テクニカル レポート

S3 in ONTAP Best Practices

ONTAP 9.8

ネットアップ、John Lantz

2021 年 1 月| TR-4814

概要

このテクニカルレポートでは、Amazon Simple Storage Service（S3）と NetApp ® ONTAP ® ソフトウェアを使用する場合のベストプラクティスについて説明します。また、ネイティブ S3 アプリケーションを使用するオブジェクトストアとして ONTAP を使用する場合や、NetApp FabricPool の階層化のデスティネーションとして を使用する場合の機能と構成についても説明します。

目次

表一覧

図一覧

概要

NetApp ONTAP 9.8 ソフトウェアは、Amazon Simple Storage Service（S3）をサポートします。ONTAP は、AWS S3 API アクションのサブセットをサポートし、AFF、FAS、ONTAP Select などの ONTAP ベースのシステムでデータをオブジェクトとして表現できるようにします。

NetApp StorageGRID® ソフトウェアは、さらに、ネットアップのオブジェクトストレージ向けフラッグシップ解決策である、今後も引き続きサービスを提供します。ONTAP は、エッジ上での取り込み / 前処理ポイントを提供することで StorageGRID を補完します。ネットアップが提供するオブジェクトデータ向けデータファブリックを拡張し、ネットアップ製品ポートフォリオの価値を高めます。

主なユースケース

ONTAP の S3 の主な目的は、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 ユニファイドストレージアーキテクチャで、ファイル（NFS および SMB）、ブロック（FC および iSCSI）、オブジェクト（S3）がサポートされるようになりました。

ネイティブ S3 アプリケーション

S3 を使用したオブジェクトのサポートに ONTAP が必要にな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は適していますが、ネイティブ S3 アプリケーションの需要は急速に拡大しており、次のようなものがあります。

- 分析
- 人工知能
- エッジからコアへの取り込み
- 機械学習

ONTAP System Manager など、使い慣れた管理ツールを使用して、ONTAP での開発や運用に必要な高性能オブジェクトストレージを迅速にプロビジョニングできるようになりました。そのため、ONTAP の Storage Efficiency 機能とセキュリティを活用できます。

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ため、ONTAP から ONTAP への階層化が可能になります。これは、既存の FAS インフラをオブジェクトストアのエンドポイントとして転用する場合に最適なオプションです。

FabricPool では、次の 2 つの方法で ONTAP への階層化がサポートさ

- **ローカルクラスタの階層化。**アクセス頻度の低いデータは、クラスタ LIF を使用してローカル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。**アクセス頻度の低いデータは、FabricPool クライアントの IC LIF と ONTAP オブジェクトストアのデータ LIF を使用して、リモートクラスタにあるバケットに階層化され、従来の FabricPool クラウド階層と同じように配置されます。

300TB を超える非アクティブデータを階層化する場合、最初のネットアップオブジェクトストア解決策である StorageGRID を使用することを推奨します。ONTAP または StorageGRID をクラウド階層として使用する場合は、FabricPool ライセンスは必要ありません。

要件

プラットフォーム

NetApp AFF ストレージ システム S3 は、ONTAP 9.8+ を使用するすべての AFF プラットフォームでサポートされます。

- **FAS ストレージシステム。**S3 は、ONTAP 9.8+ を使用するすべての FAS プラットフォームでサポートされます。
- **NetApp ONTAP Select の略。**S3 は、ONTAP Select 9.8+ を使用するすべてのプラットフォームでサポートされます。
- **Cloud Volumes ONTAP 。**Cloud Volumes ONTAP では S3 はサポートされていません。

データ LIF

オブジェクトストアサーバをホストしている Storage Virtual Machine（SVM）が 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には、データ LIF が必要です。リモートクラスタ階層化用に設定されている場合、FabricPool はクライアントで、オブジェクトストアはサーバです。

クラスタ LIF

ローカルクラスタ階層化が設定されている場合、ローカル階層（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接続されます。FabricPool は、クラスタ内のトラフィックにクラスタ LIF を使用します。

注： クラスタ LIF のリソースが最大限まで使用されないと、パフォーマンスが低下する可能性があります。この問題を回避するために、ローカルバケットに階層化する場合は 2 ノード以上のクラスタを使用することを推奨します。ベストプラクティスは、ローカル階層の HA ペアとローカルバケットの HA ペアを推奨します。シングルノードクラスタでは、ローカルバケットへの階層化は推奨されません。

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、S3 を ONTAP で使用するには、ライセンスのインストールが必要です。S3 ライセンスは無償ライセンスですが、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。

新しい ONTAP 9.8 システムには S3 ライセンスが事前にインストールされています。

S3 ライセンス [マスターライセンスキー] ページ は、ネットアップサポートサイトのからダウンロードできます。

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 で次のコマンドを実行します。

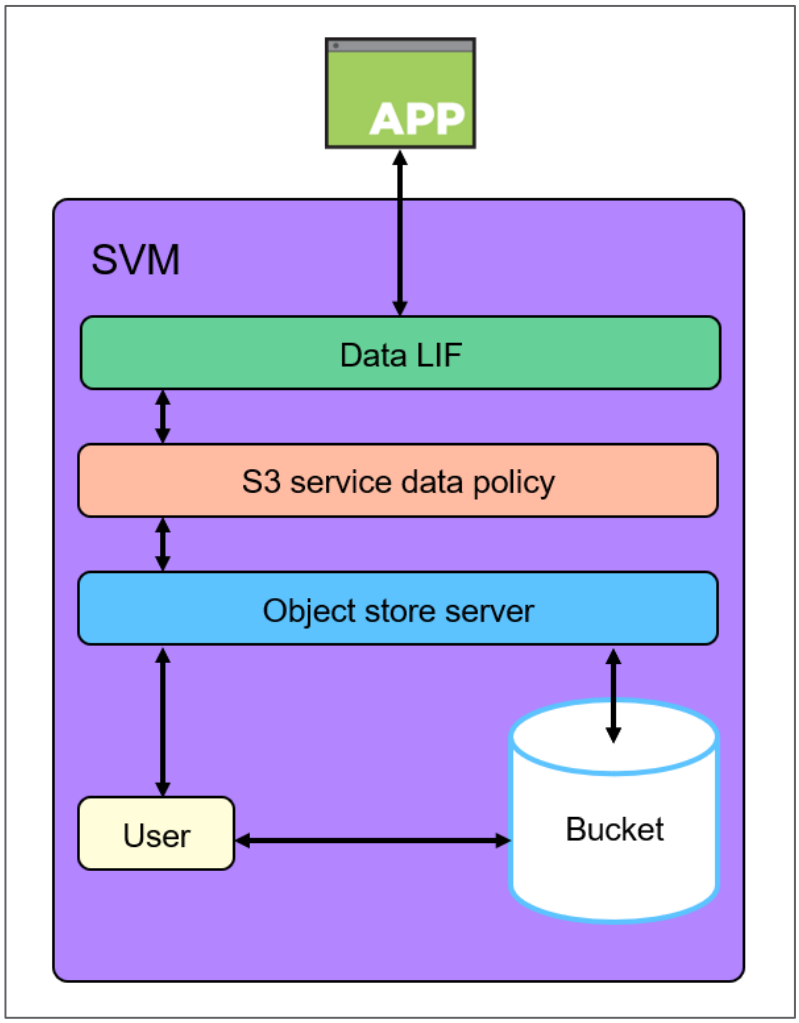
```
system license add <license_key>
```

アーキテクチャ

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ストレージ アーキテクチャです。オブジェクトは 1 つのコンテナ（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にある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のパフォーマンスはファイルストレージやブロックストレージよりも低下する可能性がありますが、拡張性は大幅に向上しており、ペタバイト単位のデータを含むバケットも珍しくありません。

図 1）ONTAP の S3 オブジェクトストレージの中核となる要素



S3 サービスのデータポリシー

データポリシーは SVM に割り当てられ、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データ LIF で必要な一連のネットワークサービスを提供します。たとえば、データ NFS は NFS トラフィックのサポートに使用され、データ iSCSI は iSCSI トラフィックのサポートに使用されます。

ONTAP 9.8 では、S3 サービスデータポリシー data-s3-server を使用することで、S3 を使用するクライアントアプリケーショントラフィックをデータ LIF でサポートできるようになりました。

オブジェクトストアサーバ

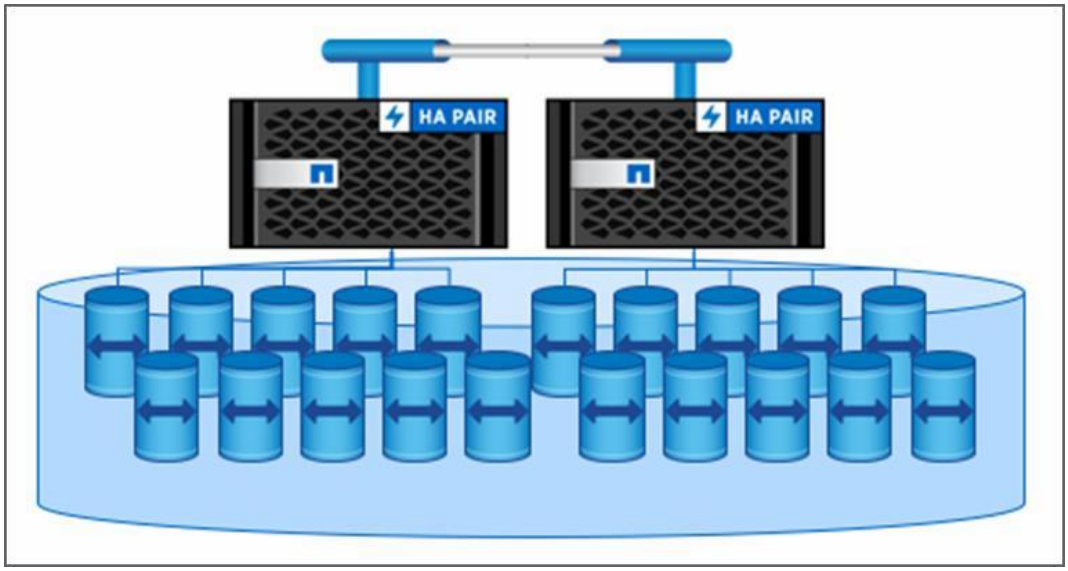
SVM のオブジェクトストアサーバは、ファイルストレージやブロックストレージなどの他のストレージアーキテクチャとは対照的に、データをオブジェクトとして管理します。バケットとユーザの権限レベルの管理は、オブジェクトストアサーバのレベルでも行われます。

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

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 FlexGroup ボリューム- です 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単一のネームスペースが、図 2 に示すように単一のボリュームとして管理されます。FlexGroup 内の個々のファイルは、個々のメンバー ボリュームに割り当てられ、複数のボリュームやノードにまたがってストライプされることはありません。

図 2）FlexGroup ボリューム



FlexGroup ボリュームは、バケットで使用する場合にエラスティックサイジングを使用します。代わりに、FlexGroups ボリュームは、基盤となるハードウェアの物理的な最大値によってのみ制限され、20PB および 4,000 億ファイルに対してテスト済みです。ONTAP S3 は最大 12、000 個のバケットをサポートします。

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ています。5TB を超えるオブジェクトは、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クライアントとの相互運用性の問題が発生する可能性があります。

注： ONTAP 9.7 のバケット（FlexGroup ごとに 1 つのバケット）と ONTAP 9.8（FlexGroup ごとに複数のバケット）でアーキテクチャを変更することはできません。新しいアーキテクチャを活用するには、既存のバケットから ONTAP 9.8 バケットにデータを移行する必要があります。

ユーザ

許可されたクライアントへの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許可が必要です。特定のバケットまたは S3 処理へのアクセスを許可、拒否、またはユーザレベルで条件付きにすることができます。

ONTAP S3 では、オブジェクトストアあたり 4、000 ユーザがサポートされます。

ネイティブの S3 アプリケーションとリモートのクラスタ階層化の設定

ネイティブの 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 システムマネージャを使用する方法です。CLI を使用する際に複数の手順が必要になるプロセスは、ネットアップが推奨するベストプラクティスに従って数回のクリックで完了するようになりました。よりカスタムな設定を行うには、CLI を使用した設定が必要です。

ONTAP System Manager

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 システムマネージャを使用して、CLI で必要な複数の手順を数回のクリックで完了させることです。ONTAP System Manager を使用して作成されたオブジェクトストアはカスタマイズが可能ですが、デフォルトでネットアップが推奨するベストプラクティスに従って作成されます。カスタム構成には CLI を使用した構成が必要です。

ONTAP System Manager を使用してオブジェクトストア、バケット、および権限のユーザを作成するには、次の手順を実行します。

オブジェクトストアを設定します

ONTAP System Manager を起動します。

2. [storage](ストレージ) をクリックします。

3. Storage VMs（Storage VM）をクリックします。

[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「設定」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 S3 を有効にするを選択します。デフォルトでは、TLS を有効にする（ポート 443）オプションとシステム生成証明書を使用する（Use System-Generated Certificate）オプションが選択されています。ただし、サードパーティの認証局からの署名証明書を使用することを推奨します。

7. S3 サーバに名前を付けます。

   注： サーバ名は、クライアントアプリケーションで Fully Qualified Domain Name（FQDN ；完全修飾ドメイン名）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イスを入力します。

バケットを設定する

ONTAP System Manager を起動します。

2. [storage](ストレージ) をクリックします。

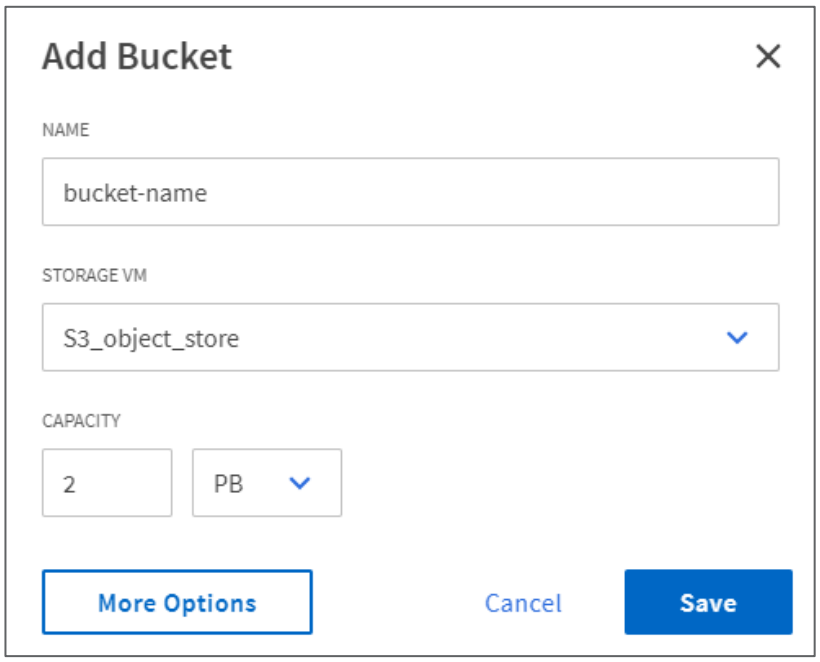
3. バケットをクリックします。

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。以前に作成した SVM とオブジェクトストアが同じである必要があります。

7. 保存をクリックします。



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 システムマネージャは最も安価なメディアにバケットを作成し、HDD > QLC > TLC > NVMe の優先順位を設定します。

パフォーマンス サービス レベル

バケットに適したサービス品質（QoS）を選択します。次のオプションがあります。

- **極限。** 50,000 MBps または 1562 IOPS
- **パフォーマンス。** 30、000 IOPS、937 Mbps
- **価値。** 15、000 IOPS、468 Mbps
- **カスタム。** 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。

注 ：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 では FlashPool ワークロードがサポートされません。

権限

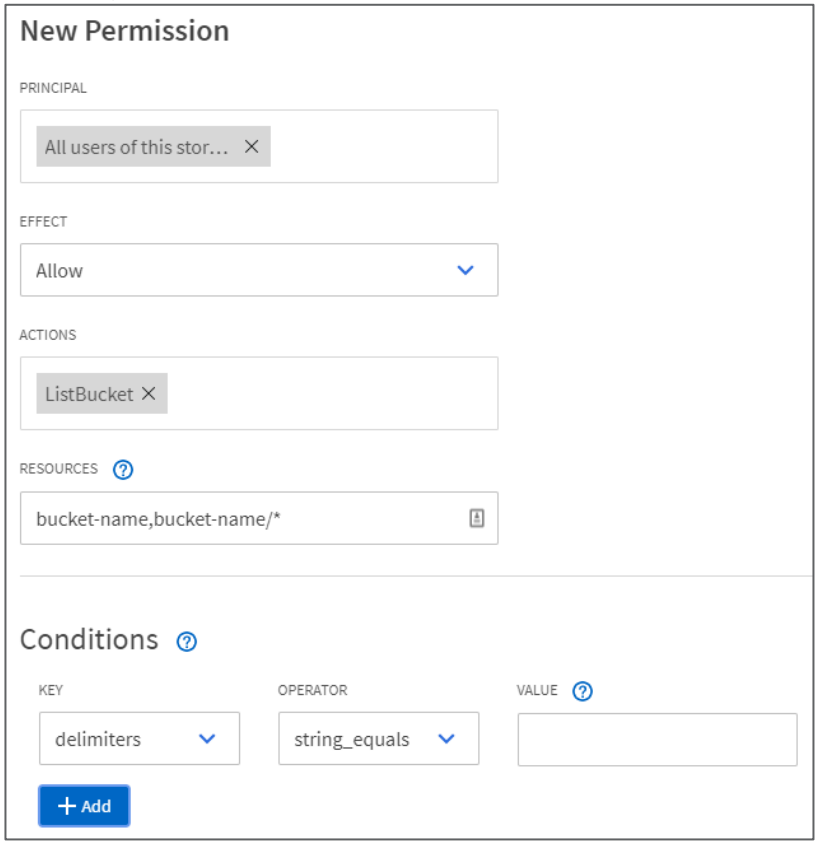
アクセス権限を既存のバケットからコピーするか、新しいバケットを作成します。

注： ユーザとグループにアクセスするには、事前にユーザとグループを設定しておく必要があります。ユーザとグループの追加

新しい権限を作成するには：

1. ［ バケットの追加 ］ ページで、［ 権限 ］ までスクロールダウンし、［ 追加 ］ をクリックします。
2. 主要ユーザーを設定します。オプションを使用して、SVM のすべてのユーザ（デフォルト）、すべてのパブリックユーザと匿名ユーザ、および SVM に関連付けられた個々のユーザを指定できます。

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。GetObject、PutObject、DeleteObject、ListBucket（デフォルト）、GetBucketAcl、GetObjectAcl、ListBucketMultipartUploads、および ListMultipartUploadParts 。
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。各条件文は、キー、演算子、および 1 つ以上の値で構成されます。



ユーザとグループの追加

許可されたクライアントへの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許可が必要です。特定のバケットまたは S3 処理へのアクセスを、権限を使用してユーザレベルおよび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 では、オブジェクトストアまたは SVM あたり 4、000 ユーザがサポートされます。

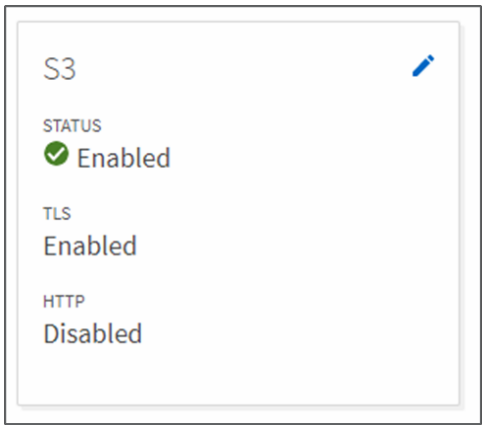
注　：バケットの作成時に、デフォルトで root ユーザ（UID 0）が作成されます。root ユーザには、すべてのバケットとオブジェクトに対するフルアクセスが許可されます。クライアントアプリケーションからのアクセスに root ユーザを使用しないでください。クライアントアクセス用に追加のユーザを作成する必要があります。

ユーザおよびグループの管理

ONTAP System Manager を起動します。

2. [storage](ストレージ) をクリックします。
3. Storage VMs（Storage VM）をクリックします。
4. ユーザとグループを追加する SVM を選択します。

5. S3 プロトコルボックスの Edit アイコンをクリックします。



6. ［ ユーザー ］ タブまたは ［ グループ ］ タブを選択します。

[追加] をクリックします。

8. ユーザまたはグループに名前を付けます。

9. あとで使用できるように、アクセスキーとシークレットキーをコピーまたはダウンロードします。

注： シークレットキーは今後表示されません。

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、[アクセス許可] メニューを使用します。

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 システムマネージャを使用する方法ですが、ONTAP システムマネージャを使用して作成したオブジェクトストアを使用すると、より簡単にカスタマイズすることができます。

たとえば、ONTAP System Manager は、ストレージ用のバケットで使用されるローカル階層（アグリゲート）を自動的に選択します。ベストプラクティスを推奨してこの方法で実施しますが、複雑な環境の場合は、経験豊富なストレージ管理者と同じローカル階層を選択しないこともあります。

カスタム構成には、ONTAP CLI を使用した構成が必要です。

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

1. S3 サービスデータ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を作成します。
5. バケットを作成します。
6. ユーザを作成します。

S3 サービスデータポリシーを作成する

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

ONTAP CLI を使用して S3 サービスデータポリシーを作成するには、次のコマンドを実行します。

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

S3 を使用するデータ LIF を作成します

オブジェクトストアサーバをホストしている SVM が 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には、データ LIF が必要です。ベストプラクティスとして、すべてのノードに S3 データ LIF を作成することを推奨します。

リモートクラスタ階層化用に設定されている場合、FabricPool はクライアントで、オブジェクトストアはサーバです。FabricPool ではオブジェクトストアで FQDN を使用する必要があるため、すべての S3 データ LIF をオブジェクトストアサーバが使用する FQDN に関連付ける必要があります。

注： ONTAP の外部に DNS エントリを作成する必要があります。S3 のデータ LIF のすべての IP アドレスを使用するホストエントリは 1 つにすることを推奨します。

DNS ゾーン設定は、ONTAP DNS ロードバランシング用です。詳細については、TR-4523『 ONTAP における DNS ロードバランシング』を参照してください。

ONTAP CLI を使用して S3 サービスデータポリシーを使用する LIF を作成するには、次のコマンドを実行します。

```
network interface create
-vserver <name>
-lif <name>
-service-policy data-s3-server
-home-node <node>
-home-port <port>
-address <number>
-netmask <number>
-status-admin up
```

CA 証明書をインストールします

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

自己署名証明書を使用できますが、サードパーティの認証局からの署名証明書を使用することを推奨します。

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-ca
```

オブジェクトストアサーバを作成

ONTAP オブジェクトストアサーバは、ファイルストレージやブロックストレージ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、次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>
```

注　　：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を解決する必要があります。

バケットを作成します

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

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constiuent volumes per aggregate> (default 4)
-size <size>
```

ユーザを作成

許可されたクライアントへの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許可が必要です。

注　　：有効なアクセス権とシークレットキーペアを持つすべての S3 ユーザは、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 を使用してユーザを作成するには、次のコマンドを実行します。

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

ONTAP CLI を使用してユーザのアクセスキーとシークレットキーを表示するには、次のコマンドを実行します。

Advanced 権限レベルが必要です。

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

root ユーザ

バケットの作成時に、デフォルトで root ユーザ（UID 0）が作成されます。root ユーザには、すべてのバケットとオブジェクトに対するフルアクセスが許可されます。クライアントアプリケーションからのアクセスに root ユーザ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のアクセスキーとシークレットキーを設定する必要があります。

ローカルクラスタ階層化の設定

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ため、ONTAP 間で階層化できます。これは、既存の FAS インフラをオブジェクトストアのエンドポイントとして転用する場合に最適なオプションです。

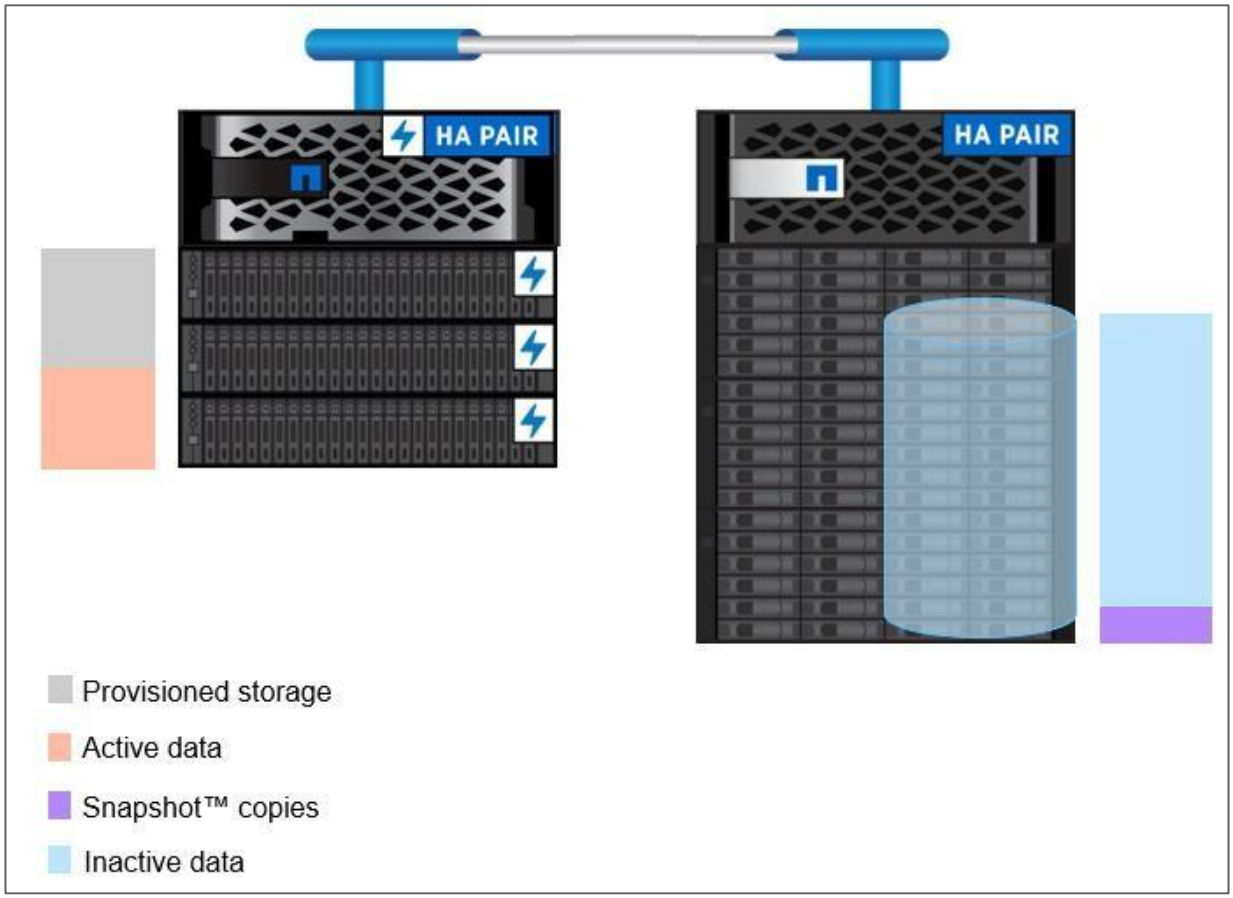
ローカルクラスタの階層化が設定されている場合、アクセス頻度の低いデータはローカルアグリゲート（通常は SSD）からローカルバケット（通常は HDD）に階層化され、クラスタ LIF を使用します。

使用頻度の低いデータを 300TB 以上階層化する場合は、ネットアップのオブジェクトストア解決策である StorageGRID を使用することを推奨します。ONTAP または StorageGRID をクラウド階層として使用する場合は、FabricPool ライセンスは必要ありません。

FabricPool の詳細について は、TR-4598 ：『 FabricPool Best Practices 』を参照してください。

注： クラスタ LIF のリソースが最大限まで使用されないと、パフォーマンスが低下する可能性があります。この問題を回避するために、ローカルバケットに階層化する場合は 2 ノード以上のクラスタを使用することを推奨します。ベストプラクティスは、ローカル階層の HA ペアとローカルバケットの HA ペアを推奨します。シングルノードクラスタでは、ローカルバケットへの階層化は推奨されません。

図 3）ローカルクラスタの階層化



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 システムマネージャを使用することです。CLI を使用する複数の手順を数回のクリックで削減できます。ONTAP システムマネージャを使用して作成したオブジェクトストアはカスタマイズが可能ですが、デフォルトでネットアップが推奨するベストプラクティスを使用してください。カスタム構成には、CLI を使用した設定が必要です。

オブジェクトストアを設定します

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

ONTAP System Manager を起動します。

2. [storage](ストレージ) をクリックします。

3. [Tiers (階層)] をクリックします

4. ローカル階層を選択します。

5. 「詳細」をクリックします。

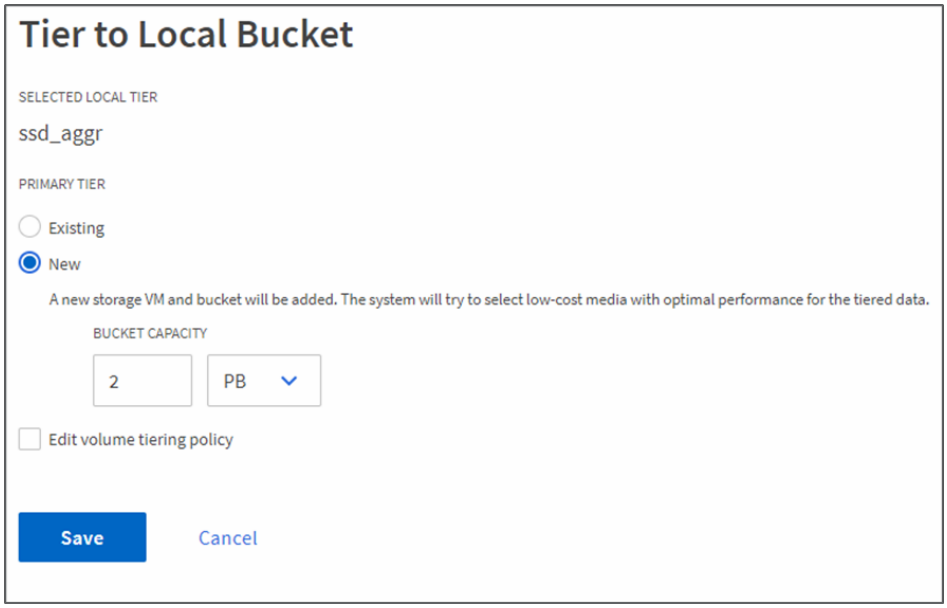
6. ローカルバケットの階層を選択します。

7. システムの最初のローカルバケットの場合は、[New] を選択します。

   新しい SVM、オブジェクトストアサーバ、およびバケットが作成されます。ONTAP システムマネージャが最も安価なメディアにバケットを作成し、HDD > QLC > TLC > NVMe の優先順位を設定します。

   ローカルバケットがすでに作成されている場合は、「既存」を選択します。

   注　：クラスタ内のすべての FabricPool ローカル階層に同じローカルバケットを接続することで、ボリューム移動の最適化が実現します。ボリューム移動のデスティネーションローカル階層がソースローカル階層と同じバケットを使用している場合、バケットに格納されているソースボリューム上のデータはローカル階層に戻されません。ボリュームの移動を最適化することで、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. ［ 保存 ］ をクリックします。

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 システムマネージャを使用する方法ですが、ONTAP システムマネージャを使用して作成したオブジェクトストアを使用すると、より簡単にカスタマイズすることができます。

たとえば、ONTAP System Manager は、ストレージ用のバケットで使用されるローカル階層（アグリゲート）を自動的に選択します。ベストプラクティスを推奨してこの方法で実施しますが、複雑な環境の場合は、経験豊富なストレージ管理者と同じローカル階層を選択しないこともあります。

カスタム構成には、ONTAP CLI を使用した構成が必要です。

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、次の手順を実行します。

1. オブジェクトストアサーバを作成します。
2. バケットを作成します。

オブジェクトストアサーバを作成

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

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

ローカル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、次のコマンドを実行します。

```
vserver object-store-server bucket create
-vserver <name>
-bucket <name>
-aggr-list <aggregate name>,<aggregate name>
-aggr-list-multiplier <number of constiuent volumes per aggregate> (default 4)
-size <size>
```

ローカルバケットをローカル階層に接続

ONTAP CLI を使用してローカルバケット階層（ストレージアグリゲート）に接続するには、次のコマンドを実行します。

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <object_store_server_name>
-name local_object_store_server
```

注： ローカルバケットをローカル階層に接続することは、永続的なアクションです。接続後にローカルバケットとローカル階層の接続を解除することはできません。FabricPool ミラーを使用すると、別のローカルバケットまたはクラウド階層を接続できます。

セキュリティ

ローカル階層

NetApp Storage Encryption（NSE）、NetApp Volume Encryption（NVE）、および NetApp Aggregate

Encryption（NAE）は、ONTAP のバケットに書き込まれるオブジェクトにも同様に適しています。ONTAP では、S3 に NSE、NVE、NAE のいずれも必要ありません。

ネットワークを介して転送

TLS/SSL 暗号化は、システムで生成された証明書を使用してデフォルトで有効になります。ただし、サードパーティの認証局からの署名証明書を使用することを推奨します。

TLS 暗号化を使用しないクライアント / オブジェクトストア通信（HTTP、ポート 80）も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。

署名バージョン 4

ONTAP の S3 では、署名バージョン 4（v4 署名）を使用する必要があります。

注　：v2 シグニチャを使用すると、接続に失敗します。一般に使用される S3 ブラウザも含め、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 の署名が使用されるため、この点に注意する必要があります。
接続エラーを回避するために、v4 署名を使用するようにクライアントアプリケーションを設定します。

サポートされる S3 処理数

バケット

アスタリスクが付いているアクションは、S3 REST API ではなく ONTAP でサポートされています。

- DeleteBucket*
- DeleteBucketPolicy *
- GetBucketAcl
- ヘッドバケット
- リストバケット
- PutBucket*

オブジェクト

- PutObject
- GetObject
- GetObjectAcl
- DeleteObject
- ヘッドオブジェクト
- ListObjects
- ListParts
- UploadPart
- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload

• ListMultipartUpload

グループ ポリシー

これらの処理は S3 に固有ではなく、一般に IAM（ID と管理）に関連付けられています。ONTAP ではこれらのコマンドをサポートしていますが、IAM REST API は使用していません。

•ポリシーの作成

•添付グループポリシー

ユーザ管理

これらの処理は S3 に固有ではなく、一般に IAM（ID と管理）に関連付けられています。

• CreateUser

• deleteUser

• CreateGroup

•グループの削除

相互運用性

表 1 に示す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 1）ネットアップの相互運用性

重点項目	サポート	サポート対象外
データ保護	• Cloud Sync	•イレイジャーコーディング •情報ライフサイクル管理 • NetApp MetroCluster™ • NDMP • NetApp SnapLock® テクノロジ • NetApp SnapMirror® テクノロジ • NetApp SyncMirror® テクノロジ •オブジェクトのバージョン管理 • SMTape • SVM-DR •ユーザー作成のスナップショット • WORM
暗号化	• NetApp Aggregate Encryption NAE • NetApp Volume Encryption NVE • NetApp Storage Encryption NSE	•スラグ

	• TLS/SSL	
ストレージの効率化	•インライン重複排除 •インライン圧縮 • コンパクション：	アグリゲートレベルの効率化
ストレージ仮想化	–	NetApp FlexArray®テクノロジ
Quality of Service（QoS; サービス品質）	QoS の最大数（上限） QoS の最小値（下限）	–
その他の機能	–	•監査 • NetApp FPolicy ソフトウェア • qtree •クォータ

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントや Web サイトを確認してください。

S3 構成パワー ガイド

https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-s3-cg/S3%20configuration.pdf

•オブジェクトストレージのプロビジョニング

https://docs.netapp.com/ontap/us-en/pdfs/sidebar/Provision_object_storage.pdf

• TR-4598 ：『 FabricPool Best Practices 』

https://www.netapp.com/us/media/tr-4598.pdf

• ONTAP 9 ドキュメントセンター

https://docs.netapp.com/ontap-9/index.jsp

• ONTAP および ONTAP System Manager のマニュアルリソース

https://www.netapp.com/us/documentation/ontap-and-oncommand-system-manager.aspx

•ネットアップの製品ドキュメント

https://www.netapp.com/us/documentation/index.asp x

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
1.1	2021 年 1 月	サポートされる S3 処理を更新しました。
1.0	2021 年 1 月	初版リリース

お問い合わせ

本テクニカル レポートの品質向上について、ご意見をお寄せください。

からお問い合わせください xdl-japan-doccomments@netapp.com

ご連絡の際は、件名に本ドキュメントのタイトル名「TR-4814 S3 のベストプラクティス」を含めてください。

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、ネットアップ サポート サイトで Interoperability Matrix Tool（IMT）を参照してください。NetApp IMT には、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4814-0121-JP

NetApp