設定
ONTAP 9

NetApp
April 29, 2024

目次

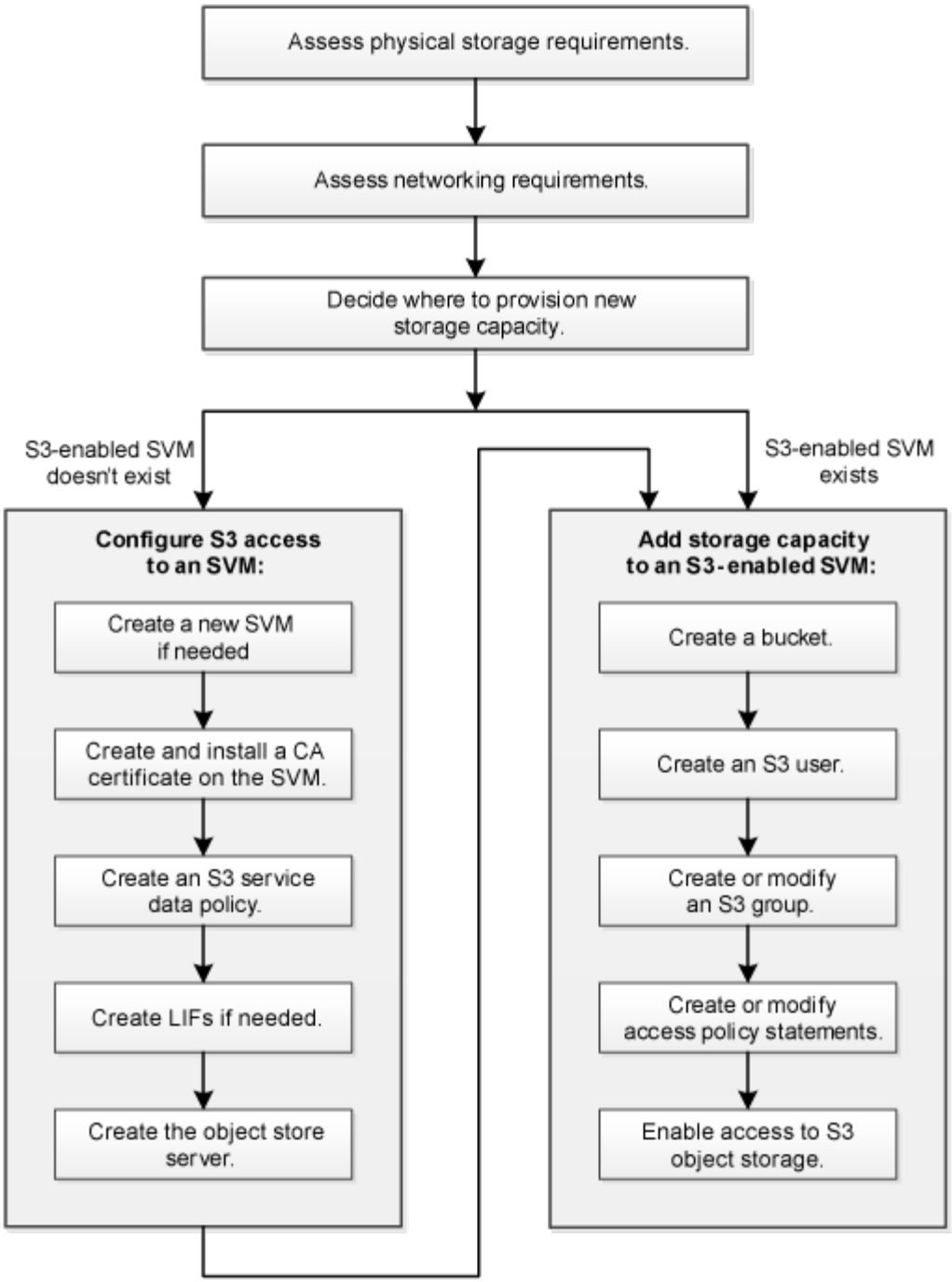
設定

S3 の設定プロセスについて

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て、目的に応じたワークフローを選択します。新規または既存の SVM への S3 アクセスを設定するか、すでに S3 アクセスの設定が完了している既存の SVM にバケットとユーザを追加するかによってワークフローが異なります。

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の情報を入力するように求められ、Storage VMとS3オブジェクトストレージサーバは一度に作成されます。



物理ストレージ要件を評価

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することができます。

このタスクについて

S3 対応 SVM で S3 バケットを作成すると、バケットをサポートする FlexGroup ボリュームが自動的に作成されます。基盤となるアグリゲートや FlexGroup コンポーネントを ONTAP Select で自動的に（デフォルト）選択するか、基盤となるアグリゲートや FlexGroup コンポーネントを手動で選択することができます。

アグリゲートと FlexGroup コンポーネントを指定する場合は、たとえば基盤となるディスクに固有のパフォーマンス要件がある場合などに、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のガイドラインに従っていることを確認する必要があります。詳細はこちら。

- "FlexGroup ボリューム管理"
- "ネットアップテクニカルレポート 4571-A ：『 NetApp ONTAP FlexGroup Volume Top Best Practices 』"

バケットをCloud Volumes ONTAP から提供している場合は、基盤となるアグリゲートを手動で選択して、使用するノードが1つだけになるように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、ノードが地理的に分離された可用性ゾーンに配置されるため、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及ぼす可能性があります。 詳細はこちら "Cloud Volumes ONTAP 用バケットの作成"。

ONTAP S3 サーバを使用して、ローカルの FabricPool 大容量階層、つまり高パフォーマンス階層と同じクラスタに作成できます。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、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
   ```

   十分なスペースがあるアグリゲートや必要なノードの場所がある場合は、S3構成用のアグリゲートの名前を記録します。

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

2. 十分なスペースまたは必要なノードの場所を備えたアグリゲートがない場合は、を使用して既存のアグリゲートにディスクを追加します `storage aggregate add-disks` コマンドを実行するか、を使用して新しいアグリゲートを作成します `storage aggregate create` コマンドを実行します

ネットワーク要件を評価

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

作業を開始する前に

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

このタスクについて

リモートの FabricPool 容量（クラウド）階層およびリモートの S3 クライアントの場合は、データ SVM を使用してデータ 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、これ以上 LIF を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、他のクラスタからローカル階層に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。

  このオプションを使用するには追加の設定が必要です。たとえば、 S3 プロトコルの LIF を有効にする必要がありますが、ローカル階層には他のクラスタのリモート FabricPool クラウド階層としてもアクセスできます。

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高であるポートを使用する必要があります。
   - 最大限のパフォーマンスを得るためには、データネットワーク内のすべてのコンポーネントの MTU 設定が同じである必要があります。

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

   ```
   network subnet show
   ```

サブネットには、同じレイヤ 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、を使用して作成されます `network subnet create` コマンドを実行します

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

新しい **S3** ストレージ容量のプロビジョニング先を決定します

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 に配置するかを決めておく必要があります。これにより、ワークフローが決まります。

選択肢

- 新しい SVM または S3 に対して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、次のトピックに記載された手順を実行します。

  "S3 用の SVM を作成します"

  "S3のバケットを作成します"

  S3 は NFS と SMB を備えた SVM 内にも共存できますが、次のいずれかに該当する場合は、新しい SVM を作成することもできます。

  - 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 を有効にしたあとに、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 に初期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、次のトピックに記載された手順を実行します。

  "S3のバケットを作成します"

SVM への **S3** アクセスを設定する

S3 用の **SVM** を作成します

S3はSVM内で他のプロトコルと共存できますが、新しいSVMを作成してネームスペースとワークロードを分離することもできます。

このタスクについて

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サーバでDNS設定を行う必要はありません。ただし、他のプロトコルを使用する場合は、 SVM に DNS を設定できます。

System Managerを使用して新しいStorage VMへのS3アクセスを設定すると、証明書とネットワークの情報を入力するように求められ、Storage VMとS3オブジェクトストレージサーバは一度に作成されます。

例 **1.** 手順

System Manager の略

S3サーバ名を完全修飾ドメイン名（FQDN）として入力できるようにして、クライアントがS3アクセスに使用できるようにしておく必要があります。S3サーバのFQDNの先頭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用の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、この手順中に証明書の入力を求められます。システムで生成された証明書を使用することもできます。

1. Storage VM で S3 を有効にします。

   a. 新しい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。

   S3サーバを既存のStorage VMに追加する場合は、* Storage > Storage VM*をクリックし、Storage VMを選択して* Settings *をクリックし、をクリックします ⚙ * S3 の下 * 。

   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と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

   c. ネットワークインターフェイスを入力してください。

2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書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。
   - シークレットキーは今後表示されません。
   - 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 の使用

1. クラスタ上で S3 のライセンスが有効であることを確認します。

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

   表示されない場合は、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>
```

- にUNIX設定を使用します `-rootvolume-security-style` オプション
- デフォルトのC.UTF-8を使用します `-language` オプション
- 。 `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` フィールドにはを表示する必要があります `running` 状態。が表示された場合 `initializing` 状態にすると、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 内に作成します。

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

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

次のコマンドは、1GBのルートボリュームでSVMが作成され、自動的に起動されてに追加されたことを示しています `running` 状態。ルートボリュームには、ルールを含ま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、に配置されます `locked` 状態。vsadmin ロールがデフォルトの 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
```

CA 証明書を作成して SVM にインストールします

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。

このタスクについて

HTTP のみを使用するように S3 サーバを設定することは可能ですが、 CA 証明書が不要なクライアントを設定することも可能です。ただし、 ONTAP S3 サーバへの HTTPS トラフィックを CA 証明書を使用して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の場合、 CA 証明書は必要ありません。

この手順に記載されている手順では、 ONTAP 自己署名証明書を作成してインストールします。サードパーティベンダーの CA 証明書もサポートされています。詳細については、管理者認証のドキュメントを参照してください。

"管理者認証と RBAC"

を参照してください `security certificate` 追加の設定オプションのマニュアルページ

手順

1. 自己署名デジタル証明書を作成します。

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

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

   。 `-common-name` オプションを指定すると、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、この手順の以降の手順で名前を保存してください。

2. 証明書署名要求を生成します。

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

   。 `-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。

   今後の参照用に、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、他の署名の詳細を指定できます。

     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`

   公開鍵証明書を保存しておき、以降のクライアント側の設定に使用します。

   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
```

S3 サービスデータポリシーを作成する

S3 のデータサービスと管理サービスのサービスポリシーを作成できます。LIF 上の 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。

このタスクについて

データ LIF とクラスタ間 LIF を使用する場合は、 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、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を提供する際には S3 だけを使用することを推奨します。

手順

1. 権限の設定を advanced に変更します。

   ```
   set -privilege advanced
   ```

2. サービスデータポリシーを作成します。

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

   。 `data-core` および `data-s3-server` ONTAP S3を有効にするために必要なサービスは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。

データ LIF を作成します。

新しい SVM を作成した場合、 S3 アクセス用に作成する専用の LIF はデータ LIF です。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。
- 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。これらはを使用して作成されます `network subnet create` コマンドを実行します

- 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。

このタスクについて

- 同じネットワークポート上に IPv4 と IPv6 の両方の LIF を作成できます。
- クラスタ内のLIFの数が多い場合は、を使用して、クラスタでサポートされるLIFの容量を確認できます `network interface capacity show` コマンドとを使用して、各ノードでサポートされるLIFの容量を確認します `network interface capacity details show` コマンド（advanced権限レベル）。

- 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、の実行時にLIFが戻るノードです `network interface revert` LIFに対してコマンドを実行します。

     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` オプション

   - `-home-port` は、の実行時にLIFが戻る物理ポートまたは論理ポートです `network interface revert` LIFに対してコマンドを実行します。
   - でIPアドレスを指定できます `-address` および `-netmask` オプションを選択するか、を使用してサブネットからの割り当てを有効にします `-subnet_name` オプション
   - 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。
   - サブネットを使用せずに手動で IP アドレスを割り当てると、クライアントまたはドメインコントローラが別の IP サブネットにある場合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。
   - をクリックします `-firewall-policy` オプションで、同じデフォルトを使用します `data` をLIFのロールとして使用します。

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

     > ONTAP 9.10.1以降では、ファイアウォールポリシーは廃止され、完全にLIFのサービスポリシー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します"。

   - `-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。デフォルト設定はです `false`に設定することもできます `false` 環境内のネットワーク管理ポリシーによって異なります。
   - 。 `-service-policy` optionは、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. でIPv6アドレスを割り当てる場合 `-address` オプション：

   a. を使用します `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するコマンド。

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

b. の形式を使用します `prefix:id` 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。

を導出するため `id`で、ランダムな64ビット16進数を選択します。

3. 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` コマンドを実行します
4. 設定した IP アドレスに到達できることを確認します。

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

例

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

```
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 および datalif3 というデータ LIF には IPv4 アドレスを設定しています。一方、 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.
```

リモートの **FabricPool** 階層化用にクラスタ間 **LIF** を作成する

ONTAP S3 を使用してリモートの FabricPool 容量（クラウド）階層化を有効にする場合は、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。

作業を開始する前に

- 基盤となる物理または論理ネットワークポートが管理用に設定されている必要があります `up` ステータス。

- 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。

このタスクについて

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クラスタ間 LIF は必要ありません。

手順

1. クラスタ内のポートの一覧を表示します。

   ```
   network port show
   ```

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

   ```
   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を作成します `cluster01_icl01` および `cluster01_icl02`：

```
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、クラスタ間LIFを示しています `cluster01_icl01` および `cluster01_icl02` をクリックします `e0c` ポートはにフェイルオーバーします `e0d` ポート：

```
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
```

S3 オブジェクトストアサーバを作成します

ONTAP オブジェクトストアサーバは、 ONTAP NAS サーバおよび SAN サーバが提供するファイルストレージまたはブロックストレージではなく、データを S3 オブジェクトとして管理します。

作業を開始する前に

S3サーバ名を完全修飾ドメイン名（FQDN）として入力できるようにして、クライアントがS3アクセスに使用できるようにしておく必要があります。バケット名の先頭にFQDNを使用することはできません。

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

このタスクについて

オブジェクトストアサーバを作成すると、 UID 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もシークレットキーも生成されません。ONTAP 管理者はを実行する必要があります `object-store-server users regenerate-keys` コマンドを使用して、このユーザのアクセスキーとシークレットキーを設定します。

> ネットアップ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は、オブジェクトストア内のすべてのバケットとオブジェクトにフルアクセスできます。

を参照してください `vserver object-store-server` 追加の設定オプションおよび表示オプションのマニュアルページ

例 **2.** 手順

System Manager の略

既存のStorage VMにS3サーバを追加する場合は、この手順 を使用します。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用の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。* Storage > Storage VM*をクリックし、Storage VMを選択して* Settings *をクリックし、をクリックします ⚙ * S3 の下 * 。
   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と独自の証明書のどちらを選択した場合も、クライアントアクセスには証明書が必要です。

   d. ネットワークインターフェイスを入力してください。
2. システムで生成された証明書を選択した場合は、新しい Storage VM の作成を確認すると証明書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。
   - シークレットキーは今後表示されません。
   - 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 の使用

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]
   ```

   S3 サーバの作成時またはあとからいつでも追加のオプションを指定できます。

   - 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 でデフォルトで有効になっています。ポート番号はを使用して変更できます `-secure-listener-port` オプション

     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。

   - 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。を使用して有効にできます `-is-http-enabled` オプションを選択するか、ポート番号を `-listener-port` オプション

     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

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。

作業を開始する前に

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。

このタスクについて

- 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ボリュームを作成すると、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 9.14.1のあとに最初に作成または削除されたバケットによって、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。
  - ONTAP 9.14.1より前に作成されたS3 FlexGroupボリュームに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で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。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と、デフォルトのストレージサービスレベルのいずれかを使用する代わりに、そのグループを定義して使用することもできます。ストレージサービスの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、ストレージをプロビジョニングすると QoS がデフォルトで有効になります。QoS を無効にするか、プロビジョニングプロセス中またはあとからカスタムの QoS ポリシーを選択できます。
- 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 対応の Storage VM で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階層化にのみ使用できます。
- ONTAP 9.14.1以降では、次のことが可能です。 "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"。
- CLIでは、バケットを作成する際に、次の2つのプロビジョニングオプションを選択できます。
  - 基盤となるアグリゲートと FlexGroup コンポーネントを ONTAP Select に提供（デフォルト）
    - ONTAP は、アグリゲートを自動的に選択することで、最初のバケット用の FlexGroup ボリュームを作成して設定します。プラットフォームに使用できる最も高いサービスレベルが自動的に選択されるほか、ストレージサービスレベルを指定することもできます。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。
    - また、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。この場合、 ONTAP は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：
    - 新しいバケットにアグリゲートとコンスティチュエントを指定すると、新しいバケット用の新しい FlexGroup が作成されます。
    - 新しいバケットに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、新しいバケットが既存の FlexGroup に追加されます。 を参照してください FlexGroup ボリューム管理 を参照してください。

      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、を使用してあとで実行できます `vserver object-store-server bucket modify` コマンドを実行します

    を参照してください "vserver object-store-serverバケットmodifyの数が変更されました" 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。基盤となるアグリゲートを手動で選択し、いずれかのノードだけを使用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、ノードが地理的に分離された可用性ゾーンに配置されるため、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及ぼす可能性があります。

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]
   ```

   Storage VM名には、データStorage VMまたは `Cluster` （システムStorage VM名）（ローカルの階層化を設定する場合）。

   オプションを指定しない場合、ONTAPは800GBのバケットを作成し、サービスレベルをシステムで使用可能な最も高いレベルに設定します。

   パフォーマンスまたは使用量に基づいて ONTAP で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

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

   - 階層化

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

     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。

   - 。 `-aggr-list` パラメータは、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。

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

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

   - 。 `-aggr-list-multiplier` パラメータは、に表示されるアグリゲートを反復する回数を指定します `-aggr-list` FlexGroup ボリューム作成時のパラメータ。

     のデフォルト値 `-aggr-list-multiplier` パラメータは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

次の例は、Storage VMのバケットを作成します。 `vs1` サイズ `1TB` アグリゲートを指定する場合

```
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
   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。
        - どのグループポリシーも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。

          S3 root ユーザを使用して ONTAP オブジェクトストレージを管理したり権限を共有したりしないでください。オブジェクトストアに無制限にアクセスできます。代わりに、割り当てた管理者権限を持つユーザまたはグループを作成してください。

        - システムで最も利用可能なサービス品質（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、を参照してください。 "AmazonのS3バケットでのバージョン管理の使用"。

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、 "ONTAP One"。 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 "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、次の手順を実行します。 "SnapLockライセンスがインストールされていることの確認"。SnapLockライセンスがインストールされていない場合は、 "をインストールします" オブジェクトロックを有効にする前に有効にします。SnapLockライセンスがインストールされていることを確認したら、バケット内のオブジェクトが削除または

上書きされ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コンプライアンス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。オブジェクトのロックは、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 "新しいバケット用のミラーを作成します"。

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。

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

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。

このタスクについて

- 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。
- プロビジョニングのガイドラインは、と同じです。 "バケットを作成する" MetroCluster環境でのバケットの作成に適用
- 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*。

- S3 SnapMirrorの略
- 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

作業を開始する前に

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 の使用

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]
   ```

   を設定します `-use-mirrored-aggregates` オプションをに設定します `true` または `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よって異なります。

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

   - 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、ONTAPは800GBのバケットを作成し、サービスレベルをシステムで使用可能な最も高いレベルに設定します。
   - パフォーマンスまたは使用量に基づいて ONTAP で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

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

     - 階層化

       を含めます `-used-as-capacity-tier true` オプション
   - 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。
     - 。 `-aggr-list` パラメータは、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。

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

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

   - 。 `-aggr-list-multiplier` パラメータは、に表示されるアグリゲートを反復する回数を指定します `-aggr-list` FlexGroup ボリューム作成時のパラメータ。

     のデフォルト値 `-aggr-list-multiplier` パラメータは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

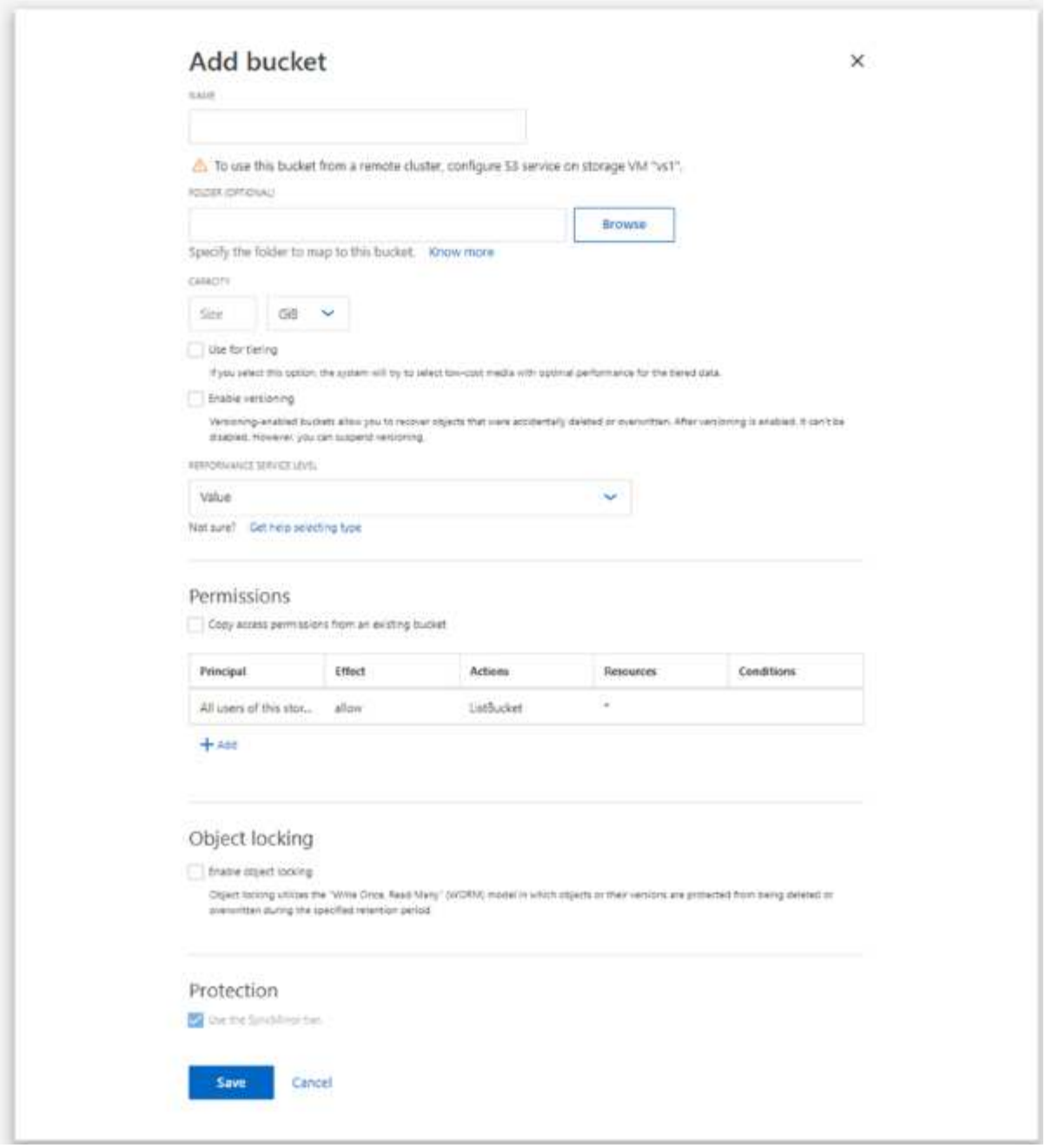
次の例では、ミラーされたアグリゲート上に1TBのSVM vs1のバケットを作成します。

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

System Manager の略

1. S3 対応 Storage VM に新しいバケットを追加
   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。
  - どのグループポリシーも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。

> S3 root ユーザを使用して ONTAP オブジェクトストレージを管理したり権限を共有したりしないでください。オブジェクトストアに無制限にアクセスできます。代わりに、割り当てた管理者権限を持つユーザまたはグループを作成してください。

  - システムで最も利用可能なサービス品質（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. 別の ONTAP システムまたは外部のサードパーティ製アプリケーションである S3 クライアント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。
   - ユーザー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。

バケットライフサイクル管理ルールを作成します

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"。

作業を開始する前に

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。を参照してください "S3 用の SVM を作成します" を参照してください。

このタスクについて

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の操作は次のとおりです。 `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の操作は次のとおりです。 `NoncurrentVersionExpiration`。
- 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の操作は次のとおりです。 `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の操作は次のとおりです。 `AbortIncompleteMultipartUpload`。

使用する手順は、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を使用してライフサイクル管理ルールを作成し、S3バケット内のオブジェクトを期限切れにすることができます。

作業を開始する前に

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ようにな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をクリーンアップします
AbortIncompleteMultipartUpload の略	• `-after-initiation-days` -アップロードを中止できる開始日数。この日数を過ぎるとアップロードが中止されます

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. を使用します `vserver object-store-server bucket lifecycle-management-rule create` バケットライフサイクル管理ルールを作成するためのexpirationアクションタイプの必須フィールドを含むコマンド。

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することができます。S3オブジェクトのライフサイクル管理ルールを追加、編集、削除できます。また、あるバケット用に作成され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は、あとで無効にして有効にすることができます。

ライフサイクル管理ルールを追加します。

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. をクリックします ⋮ 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。ルールごとに1つのプレフィックスを入力できます。有効なプレフィックスが指定されていないかぎり、ルールはバケット内のすべてのオブジェクトを環境にします。
   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：バージョンが最新でなくなってから削除できるようになるまでの日数と、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. をクリックします ⋮ 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。一度に1つのルールを選択できます。デフォルトでは最初のルールが選択されます。
7. [* インポート *] をクリックします。

ルールの編集、削除、または無効化

編集できるのは、ルールに関連付けられているライフサイクル管理アクションのみです。ルールがオブジェクトタグでフィルタされている場合は、**[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. をクリックします ⋮ 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。

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。

このタスクについて

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。S3ユーザのキーは、 `vserver object-store-server user show` コマンドを実行します

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、特定の権限を指定してadminユーザロールを作成することを推奨します。

CLI の使用

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 `-key-time-to-live` パラメータ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、次のように入力します。
     `P1DT2H3M4S`。指定されていないかぎり、キーは無期限に有効です。

     次の例では、という名前のユーザを作成します。 `sm_user1` Storage VM上 `vs0`キーの保持期間は1週間です。

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

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

System Manager の略

1. Storage > Storage VM* をクリックします。ユーザを追加する必要があるStorage VMを選択し、*[設定]*を選択して S3 の下。
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、または秒で指定できます。デフォルトでは、この値は `0` これは、キーが無期限に有効であることを示します。
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します

S3 グループを作成または変更します

適切なアクセス許可を持つ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。

作業を開始する前に

S3 対応 SVM の S3 ユーザがすでに存在している必要があります。

このタスクについて

S3 グループのユーザには、 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 のユーザには許可できません。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。

- をバケットレベルで指定します

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

- をクリックします

  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のポリシー名を指定します。これらのポリシーによって、バケットとグループメンバーのアクセスが決まります。

System Manager の略

1. Storage VM を編集します。 * Storage > Storage VM* をクリックし、 Storage VM をクリックして * Settings * をクリックし、をクリックします ✎ S3 の下。
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、今すぐ追加するか、あとからポリシーを追加できます。

CLI の使用

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

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 ユーザを作成します"。

CLI の使用

1. 次の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ます。 `vserver object-store-server user regenerate-keys` コマンドを実行します
2. デフォルトでは、生成されたキーは無期限に有効です。9.14.1以降では、キーの保持期間を変更できます。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、次のように入力します。 `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。

System Manager の略

1. Storage > Storage VM* をクリックし、 Storage VM を選択します。
2. [* 設定 *] タブで、をクリックします を * S3 * タイルに追加します。
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、 アイコン"] ユーザーの横にある*[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。

アクセスポリシーステートメントを作成または変更します

バケットとオブジェクトストアのサーバポリシーについて

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のサーバポリシーによって制御されます。ユーザまたは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あると考えられますが、ユーザやグループが多数ある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。

バケットポリシーを変更する

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コンテナバケットなので、バケットが 1 つしかない場合は最も適しています。

作業を開始する前に

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。

このタスクについて

新しいユーザとグループに新しいステートメントを追加したり、既存のステートメントの属性を変更したりできます。その他のオプションについては、を参照してください `vserver object-store-server bucket policy` マニュアルページ

ユーザとグループの権限は、バケットの作成時または必要に応じてあとから付与できます。バケットの容量と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の処理 `GetObjectTagging`、 `PutObjectTagging`および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

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

System Manager の略

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に、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 アドレスを指定できます。

> ONTAP 9.14.1以降では、* Resources *フィールドでバケットポリシーの変数を指定できます。これらの変数はプレースホルダであり、ポリシーの評価時にコンテキスト値に置き換えられます。例えば、 `${aws:username}` がポリシーの変数として指定されている場合、この変数は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。

CLI の使用

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`	この文では ' アクセスを許可または拒否できます
`-action`	を指定できます `*` すべてのアクション、または次の1つ以上のリストを意味します。 `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, および `ListMultipartUploadParts`。

`-principal`	1 つ以上の S3 ユーザまたはグループのリスト。 • 最大 10 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、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すべてのオブジェクト。ワイルドカード文字 `*` および `?` リソースを指定するための正規表現を作成するために使用できます。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、ポリシーが評価されるときにコンテキスト値に置き換えられるプレースホルダです。

オプションで、テキスト文字列をコメントとして指定できます `-sid` オプション

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用のサーババケットポリシーステートメントを作成します。 `svm1` および `bucket1`、およびを指定します。 `${aws:username}` ポリシーリソースの変数として指定します。ポリシーが評価されると、ポリシー変数は要求コンテキストのユーザ名に置き換えられ、そのユーザに対して設定されたとおりにポリシーアクションを実行できます。たとえば、次のポリシーステートメントが評価されると、 `${aws:username}` は、S3処理を実行するユーザに置き換えられます。ユーザーが `user1` 操作を実行し、そのユーザーにアクセスを許可します。 `bucket1` として `bucket1/user1/*`。

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

オブジェクトストアサーバポリシーを作成または変更する

オブジェクトストア内の 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のポリシーをユーザのグループに関連付けることで、複数のバケット間のリソースアクセスの管理を簡易化することができます。

作業を開始する前に

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。

このタスクについて

オブジェクトストレージサーバグループにデフォルトまたはカスタムのポリシーを指定することで、 SVM レベルでアクセスポリシーを有効にすることができます。ポリシーは、グループ定義で指定され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の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使用する読み取り専用のデフォルトポリシーは 3 つあります。

- フルアクセス
- NoS3アクセス
- ReadOnlyAccess の略

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に新しいステートメントを追加したり、既存のステートメントの属性を変更したりすることもできます。その他のオプションについては、を参照してください `vserver object-store-server policy` "コマンドリファレンス"。

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の処理 `GetObjectTagging`、 `PutObjectTagging`および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

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

System Manager の略

- 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。 * Storage > Storage VM* をクリックし、 Storage VM をクリックして * Settings * をクリックし、をクリックします S3 の下。
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際には、次のパラメータを指定できます。

      - グループ：アクセス権が付与されるグループ。
      - Effect ： 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。
      - アクション：特定のグループの 1 つ以上のバケットで許可されるアクション。
      - リソース：アクセスが許可または拒否されるバケット内のオブジェクトのパスと名前。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 の使用

- 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`	この文では ' アクセスを許可または拒否できます

-action	を指定できます * すべてのアクション、または次の1つ以上のリストを意味します。 GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, および ListMultipartUploadParts。
-resource	バケットとバケットに含まれるすべてのオブジェクト。ワイルドカード文字 * および ? リソースを指定するための正規表現を作成するために使用できます。

オプションで、テキスト文字列をコメントとして指定できます -sid オプション

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末尾に追加され、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、ステートメントのを変更するオプションがあります -index 処理順序を変更するための設定。

外部ディレクトリサービス用の**S3**アクセスの設定

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バケットへの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 の使用方法の概要"。

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。

作業を開始する前に

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。を参照してください "S3 用の SVM を作成します"。
2. そのStorage VMにバケットが作成されている。を参照してください "バケットを作成する"。
3. Storage VMにDNSが設定されています。を参照してください "DNS サービスを設定する"。
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。を参照してください "自己署名ルート CA 証明書を SVM にインストールします"。

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。を参照してください "LDAP クライアント設定を作成します" および "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
```

このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

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 `principal` アクセスを許可するLDAPグループにを設定します。

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

例：次の例では、 `buck1`。このポリシーは、LDAPグループへのアクセスを許可します。 `group1` リソース（バケットとそのオブジェクト）に `buck1`。

```
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 `group1` S3クライアントからS3処理を実行できます。

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
```

このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

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 -エンコード(ldapuser:password)。結果は次のようになります。
      `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

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

   b. ユーザ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。

LDAPユーザまたはドメインユーザが自分のS3アクセスキーを生成できるようにする

ONTAP 9.14.1以降では、ONTAP管理者がカスタムロールを作成してローカルグループ、ドメイングループ、またはLightweight Directory Access Protocol（LDAP）グループに付与し、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に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。

作業を開始する前に

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。を参照してください "S3 用の SVM を作成します"。
2. そのStorage VMにバケットが作成されている。を参照してください "バケットを作成する"。
3. Storage VMにDNSが設定されています。を参照してください "DNS サービスを設定する"。
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。を参照してください "自己署名ルート CA 証明書を SVM にインストールします"。
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。を参照してください "LDAP クライアント設定を作成します" および。
6. クライアント設定をSVMに関連付けます。を参照してください "LDAP クライアント設定を SVM に関連付けます" および "vserver services name-service ldap createを使用して"。
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。を参照してください "ネットワークインターフェイスの作成" および "network interface service-policy createを実行します" コマンド

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
```

このコマンドの詳細については、を参照してください "vserver services name-service ns-switch modify" コマンドを実行します

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します。
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
この例では、を使用しています `s3-role` Storage VMのユーザ用にロールが生成されました `svm-1`をクリックします。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
```

このコマンドの詳細については、を参照してください "security login rest -role create" コマンドを実行します

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。このコマンドの詳細については、を参照してください "security login create を実行します" コマンドを実行します

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

この例では、LDAPグループ `ldap-group-1` が作成された場所 `svm-1`、およびカスタムロール `s3role` APIエンドポイントにアクセスするために追加され、高速バインドモードで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できます"。

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にONTAPへの制限付きアクセスが許可されます。 `/api/protocols/s3/services/{svm.uuid}/users` エンドポイント。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ください。 "APIドキュメント"。

HTTP メソッド	パス
投稿（ Post ）	/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します

リモートの FabricPool 階層化のために ONTAP S3 アクセスを有効にします

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

このタスクについて

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 サーバ内のリモート ONTAP S3 サーバのホスト名のエントリに、 S3 サーバの FQDN 名と LIF の IP アドレスが含まれている必要があります。
- クラスタピアリングは必要ありませんが、ローカルクラスタにクラスタ間LIFを設定する必要があります。

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

"FabricPool を使用したストレージ階層の管理"

ローカルの **FabricPool** 階層化のために **ONTAP S3** アクセスを有効にします

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、パフォーマンス階層のアグリゲートにオブジェクトストアを接続して FabricPool を作成する必要があります。

作業を開始する前に

ONTAP S3サーバ名とバケット名を確認し、（と）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` パラメータ）。

このタスクについて

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の情報が含まれています。

作成したオブジェクトストア設定は、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。ローカル階層には複数のバケットを作成できますが、 1 つのバケットに複数のオブジェクトストアを作成することはできません。

ローカルの大容量階層には FabricPool ライセンスは必要ありません。

手順

1. ローカルの大容量階層用のオブジェクトストアを作成します。

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

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

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

2. オブジェクトストアの設定情報を表示して確認します。

   `storage aggregate object-store config show`

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

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

4. オブジェクトストアをアグリゲートに接続します。

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

   を使用できます `allow-flexgroup` **`true`** 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するオプション。

```
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 アプリケーションからのクライアントアクセスを有効にします

S3 クライアントアプリケーションが ONTAP S3 サーバにアクセスするためには、ONTAP S3 管理者が S3 ユーザに設定情報を指定する必要があります。

作業を開始する前に

S3クライアントアプリケーションが、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
- シグニチャバージョン2、ONTAP 9.11.1以降

それ以外のシグニチャバージョンは、ONTAP S3でサポートされていません。

ONTAP S3 管理者は、 S3 ユーザを作成し、個々のユーザまたはグループメンバーとして、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で ONTAP S3 サーバ名を解決できる必要があります。そのためには、ONTAP S3 管理者が S3 サーバの LIF の S3 サーバ名（ FQDN ）と IP アドレスを指定する必要があります。

このタスクについて

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

  キーと値のペアのセットは、 PUT （または POST ）を使用してオブジェクトを作成するときに、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

  キーと値のペアのセットは、オブジェクトを分類するためのタグとして個別に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 REST API でオブジェクトから独立して作成および読み取りされ、オブジェクトの作成時または作成後にいつでも実装されます。

  > クライアントがタグ情報を取得および取得できるようにするには、アクションを実行します `GetObjectTagging`、 `PutObjectTagging`および `DeleteObjectTagging` バケットまたはグループポリシーを使用して許可されている必要があります。

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

ストレージサービスの定義

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
価値	TBあたり128	TBあたり512	七五	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	TB あたり 4096	500ドル	2 ミリ秒	はい。
最高レベル	TBあたり6、144	TB あたり 12288 回	1000	1 ミリ秒	はい。

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	価値
仮想マシンディスク	価値
FlexArray LUN の略	価値
ハイブリッド	価値
大容量フラッシュ	価値
ソリッドステートドライブ（ SSD ） - AFF 以外のドライブです	価値
パフォーマンスが最適化されたフラッシュ - SSD （ AFF ）	最高レベル、パフォーマンス、バリュー