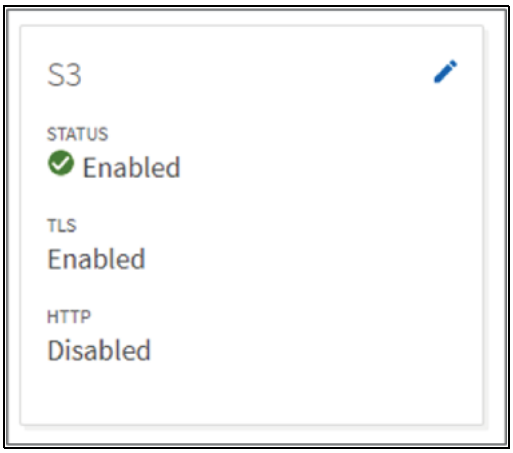
ONTAP S3 は、オブジェクトストアまたは SVM ごとに 4,000 ユーザーをサポートします。

備考

デフォルトでは、バケットの作成時にルートユーザー（UID 0）が作成されます。root ユーザーは、すべてのバケットとオブジェクトにフルアクセスできます。クライアントアプリケーションアクセスには root ユーザーを使用しないでください。クライアントアクセス用に追加のユーザーを作成する必要があります。

ユーザーとグループを管理するには、以下の手順で行います。

1. ONTAP System Manager を起動します。
2. [ストレージ] をクリックします。
3. [Storage VM] をクリックします。
4. ユーザーおよびグループを追加する SVM を選択します。
5. S3 protocol ボックスの [Edit] アイコンをクリックします。



6. [Users] または [Groups] タブを選択します。
7. [Add] をクリックします。
8. ユーザーまたはグループの名前を指定します。
9. 後で使用するために、アクセスキーと秘密キーをコピーまたはダウンロードします。

   備考

   シークレットキーは再表示されません。

10. グループを設定する場合は、ユーザーとポリシーを割り当てます。
11. ユーザーを設定する場合は、Permissions メニューを使用します。

5.2 ONTAP CLI

ONTAP でオブジェクトストアを作成する最も簡単な方法は ONTAP System Manager を使用することですが、ONTAP System Manager を使用してオブジェクトストアを作成した場合、カスタマイズできる項目が少なくなります。

たとえば、ONTAP System Manager はストレージのバケットで使用するローカル層 （アグリゲート）を自動的に選択します。その際は推奨されるベストプラクティスが使用されますが、複雑な環境では、選択されたローカル層は、経験豊富なストレージ管理者が使用するものとは異なる場合があります。

カスタム設定には、ONTAP CLI を使用した設定が必要です。

ONTAP CLI を使用してオブジェクトストア、バケット、および権限ユーザーを作成するには、以下の手順を実行します。

1. サービスポリシーを作成します。
2. S3 を使用するデータ LIF を作成します。
3. CA 証明書をインストールします。
4. オブジェクトストアサーバーを作成します。
5. バケットを作成します。
6. ユーザーを作成します。

5.2.1 サービスポリシーの作成

SVM LIF で S3 データトラフィックを有効にするには、サービスポリシーが必要です。

ONTAP CLI を使用してサービスポリシーを作成するには、以下のコマンドを実行します。

```
network interface service-policy create
-vserver <name>
-policy <name>
-services data-s3-server, data-core
```

備考

LIF を用いるアプリケーションを期待したとおり確実に動かすためには、data-s3-server サービスに加えて、すべてのサービスポリシーに data-core サービスを含める必要があります。

5.2.2 S3 を使用するデータ LIF の作成

オブジェクトストアサーバーをホストするストレージ仮想マシン（SVM）には、S3 を使用してクライアントアプリケーションと通信するためのデータ LIF が必要です。当社では、ベストプラクティスとして、すべてのノードに S3 データ LIF を作成することを推奨しています。

リモートクラスタ階層化用に構成されている場合、FabricPool はクライアントで、オブジェクトストアはサーバーです。FabricPool ではオブジェクトストアが FQDN を使用する必要があるため、すべての S3 DATA LIF は、オブジェクトストアサーバーによって使用される FQDN に関連付けられている必要があります。

備考

DNS エントリの作成は ONTAP の外部で行われます。当社では、すべての S3 データ LIF IP アドレスを使用する単一のホストエントリを作成することをお勧めします。
dns-zone 設定は ONTAP DNS ロードバランシング用です。

ONTAP CLI を使用してサービスポリシーを使用する LIF を作成するには、以下のコマンドを実行します。

```
network interface create
-vserver <name>
-lif <name>
-service-policy <name>
-home-node <node>
-home-port <port>
-address <number>
-netmask <number>
-status-admin up
```

5.2.3 CA 証明書のインストール

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ーの間に信頼関係が作成されます。リモートクライアントからアクセス可能なオブジェクトストアとして使用する前に、ONTAP に CA 証明書をインストールする必要があります。

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が発行した署名付き証明書を使用することをお勧めします。

ONTAP CLI を使用して CA 証明書をインストールするには、以下のコマンドを実行します。

```
security certificate install -type server -vserver <name> -type server
```

5.2.4 オブジェクトストアサーバーを作成する

SVM のオブジェクトストアサーバーは、ファイルやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。

ONTAP CLI を使用してオブジェクトストアサーバーを作成するには、以下のコマンドを実行します。

```
vserver object-store-server create
-vserver <name>
-object-store-server <FQDN>
-certificate-name <name>
-secure-listener-port <443>
-is-http-enabled <false>
```

備考

FabricPool は、DNS を介して S3 データ LIF で使用されるすべての IP アドレスにこの名前解決をする必要があります。

5.2.5 ユーザーの作成

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー認証が必要です。

備考

有効なアクセス権と秘密キーペアを持つすべての S3 ユーザーは、SVM 内のすべてのバケットとオブジェクトにアクセスできます。

ONTAP CLI を使用してユーザーを作成するには、以下のコマンドを実行します。

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

ONTAP CLI を使用してユーザーのアクセスと秘密キーを表示するには、以下のコマンドを実行します。

備考

高度な権限レベルが必要です。

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

5.2.6 root ユーザー

デフォルトでは、バケットの作成時にルートユーザー（UID 0）が作成されます。root ユーザーは、すべてのバケットとオブジェクトにフルアクセスできます。クライアントアプリケーションアクセスには root ユーザーを使用しないでください。クライアントアクセス用に追加のユーザーを作成する必要があります。

ONTAP 管理者は、`object-store-server users regenerate-keys` コマンドを実行して、このユーザーのアクセスキーと秘密キーを設定する必要があります。

5.2.7 バケットの作成

ONTAP CLI を使用してバケットを作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type s3
-used-as-capacity-tier <true|false>
-aggr-list <aggregate name>, <aggregate name> (option for non-capacity tier)
-exclude-aggr-list <aggregate name>, <aggregate name> (option for capacity tier)
-aggr-list-multiplier <number of constituent volumes per aggregate> (default 4)
-size <size>
```

ONTAP 9.11.1 以降、ONTAP S3 ではバケットのバージョニングがサポートされています。バージョニングを有効にすると、ひとつのオブジェクトに対して複数のバージョンを作成できます。これらのオブジェクトは、スナップショットコピーと同様に取得およびリストアが可能です。これにより、クライアントアプリケーションで削除されたオブジェクトをリストアしたり、オブジェクトの以前のバージョンを取得したりできます。

ONTAP CLI を使用してバケットを作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket modify
-vserver <name>
-bucket <name>
-versioning-state <disabled|enabled|suspend>
```

備考

デフォルトのバージョニング状態は、「disabled」に設定されています。

6. ローカルクラスタ階層化の構成

ONTAP 9.8 以降では、FabricPool で ONTAP のバケットへの階層化がサポートされるようになり、ONTAP から ONTAP への階層化が可能になりました。これは、既存の ETERNUS AX/HX インフラストラクチャをオブジェクトストアエンドポイントとして再利用したいお客様に最適なオプションです。

ローカルクラスタの階層化を設定する場合、非アクティブデータはクラスタ LIF を使用して、ローカルアグリゲート（通常は SSD）からローカルバケット（通常は HDD）に階層化されます。

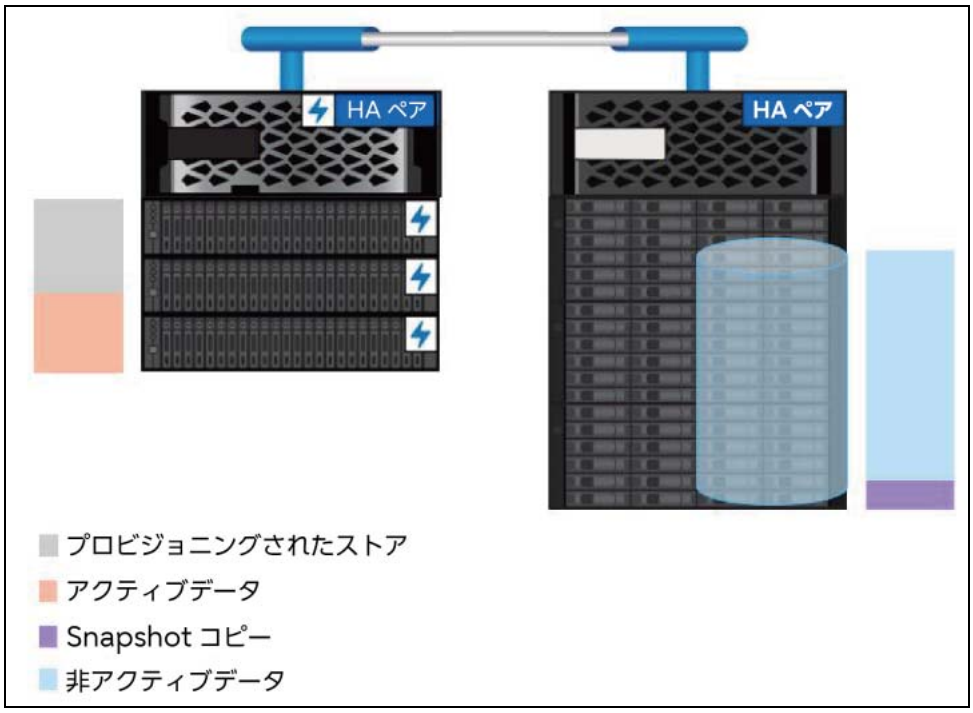
300TB を超える使用頻度の低いデータを階層化する場合、最高クラスのオブジェクトストアソリューションである StorageGRID の使用を推奨します。クラウド層として ONTAP または StorageGRID を使用する場合、FabricPool ライセンスは必要ありません。

FabricPool の詳細については、マニュアルサイトの「FabricPool のベストプラクティス」を参照してください。

注意

クラスタ LIF のリソースが飽和状態になると、パフォーマンスが低下する場合があります。これを回避するために、ローカルバケットへの階層化時に 2 ノード以上のクラスタを使用することをお勧めします。推奨するベストプラクティスは、ローカル層とローカルバケットにそれぞれ HA ペアを使用することです。単一ノードクラスタでのローカルバケットへの階層化はお勧めしません。

図 6.1　ローカルクラスタ階層化



6.1 ONTAP System Manager

ONTAP でローカル階層化用のオブジェクトストアを作成する最も簡単な方法は、ONTAP System Manager を使用することです。これにより、CLI を使用する際の複数の手順が数回クリックするだけで完了します。
ONTAP System Manager を使用して作成されたオブジェクトストアでは、カスタマイズできる項目が少なくなりますが、当社が推奨するベストプラクティスがデフォルトで使用されます。カスタム設定には、CLI による設定が必要です。

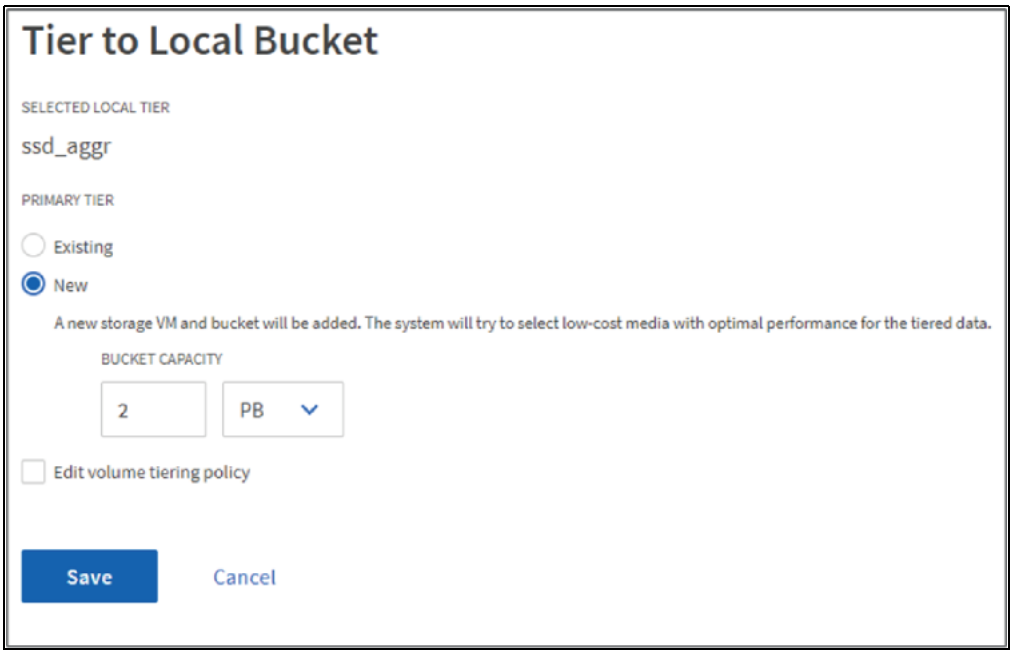
6.1.1 オブジェクトストアの設定

ローカルクラスタ階層化に使用するオブジェクトストアを作成するには、以下の手順を実行します。

1. ONTAP System Manager を起動します。
2. [STORAGE] をクリックします。
3. [Tiers] をクリックします。
4. ローカル層を選択します。
5. [More] をクリックします。
6. [Tier to Local Bucket] を選択します。
7. これがシステムの最初のローカルバケットである場合は、[New] を選択します。
   新しい SVM、オブジェクトストアサーバー、およびバケットが作成されます。ONTAP System Manager は HDD > QLC > TLC > NVMe の順に最も安価なメディアにバケットを作成します。
   ローカルバケットがすでに作成されている場合は、[Existing] を選択します。

   備考

   クラスタ内のすべてのローカル FabricPool 層に同じローカルバケットを割り当てると、最適化されたボリューム移動が可能になります。ボリュームの移動先となるローカル層が移動元のローカル層と同じバケットを使用している場合、バケットに保存された移動元ボリュームのデータはローカル層に戻りません。最適化されたボリューム移動により、ネットワーク効率が大幅に向上します。



8. バケット容量を設定します。
9. ボリューム階層化ポリシーを編集します（オプション）。
10. [Save] をクリックします。

6.2 ONTAP CLI

ONTAP でローカル階層化用のオブジェクトストアを作成する最も簡単な方法は ONTAP System Manager を使用することですが、ONTAP System Manager を使用してオブジェクトストアを作成した場合、カスタマイズできる項目が少なくなります。

たとえば、ONTAP System Manager はストレージのバケットで使用するローカル層 （アグリゲート）を自動的に選択します。その際、ONTAP System Manager は推奨されるベストプラクティスを使用しますが、複雑な環境では、選択されたローカル層は、経験豊富なストレージ管理者が使用するものとは異なる場合があります。

カスタム設定には、ONTAP CLI を使用した設定が必要です。

ONTAP CLI を使用してローカル階層化用のオブジェクトストアとバケットを作成するには、以下の手順を実行します。

1. クラスタ SVM 上にオブジェクトストアサーバーを作成します。
2. データ SVM にバケットを作成します。
3. ユーザーを作成します。
4. オブジェクトストアとバケットを使用してクラウド層を追加します。
5. クラウド層をローカル層に割り当てます。

6.2.1 クラスタ SVM 上でのオブジェクトストアサーバーの作成

ONTAP CLI を使用してクラスタ SVM 上にオブジェクトストアサーバーを作成するには、以下のコマンドを実行します。

```
vserver object-store-server create
-vserver Cluster
-object-store-server <name> (This is the FGDN used by FabricPool)
-is-http-enabled true
-is-https-enabled false
-status-admin up
```

認証局（CA）が発行する証明書をインストールして使用することをお勧めしますが、ローカルで階層化する場合は CA 証明書をインストールする必要はありません。証明書を使用しない場合は、HTTP を有効にし、HTTPS を無効にする必要があります。

object-store のアクセス許可を設定する

アクセス許可は、オブジェクトストア内のすべての（または指定された）バケットに適用されるオブジェクトストアレベルで設定できます。ONTAP CLI を使用してオブジェクトストアポリシーステートメントを設定するには、以下のコマンドを実行します。

```
vserver vserver object-store-server policy statement create
-vserver <data svm>
-policy <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name>
```

6.2.2 データ SVM でバケットを作成する

ONTAP CLI を使用してバケットを作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type s3
-used-as-capacity-tier true
-exclude-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constituent volumes per aggregate> (default 4)
-size <size> (95GB minimum)
```

備考

`-aggr-list` を使用するには高度な権限が必要です。

バケットのアクセス許可を設定する

ONTAP CLI を使用してバケットのアクセス許可ステートメントを設定するには、以下のコマンドを実行します。

```
vserver vserver object-store-server bucket policy add-statement
-vserver <data svm>
-bucket <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name, bucket-name/*>
```

備考

匿名アクセスを追加するには、プリンシパルの属性に「*」を設定する必要があります。

6.2.3 ユーザーの作成

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー許可が必要です。

備考

有効なアクセス権と秘密キーペアを持つすべての S3 ユーザーは、SVM 内のすべてのバケットとオブジェクトにアクセスできます。

ONTAP CLI を使用してユーザーを作成するには、以下のコマンドを実行します。

```
vserver object-store-server user create
-vserver <name>
-user <name>
```

ONTAP CLI を使用してユーザーのアクセスと秘密キーを表示するには、以下のコマンドを実行します。

備考

高度な権限レベルが必要です。

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

ユーザーグループ

ユーザーは、オブジェクトストアレベルまたはバケットレベルでポリシーステートメントに関連付けることができるグループに追加できます。ONTAP CLI を使用して、グループポリシーの作成と作成したグループポリシーへのユーザー追加を実施するには、以下のコマンドを実行します。

```
vserver vserver object-store-server group create
-vserver <data svm>
-name <group name>
-users <user1, user2, etc.
-policy <policy name>
```

6.2.4 オブジェクトストアとバケットを使用してクラウド層を追加する

ONTAP CLI を使用してクラウド層を追加するには、以下のコマンドを実行します。

```
storage aggregate object-store config create
-object-store-name <name the cloud tier>
-provider-type ONTAP_S3
-server <name of the Cluster svm object store server>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ipspace Cluster
-ssl-enabled <true/false>
-is-certificate-validation-enabled true
-use-http-proxy false
-url-stle <path-style/virtual-hosted-stle>
```

6.2.5 クラウド層をローカル層にアタッチする

ONTAP CLI を使用してローカルバケット階層をローカル層（ストレージアグリゲート）に割り当てる場合は、以下のコマンドを実行します。

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <cloud tier name>
```

注意

ローカルバケットのローカル層への割り当ては、永続的なアクションです。一度ローカルバケットを割り当てると、ローカル層から割り当てを解除することができません。

7. マルチプロトコル NAS ボリュームでの S3 の構成

ONTAP 9.12.1 以降では、NFS または SMB クライアントにサービスを提供するようにあらかじめ完全に構成された NAS ボリュームで S3 を有効にできます。NFS や SMB をサポートしていても、データを提供するように構成されていないボリュームで S3 プロトコルを有効にしても、機能しません。ONTAP は、S3 ユーザーを Unix または Windows のセキュリティスタイルで作成された既存のユーザーにマップできる必要があります。NFS または SMB クライアントにサービスを提供するように設定されていない NAS ボリュームで S3 を有効にしても、機能しません。

NAS プロトコルを有効にするには、以下のリソースを参照してください。

- NFS を使用した Linux サーバー用の NAS ストレージのプロビジョニング
- SMB を使用した Windows サーバー用の NAS ストレージのプロビジョニング

注意

マルチプロトコル NAS ボリュームは、NAS 階層およびファイルをバケットおよびオブジェクトとして提供する NAS ボリュームです。マルチプロトコル NAS ボリュームで S3 を使用する場合、メタデータ、マルチパートオブジェクト、タグ、およびバージョニングに関連付けられたアクションと機能はサポートされません。これらのアクションと機能を必要とするクライアントは、ネイティブの ONTAP S3 を使用する必要があります。

7.1 ONTAP System Manager

ONTAP でマルチプロトコル NAS ボリュームの S3 を有効にするには、ONTAP System Manager を使用することが最も簡単です。これにより、CLI で必要な複数の手順が数回のクリックだけで完了します。ONTAP System Manager を使用して作成されたオブジェクトストアではカスタマイズのできる項目が少なくなりますが、当社が推奨するベストプラクティスに従ったオブジェクトストアがデフォルトで作成されます。カスタム設定には、CLI による設定が必要です。

ONTAP System Manager を使用してマルチプロトコル NAS ボリュームの S3 を有効にするには、以下の手順を実行します。

1. SVM で S3 を有効にします。
2. バケットを作成します。
3. ネームマッピングを有効にします。
4. バケットのアクセス許可を追加します。

7.1.1 SVM で S3 を有効にする

1. ONTAP System Manager を起動します。
2. [ストレージ] をクリックします。
3. [Storage VM] をクリックします。
4. NFS または SMB/CIFS プロトコルを使用するように設定された SVM を選択します。

5 [設定] をクリックします。

6 S3 の歯車アイコンをクリックします。

7 S3 サーバーに名前を付けます。

> **備考**
>
> サーバー名は、クライアントアプリケーションによって完全修飾ドメイン名 （FQDN）として使用されます。

8 アクセスプロトコルとして [有効化 S3] を選択します。[TLS を有効にする]（ポート 443）および [システムで生成された証明書を使用する] オプションは、デフォルトで選択されています。サードパーティの認証局が発行する署名付き証明書を使用することをお勧めします。

9 ノードのネットワークインターフェースを入力します。

7.1.2 バケットの作成

1 [ストレージ] をクリックします。

2 [バケット] をクリックします。

3 [追加] をクリックします。

4 バケットに名前を付けます。

5 バケットを割り当てる SVM/ オブジェクトストアを選択します。SVM/ オブジェクトストアは、以前にマルチプロトコル SVM で作成した S3 サーバーと同一である必要があります。[その他のオプション] をクリックすると、バケットをボリューム内の特定のフォルダーにマッピングできます。

> **備考**
>
> マルチプロトコル NAS ボリューム内の S3 バケットは、FabricPool クラウド層の階層化としては使用できません。

6 [保存] をクリックします。

7.1.3 ネームマッピングの有効化

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー許可が必要です。ユーザー許可を使用すると、特定のバケットまたは S3 アクションへのアクセスが、ユーザーまたはグループレベルで許可、拒否、または条件付きにすることができます。

ONTAP S3 は、オブジェクトストアまたは SVM ごとに 4,000 ユーザーをサポートします。

注意

デフォルトでは、バケットの作成時に root ユーザー（UID 0）が作成されます。root ユーザーには、すべてのバケットとオブジェクトのフルアクセス権限があります。クライアントアプリケーションへのアクセスには、root ユーザーを使用しないでください。クライアントアクセス用に追加のユーザーを作成する必要があります。

ユーザーとグループを管理するには、以下の手順で行います。

1. [ストレージ] をクリックします。
2. [Storage VM] をクリックします。
3. ユーザおよびグループを追加する SVM を選択します。
4. [設定] タブをクリックします。
5. [ネームマッピング] をクリックします。
6. [S3 から Windows] または [S3 から Unix] を選択します（どちらも使用できます）。
7. [追加] をクリックします。
8. パターン (S3) とリプレースメント (Windows または Unix) を選択します。

7.1.4 バケットアクセス権の追加

既存のバケットからアクセス許可をコピーするか、アクセス許可を新規作成します。

注意

ユーザーとグループは、アクセスを許可する前に設定する必要があります。「5.1.4 ユーザーとグループの追加」(P.20) を参照してください。

新しいアクセス許可を作成するには、以下の手順を実行します。

1. [ストレージ] をクリックします。
2. [バケット] をクリックします。
3. バケットを選択します。
4. [編集] をクリックします。
5. プリンシパルユーザーを設定します。オプションには、SVM のすべてのユーザー（デフォルト）、すべてのパブリックユーザーと匿名ユーザー、および SVM に関連付けられた個々のユーザが含まれます。
6. 効果を設定します。オプションには、[Allow]（デフォルト）と [Deny] があります。
7. アクションを設定します。
8. リソースを設定します。デフォルトでは、"bucket-name" と "bucket-name/*" が使用されます。NAS ディレクトリ / フォルダパスも使用できます。
9. 条件を設定します。

10 条件を追加します。最大 10 個の条件ステートメントを追加できます。各条件ステートメントは、キー、演算子、および 1 つ以上の値で構成されます。

7.2 ONTAP CLI

ONTAP CLI を使用してマルチプロトコル NAS ボリュームの S3 を有効にするには、以下の手順を実行します。

1. S3 サービスポリシーを追加します。
2. データ LIF を確認します。
3. CA 証明書をインストールします。
4. オブジェクトストアサーバを作成します。
5. バケットを作成します。
6. ネームマッピングを有効にします。

7.2.1 S3 サービスポリシーの追加

SVM LIF で S3 データトラフィックを有効にするには、S3 サービスポリシーが必要です。

ONTAP CLI を使用してサービスポリシーを追加するには、以下のコマンドを実行します。

```
network interface service-policy add-service
-vserver <name>
-policy <name>
-services data-s3-server
```

備考

マルチプロトコルボリューム内の S3 には、data-core サービスと、data-nfs サービスまたは data-cifs サービスのどちらかまたは両方を使用して、NAS データを提供するように構成された既存の SVM が必要です。

7.2.2 データ LIF の検証

オブジェクトストアサーバーをホストする SVM には、NFS、SMB/CIFS、および S3 を使用してクライアントアプリケーションと通信するためのデータ LIF が必要です。ベストプラクティスとして、すべてのノードでデータ LIF を使用することを推奨します。

注意

DNS エントリの作成は、ONTAP の外部で行われます。すべての S3 データ LIF IP アドレスを使用する、単一のホストエントリを作成することを推奨します。
dns-zone 設定は、ONTAP の DNS ロードバランシング用です。

データ LIF がクライアントトラフィックをサポートするように設定されていることを確認するには、以下のコマンドを実行します。

```
network interface show
-vserver <name>
```

7.2.3 CA 証明書のインストール

CA 証明書を使用すると、クライアントアプリケーションと ONTAP オブジェクトストアサーバの間に信頼関係が作成されます。リモートクライアントへアクセスが可能なオブジェクトストアとして使用する前に、ONTAP に CA 証明書をインストールする必要があります。

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が発行した署名付き証明書を使用することをお勧めします。

ONTAP CLI を使用して CA 証明書をインストールするには、次のコマンドを実行します。

```
security certificate install -type server -vserver <name> -type server
```

7.2.4 オブジェクトストアサーバの作成

SVM のオブジェクトストアサーバは、ファイルやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。

ONTAP CLI を使用してオブジェクトストアサーバを作成するには、以下のコマンドを実行します。

```
vserver object-store-server create
-vserver <name>
-object-store-server <FQDN>
-certificate-name <name>
-secure-listener-port <443>
-is-http-enabled <false>
```

7.2.5 バケットの作成

ONTAP CLI を使用してバケットを作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-type nas
-nas-path <junction_path>
```

注意

- マルチプロトコル NAS ボリューム内の S3 は、既存の FlexVol または FlexGroup ボリュームを使用するため、S3 オブジェクト専用の新しい FlexGroup ボリュームは作成されません。ボリュームはすでに存在するため、アグリゲート、構成ボリューム、またはサイズを定義する必要はありません。
- ONTAP S3 は、ネイティブ S3 バケットでのオブジェクトのバージョニングをサポートします。マルチプロトコル NAS ボリュームでは、オブジェクトのバージョニングはサポートされていません。代わりに SnapMirror の使用を検討してください。

7.2.6 ネームマッピングの有効化

許可されたクライアントにのみ接続を許可する場合、すべての ONTAP オブジェクトストアでユーザー許可が必要です。マルチプロトコル NAS ボリュームで S3 を使用する場合、ONTAP は S3 ユーザーを Unix または Windows のセキュリティスタイルで作成された既存のユーザーにマッピングできる必要があります。

S3 ユーザーを既存の Unix ユーザーや Windows ユーザーにマッピングするには、以下のコマンドを実行します。

```
vserver name-mapping create
-vserver <name>
-direction <s3-win|s3-unix>
-position <1|2>
-pattern <S3 user>
-replacement <unix or windows user>
```

7.2.7 バケットポリシーの作成

ONTAP CLI を使用してバケットのアクセス許可ステートメントを設定するには、以下のコマンドを実行します。

```
vserver vserver object-store-server bucket policy add-statement
-vserver <data svm>
-bucket <name>
-effect <allow/deny>
-action <*, GetObject, PutObject, DeleteObject, ListBucket, etc.>
-principal <S3 user or group> (maximum of 10 per policy)
-resource <bucket name, bucket-name/*>
```

ONTAP CLI を使用してユーザーのアクセスと秘密キーを表示するには、以下のコマンドを実行します。

注意

高度な権限レベルが必要です。

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

8. ライフサイクルルール

ONTAP 9.13.1 以降の ONTAP S3 では、バケットレベルの情報ライフサイクル管理（ILM）機能を提供するために使用する、有効期限ルールをサポートしています。有効期限ルールを使用して、ONTAP S3 バケット内の特定のオブジェクトに適用する保存ポリシーを作成できます。各有効期限ルールは、以下の要素で構成されます。

- ルール ID およびルールの使用が可能か不可能かを示すステータスを含むメタデータ。
- 1 つ以上の有効期限アクション。以下のオプションがあります。Expiration（期限）、Noncurrent Version Expiration（最新でないバージョンの期限）、および Abort Incomplete Multipart Upload（未完了のマルチパートアップロードを中止できるようになるまでの日数）。
- 削除する必要があるオブジェクトのセットを一致させるために使用するフィルタ。フィルタには、オブジェクトの接頭辞、タグ、オブジェクトのサイズ、作成されてからの経過時間などが含まれます。フィルタが設定されていない場合、有効期限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。

バケットのライフサイクルルールが作成されると、バケットに追加されるすべての新しいオブジェクトのヘッダーに有効期限ルールが追加されます。

注意

ONTAP S3 は、移行ルールをサポートしていません。

8.1 Expiration

ONTAP CLI を使用して「期限」ルールをバケットに作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action Expiration
-obj-age-days <#>
-obj-exp-date <"MM/DD/YYYY HH:MM:SS">
-expired-obj-del-marker <true|false>
-prefix <name>
-tags <name, name> (maximum of 4)
-obj-size-greater-than <#[KB|MB|GB|TB|PB]>
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

8.1.1 例

■ 「test」で始まるオブジェクトを 30 日後に期限切れにする

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule1
-index 1
-is-enabled true
-action Expiration
-prefix testobj
-obj-age-days 30
```

■ 「proj 1=test」タグが付けられたオブジェクトを 2025 年 1 月 1 日に期限切れにする

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule2
-index 2
-is-enabled true
-action Expiration
-tags proj1=test
-obj-exp-date "2025-01-01T00:00:00"
```

■ 100MB ～ 1GB のオブジェクトを 365 日後に期限切れにする

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule3
-index 3
-is-enabled true
-action Expiration
-obj-size-greater-than 100MB
-obj-size-less-than 1GB
-obj-age-days 365
```

8.2 Noncurrent Version Expiration

ONTAP CLI を使用して、「最新でないバージョンの期限」ルールをバケットに作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action NonCurrentVersionExpiration
-new-non-curr-versions <#>
-non-curr-days <#>
-prefix <name>
-tags <name, name> (maximum of 4)
-obj-size-greater-than <#[KB|MB|GB|TB|PB]
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

8.2.1 例

■ オブジェクトの最新でないバージョンを 30 日後に期限切れにし、最新でないバージョンを 10 個まで保持する

```
vserver server object-store-server bucket lifecycle-management-rule create
-vserver svm1
-bucket mybucket
-rule-id rule4
-index 4
-action NoncurrentVersionExpiration
-is-enabled true
-non-curr-days 30
-new-non-curr-versions 10
```

8.3 Abort Incomplete Multipart Upload

ONTAP CLI を使用して、「未完了のマルチパートアップロードを中止できるようになるまでの日数」ルールをバケットに作成するには、以下のコマンドを実行します。

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <name>
-bucket <name>
-rule-id <name>
-index <#>
-is-enabled <true|false>
-action AbortIncompleteMultipartUpload
-after-initiation-days <#>
-prefix <name>
-obj-size-greater-than <#[KB|MB|GB|TB|PB]>
-obj-size-less-than <#[KB|MB|GB|TB|PB]>
```

8.3.1 例

■ 未完了のマルチパートのアップロードを 7 日後に中止する

```
vserver object-store-server bucket lifecycle-management rule create
-vserver svm1
-bucket mybucket
-rule-id rule4
-index 4
-action AbortIncompleteMultipartUpload
-is enabled true
-after-initiation-days 7
```

9. セキュリティ

9.1 ローカル層

ストレージ暗号化（SE）、ボリューム暗号化（VE）、およびアグリゲート暗号化（AE）は、ONTAP のバケットに書き込まれたオブジェクトに対しても同様に機能します。ONTAP では S3 に SE、VE、AE は必要ありません。

9.2 Over the Wire

TLS/SSL 暗号化は、システムが生成した証明書を使用してデフォルトで有効になります。サードパーティの認証局が発行する署名付き証明書を使用することをお勧めします。

TLS 暗号化なしのクライアントオブジェクトストア通信（HTTP、ポート 80）はサポートされていますが、推奨されるベストプラクティスではありません。

9.3 署名バージョン 4

ONTAP 9.11.1 以前では、ONTAP の S3 は署名バージョン 2 (v2 シグニチャ) をサポートしておらず、v4 シグニチャを使用する必要がありました。

注意

ONTAP 9.11.1 以前では、v2 シグニチャを使用すると接続に失敗します。一般的に使用される S3 ブラウザを含む多くのクライアントアプリケーションでは、デフォルトで v2 シグニチャが使用される点に留意してください。可能な限り、クライアントアプリケーションで v4 シグニチャを使用することを推奨します。

10. S3 SnapMirror

ONTAP 9.10.1 以降では、ONTAP S3 バケット内のデータを S3 SnapMirror で保護できます。SnapMirror を使用すると、指定した RPO (目標復旧時点) に合わせて同期スケジュールを定義できます。SnapMirror は、ソースからデスティネーション、ファンアウト、カスケードなど、さまざまなデータ保護関係を作成するためにも使用できます。ファンイン関係はサポートされていません。

S3 SnapMirror には、主に以下の 2 つの使用例があります。

- バックアップとリカバリ。デスティネーションバケットにフェイルオーバーすることなく、デスティネーションバケットからソースバケットにリストアすることを目的とします。S3 SnapMirror 関係が壊れている場合、デスティネーションバケット内のオブジェクトは読み取り専用のままになります。
- ディザスタリカバリ (DR) およびフェイルオーバー。災害イベントの発生時に、デスティネーションバケットからクライアントのアプリケーションにデータを提供できるようにすることを目的とします。S3 SnapMirror 関係が壊れている場合、デスティネーションバケットが読み取りと書き込みをサポートします。ONTAP は、DR およびフェイルオーバー操作をサポートする唯一のデスティネーションターゲットです。

注意

S3 SnapMirror は、ネイティブ S3 オブジェクトの保護専用です。FabricPool によって ONTAP S3 バケットに階層化された NAS および SAN データは、S3 SnapMirror ではなく、SnapMirror またはその他のデータ保護アプリケーションを使用して通常どおり保護されます。

10.1 Snapshot コピー

ONTAP S3 はオブジェクトのバージョニングをサポートしていますが、オブジェクトストレージはファイルストレージやブロックストレージのようにトランザクション型ではありません。そのため、S3 SnapMirror では、特定の時点でのファイルの状態をキャプチャし、高効率なポイントインタイムの差分情報として機能するスナップショットコピーは使用しません。

10.2 S3 SnapMirror を使用したバケットの保護

バケットデータのミラーリング、データを復元するデータ保護ポリシーの設定、およびテイクオーバー操作の実行については、マニュアルサイトの関連マニュアルを参照してください。

10.3 要件

S3 SnapMirror には、ONTAP 9.10.1 以降が必要です。ONTAP 9.10.1 以前では、Cloud Sync を使用してデータ保護を実現していました。

10.3.1 デスティネーションターゲット

- 当社
  - ONTAP
  - Cloud Volumes ONTAP for AWS
  - Cloud Volumes ONTAP for Azure

  - Amazon FSx for NetApp ONTAP
  - FUJITSU Hybrid IT Service for Microsoft Azure の Cloud Volumes ONTAP
- サードパーティ
  - Amazon S3

注意

ONTAP をデスティネーションターゲットとして使用する場合、S3 SnapMirror は、ソースバケットおよびデスティネーションバケット間のデータ保護関係を、同一クラスタ関係とリモートクラスタ関係の両方で作成します。同一クラスタ関係は、クラスタまたはサイト全体の災害イベントからデータを保護するものではありません。そのため、S3 SnapMirror をローカルクラスタ外のターゲットに使用することをお勧めします。

10.3.2 ライセンス

S3 SnapMirror を有効にするには、Data Protection Bundle を使用する必要があります。S3 SnapMirror を使用して Amazon S3 などのサードパーティのオブジェクトストアにデータをレプリケートする場合は、Data Protection Bundle と Hybrid Cloud Bundle の両方が必要です。

10.3.3 認証局 (CA) 証明書

TLS を使用する場合は、ソースとデスティネーションの両方でデスティネーションの CA 証明書を使用するように S3 SnapMirror を設定する必要があります。

CA 証明書は必須ではありませんが、ONTAP S3 では TLS 証明書と自己署名証明書がデフォルトで使用されます。サードパーティの認証局が発行する署名付き証明書を使用することをお勧めします。

10.3.4 クラスタピア関係

S3 SnapMirror ターゲットのデスティネーションとして別の ONTAP クラスタを使用する場合は、事前にクラスタピア関係を確立しておく必要があります。詳細については、「ミラーとバックアップの準備」および「クラスタ ピア関係の作成」を参照してください。

10.3.5 クラウドオブジェクトストア

S3 SnapMirror ターゲットのデスティネーションとして StorageGRID、Amazon S3、Microsoft Azure Blob Storage などのクラウドオブジェクトストアを使用する場合は、事前に ONTAP によって認証される必要があります。詳細については、「クラウドオブジェクトストアの追加」を参照してください。

10.4 保護ポリシー

S3 SnapMirror は、ソースバケット内のデータのレプリケーションをデスティネーションバケットに作成するデータ保護関係を作成します。データのレプリケーションは、バケットを保護する際に選択する保護ポリシーに基づきます。S3 SnapMirror のデフォルトの保護ポリシーである `Continuous` は、1 時間の RPO を使用して

データのレプリケーションをデスティネーションバケットに継続的に作成し、データのスロットルは行いません。

保護ポリシーは、1 つ以上のバケットを保護する場合に使用するために作成および保存できます。カスタマイズが可能なパラメータは、以下の通りです。

- ポリシータイプ
  S3 SnapMirror 保護ポリシーでは、ポリシータイプとして Continuous を使用する必要があります。Asynchronous ポリシーと Synchronous ポリシーは、「保護ポリシーの追加」メニューを使用して作成できますが、バケットを保護する際の保護ポリシーとしては選択できません。
- スロットル
  RPO を達成するための最大帯域幅を設定します。デフォルトの設定は 0 で、この場合はスロットルを設定しません。
- RPO
  ソースバケットで変更が行われてから、その変更がデスティネーションバケットに転送されるまでの遅延を設定します。デフォルトの設定は 1 時間です。

11. サポートされている S3 アクション

11.1 バケット

アスタリスク (*) が付いたアクションは、S3 REST API ではなく ONTAP でサポートされます。

- CreateBucket (9.11.1)
- DeleteBucket (9.11.1)
- DeleteBucketLifecycleConfiguration (9.13.1)
- DeleteBucketPolicy (9.12.1)
- GetBucketAcl
- GetBucketLifecycleConfiguration (9.13.1)
- GetBucketLocation (9.10.1)
- GetBucketPolicy (9.12.1)
- GetBucketVersioning (9.11.1)
- HeadBucket
- ListBuckets
- ListBucketVersioning (9.11.1)
- PutBucket*
- PutBucketLifecycleConfiguration (9.13.1)
- PutBucketPolicy (9.12.1)
- PutBucketVersioning (9.11.1)

11.2 オブジェクト

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (9.12.1)
- CreateMultipartUpload
- DeleteObject
- DeleteObjects (9.11.1)
- DeleteObjectTagging (9.9.1)
- GetObject
- GetObjectAcl
- GetObjectTagging (9.9.1)
- HeadObject
- ListMultipartUpload
- ListObjectVersions (9.11.1)
- ListObjects
- ListParts
- PutObject
- PutObjectTagging (9.9.1)
- HeadObject
- UploadPart
- UploadPartCopy (9.12.1)

11.3 グループポリシー

これらの操作は S3 に固有のものではなく、通常は Identity and Management (IAM) に関連付けられています。ONTAP はこれらのコマンドをサポートしますが、IAM REST API を使用しません。

ONTAP S3 グループには、最大で 10 個のポリシーを付与できます。グループポリシーは最大で 5 つのステートメントを持つことができ、各ステートメントには最大で 10 個のリソースを設定可能です。

- Create Policy
- AttachGroup Policy

11.4 ユーザー管理

これらの操作は S3 に固有のものではなく、通常は IAM に関連付けられています。

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

11.5 マルチプロトコル NAS ボリュームで未サポートのアクションと機能

マルチプロトコル NAS ボリュームで S3 を使用している場合、メタデータ、マルチポートオブジェクト、タグ、およびバージョニングに関連するアクションと機能はサポートされません。以下に未サポートの項目を示します。

- `x-amz-meta-<key>` を使用したキーバリューペアは保存されず、`x-amz-meta` を使用したリクエストヘッダは無視されます。
- タグのアップデート要求は却下され、`x-amz-tagging` を使用したヘッダーは無視されます。
- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObjectTagging
- GetBucketVersioning
- GetObjectTagging
- PutBucketVersioning
- PutObjectTagging
- ListBucketVersioning
- ListMultipartUpload
- ListObjectVersions

12. リリース済みの S3 アクション

12.1 ONTAP 9.13.1

ONTAP 9.13.1 では、バケットのライフサイクル設定が追加されました。

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

12.2 ONTAP 9.12.1

ONTAP 9.12.1 では、バケットポリシーおよびオブジェクトのコピー機能が追加されました。

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- UploadPartCopy

12.3 ONTAP 9.11.1

ONTAP 9.11.1 では、バージョニング、署名済み URL、分割アップロード、および S3 API を用いたバケットの作成や削除などの一般的な S3 アクションのサポートが追加されました。

- OTNAP S3 は、`x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD` を使用してリクエストに署名する分割アップロードをサポートしました。
- ONTAP S3 は、署名済み URL を使用したクライアントアプリケーションをサポートし、オブジェクトの共有、またはユーザーの認証情報を要求しないでユーザーがオブジェクトをアップロードできる機能をサポートしました。
- CreateBucket
- DeleteBucket
- GetBucketVersioning
- ListBucketVersioning
- PutBucketVersioning
- DeleteObjects
- ListObjectVersions

注意

基盤となる FlexGroup は、最初のバケットを作成するまでは作成されないため、まず ONTAP 内でバケットを作成する必要があります。その後に、外部クライアントは CreateBucket を使用したバケット作成が可能になります。

12.4 ONTAP 9.10.1

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

- GetBucketLocation

12.5 ONTAP 9.9.1

ONTAP 9.9.1 では、ONTAP S3 でオブジェクトメタデータとタグ付けをサポートします。

- PutObject および CreateMultipartUpload に、`x-amz-meta-<key>` を使用したキー値のペアが追加されました。
  例：`x-amz-meta-project: ontap_s3`
- GetObject および HeadObject がユーザー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、タグは以下のもの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

13. 相互運用性

表 13.1 にリストアップされている通常の相互運用性の例外は、ONTAP オブジェクトストアに固有です。

表 13.1　相互運用性

フォーカス	サポート対象	未サポート
データ保護	• Cloud Sync • S3 SnapMirror（9.10.1） • ミラーリングされていない MetroCluster アグリゲート（9.12.1）	• イレイジャー コーディング • ミラーリングされた MetroCluster アグリゲート • NDMP • SnapLock technology • SnapMirror technology • SyncMirror technology • SMTape • SVM-DR • WORM
暗号化	• アグリゲート暗号化 （AE） • ストレージ暗号化 （SE） • ボリューム暗号化 （VE） • TLS/SSL	• SLAG
ストレージ効率	• 圧縮 • コンパクション • 重複排除 • 温度依存型ストレージ効率化（TSSE）	アグリゲートレベルの効率性
ストレージ仮想化	–	FlexArray テクノロジー
QoS	QoS の最大値 （上限） QoS の最小値 （下限）	–
その他の機能	• 監査 • バケットのライフサイクル管理（9.13.1） • FabricPool クラウド階層 （ネイティブ S3 のみ） • FabricPool ローカル階層 （NAS ボリュームのみ）	• FabricPool クラウド階層 （NAS ボリュームのみ） • FabricPool ローカル階層 （ネイティブ S3 のみ） • FPolicy ソフトウェア • Qtree • クォータ

ETERNUS AX series オールフラッシュアレイ , ETERNUS HX series ハイブリッドアレイ
ONTAP での S3 ベストプラクティス ONTAP 9.13.1

P3AG-6642-03Z0

発行年月　2025 年 3 月
発行責任　エフサステクノロジーズ株式会社

- 本書の内容は、改善のため事前連絡なしに変更することがあります。
- 本書の内容は、細心の注意を払って制作致しましたが、本書中の誤字、情報の抜け、本書情報の使用に起因する運用結果に関しましては、責任を負いかねますので予めご了承願います。
- 本書に記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。
- 無断転載を禁じます。

Fsas Technologies