NASデータへのS3クライアントアクセスを提供

ONTAP 9

NetApp
April 24, 2024

目次

NASデータへのS3クライアントアクセスを提供

S3マルチプロトコルの概要

ONTAP 9.12.1以降では、S3プロトコルを実行するクライアントが、NFSプロトコルおよびSMBプロトコルを使用するクライアントに提供されているデータに再フォーマットせずにアクセスできるようにすることができます。この機能により、NASデータは引き続きNASクライアントに提供され、S3アプリケーション（データマイニングや人工知能など）を実行するS3クライアントにオブジェクトデータが提供されます。

S3マルチプロトコル機能は次の2つのユースケースに対応します。

1. S3クライアントを使用した既存のNASデータへのアクセス

   既存のデータが従来のNASクライアント（NFSまたはSMB）を使用して作成され、NASボリューム（FlexVol またはFlexGroup ボリューム）にある場合、S3クライアント上の分析ツールを使用してこのデータにアクセスできるようになりました。

2. NASとS3の両方のプロトコルを使用したI/O処理に対応できる、最新のクライアント用のバックエンドストレージです

   NASプロトコルとS3プロトコルの両方を使用して同じデータの読み取りと書き込みが可能なSparkやKafkaなどのアプリケーションに、統合アクセスを提供できるようになりました。

S3マルチプロトコルの仕組み

ONTAP マルチプロトコルを使用すると、同じデータセットをファイル階層またはバケット内のオブジェクトとして表示できます。そのために、ONTAP はS3オブジェクト要求を使用してNASストレージ内のファイルの作成、読み取り、削除、および列挙をS3クライアントに許可する「S3 NASバケット」を作成します。このマッピングは、NASセキュリティ設定に準拠しており、ファイルおよびディレクトリのアクセス権限を監視し、必要に応じてセキュリティ監査証跡に書き込みます。

このマッピングは、指定されたNASディレクトリ階層をS3バケットとして提供することで実現されます。ディレクトリ階層内の各ファイルは、マップされたディレクトリから下の位置に相対的な名前を持つS3オブジェクトとして表され、ディレクトリ境界はスラッシュ文字（/）で表されます。

ONTAPで定義された通常のS3ユーザは、このストレージにアクセスできます。このストレージは、NASディレクトリにマッピングされるバケットに定義されたバケットポリシーで管理されます。これを可能にするには、S3ユーザとSMB / NFSユーザ間にマッピングを定義する必要があります。SMB / NFSユーザのクレデンシャルはNAS権限のチェックに使用され、これらのアクセスから発生する監査レコードに含まれます。

SMBクライアントまたはNFSクライアントが作成すると、ファイルはすぐにディレクトリに配置され、クライアントからはデータが書き込まれる前に参照できます。S3クライアントはセマンティクスが異なることを要求します。セマンティクスでは、新しいオブジェクトはすべてのデータが書き込まれるまでネームスペースに表示されません。S3からNASストレージへのマッピングではS3のセマンティクスを使用してファイルが作成され、S3の作成コマンドが完了するまでファイルは外部には表示されません。

S3 NASバケットのデータ保護

S3 NAS「バケット」は、S3クライアントのNASデータをマッピングするだけで、標準のS3バケットではありません。したがって、NetApp S3 SnapMirror機能を使用してS3 NASバケットを保護する必要はありません。代わりに、非同期SnapMirrorボリュームレプリケーションを使用して、S3 NASバケットを含むボリュームを保護できます。SnapMirror SynchronousおよびSVMディザスタリカバリはサポートされていません。

ONTAP 9.14.1以降では、MetroCluster IPおよびFC構成の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でS3 NASバケットがサポートされます。

詳細はこちら "非同期SnapMirror"。

S3 NASバケットの監査

S3 NASバケットは従来のS3バケットではないため、S3監査を設定してアクセスを監査することはできません。の詳細を確認してください "S3監査"。

ただし、S3 NASバケットにマッピングされているNASファイルとディレクトリは、従来のONTAP 監査手順を使用してアクセスイベントを監査できます。したがって、S3処理ではNAS監査イベントがトリガーされますが、次の例外があります。

- S3ポリシーの設定（グループまたはバケットポリシー）によってS3クライアントアクセスが拒否された場合、イベントのNAS監査は開始されません。これは、SVMの監査チェックの前にS3権限がチェックされるためです。
- S3 GET要求のターゲットファイルのサイズが0の場合、GET要求には0個のコンテンツが返され、読み取りアクセスはログに記録されません。
- S3 GET要求のターゲットファイルがユーザにトラバース権限のないフォルダにある場合は、アクセスの試行が失敗し、イベントはログに記録されません。

詳細はこちら "SVMでNASイベントを監査する"。

S3およびNASの相互運用性

ONTAP S3 NASバケットは、ここに記載されている点を除いて、NASとS3の標準機能をサポートします。

NAS機能は、現在**S3 NAS**バケットではサポートされていません

FabricPool の大容量階層

S3 NASバケットをFabricPool の大容量階層として設定することはできません。

S3 NASバケットでは現在、**S3**機能はサポートされていません

AWSユーザメタデータ

- S3ユーザメタデータの一部として受信したキーと値のペアは、現在のリリースのオブジェクトデータと一緒にディスクに格納されません。
- プレフィックスが「x-amz-meta」の要求ヘッダーは無視されます。

AWSタグ

- PUT Object要求とMultipart Initiate要求では、プレフィックスが「x-amz-tagging」のヘッダーは無視さ

れます。

- 既存のファイル（つまり、「tagging」クエリー文字列を持つPUT、GET、Deleteの各要求）でタグを更新する要求は、エラーで拒否されます。

バージョン管理

バージョン管理をバケットのマッピング設定で指定することはできません。

- バージョンがnullでない仕様（versionId=xyzクエリ文字列）を含む要求は、エラー応答を受信します。
- バケットのバージョン管理状態に影響する要求は拒否され、エラーが発生します。

マルチパート処理

次の操作はサポートされません。

- AbortMultipartUpload の略
- CompleteMultipartUpload
- CreateMultipartUpload を実行します
- ListMultipartUpload の略

NASデータのS3クライアントアクセス要件

NASファイルとディレクトリをS3アクセス用にマッピングする場合は、互換性が確保されていない問題がいくつかあることに注意してください。NASファイル階層は、S3 NASバケットを使用して階層を提供する前に調整しなければならない場合があります。

S3 NASバケットは、S3バケット構文を使用してディレクトリをマッピングすることでNASディレクトリへのS3アクセスを提供し、ディレクトリツリー内のファイルはオブジェクトとみなされます。オブジェクト名は、S3バケットの設定で指定されたディレクトリに相対的な、ファイルのスラッシュで区切られたパス名です。

このマッピングは、S3 NASバケットを使用してファイルとディレクトリにサービスを提供する際にいくつかの要件を適用します。

- S3の名前は1024バイトに制限されているため、長いパス名を持つファイルにS3を使用してアクセスすることはできません。
- ファイル名とディレクトリ名は255文字に制限されているため、オブジェクト名には、連続する255文字以外の文字（「/」）を使用できません
- バックスラッシュ（「\」）で区切られたSMBパス名は、s3にはスラッシュ（「/」）ではなく、オブジェクト名として表示されます。
- 有効なS3オブジェクト名のペアの一部は、マッピングされたNASディレクトリツリーに共存できません。たとえば、有効なS3オブジェクト名「part1/part2」と「part1/part2/part3」は、NASディレクトリツリーに同時に存在できないファイルにマッピングされます。「part1/part2」は、最初の名前に含まれるファイルで、もう一方の名前に含まれるディレクトリです。
  - 「part1/part2」が既存のファイルの場合、「part1/part2/part3」のS3作成は失敗します。
  - "part1/part2/part3"が既存のファイルの場合、"part1/part2"のS3作成または削除が失敗します。
  - 既存のオブジェクトの名前と一致するS3オブジェクトの作成によって、（バージョン管理されていな

いバケット内の）既存のオブジェクトが置き換えられます。これはNASを保持するが、完全に一致する必要があります。上記の例では、名前が競合している間は原因 によって既存のオブジェクトが削除されないため、これらのオブジェクトは削除されません。

オブジェクトストアは非常に多くの任意の名前をサポートするように設計されていますが、NASディレクトリ構造では、非常に多数の名前が1つのディレクトリに配置されているとパフォーマンスの問題が発生する可能性があります。特に、名前にスラッシュ（/）文字が含まれていない場合、名前はすべてNASマッピングのルートディレクトリに配置されます。NASに対応していない名前を多用するアプリケーションは、NASマッピングではなく実際のオブジェクトストアバケットでホストされる方が適切です。

NASデータへのS3プロトコルアクセスを有効にします

S3プロトコルアクセスを有効にするには、NAS対応のSVMがS3対応サーバと同じ要件を満たしていることを確認する（オブジェクトストアサーバの追加、ネットワークと認証の要件の確認を含む）ことが必要です。

ONTAP を新規にインストールする場合は、クライアントにNASデータを提供するようにSVMを設定したあとに、SVMへのS3プロトコルアクセスを有効にすることを推奨します。NASプロトコルの設定については、以下を参照してください。

- "NFS構成"
- "SMBの設定"

作業を開始する前に

S3プロトコルを有効にする前に、次の項目を設定する必要があります。

- S3プロトコルおよび目的のNASプロトコル（NFS、SMB、またはその両方）のライセンスが設定されている。
- SVMが目的のNASプロトコル用に設定されている。
- NFSサーバとSMBサーバが存在します。
- DNSおよびその他の必要なサービスが設定されていること。
- NASデータをクライアントシステムにエクスポートまたは共有しています。

このタスクについて

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。次の3つのソースのCA証明書を使用できます。

- 新しいONTAP 自己署名証明書をSVMに作成します。
- 既存のONTAP 自己署名証明書がSVMに存在している。
- サードパーティの証明書。

NASデータの提供に使用するS3 / NASバケットにも同じデータLIFを使用できます。特定のIPアドレスが必要な場合は、を参照してください "データ LIF を作成します。"。S3データトラフィックをLIFで有効にするには、S3サービスデータポリシーが必要です。SVMの既存のサービスポリシーを変更して、S3を含めることができます。

S3オブジェクトサーバを作成するときは、クライアントがS3アクセスに使用する完全修飾ドメイン名

（FQDN）としてS3サーバ名を入力できるように準備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。

System Manager の略

1. NASプロトコルが設定されているStorage VMでS3を有効にします。
   a. Storage > Storage VM*の順にクリックし、NAS対応のStorage VMを選択して、Settings（設定）をクリックし、をクリックします ⚙ S3 の下。
   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. SVMでS3プロトコルが許可されていることを確認します。+ `vserver show -fields allowed-protocols`
2. このSVMの公開鍵証明書を記録します。[+] 新しいONTAP自己署名証明書が必要な場合は、を参照してください。 "CA 証明書を作成して SVM にインストールします"。
3. サービスデータポリシーを更新します
   a. SVMのサービスデータポリシーを表示します。+ `network interface service-policy show -vserver *svm_name*`
   b. を追加します `data-core` および `data-s3-server services` 表示されない場合は、[+] `network interface service-policy add-service -vserver *svm_name* -policy *policy_name* -services data-core,data-s3-server`
4. SVMのデータLIFが要件を満たしていることを確認します。+ `network interface show -vserver *svm_name*`
5. 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 *ca_cert_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。

- 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、-secure-listener-portオプションを使用して変更できます。[+] HTTPS を有効にすると、 SSL/TLS との適切な統合に CA 証明書が必要になります。
- HTTP はデフォルトではディセーブルです。イネーブルにすると、サーバはポート 80 をリッスンします。is-http-enabledオプションを指定して有効にするか、-listener-portオプションを使用してポート番号を変更できます。[+] HTTP が有効な場合は、すべての要求と応答がクリアテキストでネットワーク経由で送信されます。
  1. S3が必要に応じて設定されていることを確認します。+ `vserver object-store-server show`

例+ 次のコマンドは、すべてのオブジェクトストレージサーバの設定値を検証します。+ `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 NASバケットを作成する

S3 NASバケットは、S3バケット名とNASパスのマッピングです。S3 NASバケットを使用すると、既存のボリュームとディレクトリ構造を持つSVMネームスペースのすべての部分にS3アクセスを提供できます。

作業を開始する前に

- NASデータを含むSVMにS3オブジェクトサーバが設定されている。
- NASデータはに準拠しています "S3クライアントアクセスの要件"。

このタスクについて

S3 NASバケットは、SVMのルートディレクトリ内のすべてのファイルとディレクトリのセットを指定するように設定できます。

また、次のパラメータを任意に組み合わせて、NASデータへのアクセスを許可または禁止するバケットポリシーを設定することもできます。

- ファイルおよびディレクトリ
- ユーザおよびグループの権限
- S3処理

たとえば、大規模なユーザグループに読み取り専用データアクセスを許可するバケットポリシーと、そのデータのサブセットに対して処理を実行する権限を制限するグループが別々に必要になることがあります。

S3 NAS「バケット」はマッピングであり、S3バケットではないため、標準S3バケットの次のプロパティはS3 NASバケットには適用されません。

- * aggr-list\aggr-list-multiplier\storage-service-level\volume\size\exclude-aggr-list\qos-policy-group *+ S3 NASバケットの設定時にボリュームまたはqtreeが作成されません。
- * role\is-protected\is-protected-on-ontap\is-protected-on-cloud *+ S3 NASバケットは、S3 SnapMirrorを使用して保護またはミラーリングされませんが、代わりにボリューム単位で使用できる通常のSnapMirror保護を使用します。

- バージョン管理状態+ NASボリュームには通常、異なるバージョンを保存するためのSnapshotテクノロジが用意されています。ただし、バージョン管理は現在S3 NASバケットでは使用できません。
- * logical-used\ object-count *+ NASボリュームについては、volumeコマンドを使用して同等の統計情報を使用できます。

System Manager の略

NAS対応Storage VMに新しいS3 NASバケットを追加

1. [* 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。
2. S3 NASバケットの名前を入力してStorage VMを選択し、サイズを入力せずに* More Options *をクリックします。
3. 有効なパス名を入力するか、[参照]をクリックして有効なパス名のリストから選択します。[+] 有効なパス名を入力すると、S3 NAS設定に関連しないオプションは非表示になります。
4. S3ユーザをNASユーザとグループにすでにマッピングしている場合は、権限を設定し、* Save *をクリックします。[+] この手順で権限を設定する前に、S3ユーザをNASユーザにマッピングしておく必要があります。

それ以外の場合は、* Save *をクリックしてS3 NASバケットの設定を完了します。

CLI の使用

NASファイルシステムを含むSVMにS3 NASバケットを作成します。[+] `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-type nas -nas-path` *`junction_path`* `[-comment` *`text`*`]`

例：+ `cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1`

S3クライアントユーザを有効にします

S3クライアントユーザがNASデータにアクセスできるようにするには、S3ユーザ名を対応するNASユーザにマッピングし、バケットサービスポリシーを使用してNASデータへのアクセス権を付与する必要があります。

作業を開始する前に

クライアントアクセス用のユーザ名（Linux/UNIX、Windows、S3クライアントユーザ）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ユーザ名を対応するLinux/UNIXまたはWindowsユーザにマッピングすると、NASファイルに対する許可チェックがS3クライアントからアクセスされたときに実施されます。S3からNASへのマッピングは、単一の名前またはPOSIXの正規表現で指定できるS3ユーザ名_Pattern_、およびLinux/UNIXまたはWindowsのユーザ名_Replacement _を指定して指定します。

ネームマッピングがない場合は、デフォルトのネームマッピングが使用され、S3ユーザ名自体がUNIXユーザ名およびWindowsユーザ名として使用されます。UNIXおよびWindowsのデフォルトのユーザ名マッピングは、を使用して変更できます `vserver object-store-server modify` コマンドを実行します

ローカルのネームマッピング構成のみがサポートされます。LDAPはサポートされません。

S3ユーザをNASユーザにマッピングすると、ユーザにアクセスを許可するリソース（ディレクトリとファイル）と、ユーザがアクセスを許可された操作、または許可されなかった操作を指定する権限を付与できます。

System Manager の略

1. UNIXまたはWindowsクライアント（あるいはその両方）のローカルネームマッピングを作成します。
   a. Storage > Buckets *をクリックし、S3 / NAS対応のStorage VMを選択します。
   b. 「* Settings（設定）」を選択し、をクリックします → *ネームマッピング（*ホストユーザーおよびグループ*の下）で検索します。
   c. S3からWindows または S3からUNIX へのタイル（またはその両方）で、 Add をクリックし、目的の Pattern （**S3**）および Replacement *（NAS）ユーザ名を入力します。
2. クライアントアクセスを許可するバケットポリシーを作成します。
   a. [ストレージ**]**、**[**バケット**]**の順にクリックし、をクリックします ⋮ 目的の**S3**バケットの横にある Edit *をクリックします。
   b. [*追加（Add）]をクリックし、必要な値を入力する。
      - * Principal *- S3ユーザ名を指定するか、デフォルト（すべてのユーザ）を使用します。
      - エフェクト-「*許可」または「*拒否」を選択します。
      - アクション-これらのユーザーとリソースのアクションを入力します。オブジェクトストアサーバで現在S3 NASバケットに対してサポートされているリソース処理のセットは、GetObject、PutObject、DeleteObject、ListBucket、GetBucketAclです。 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning、ListBucketVersionsの各メソッドに対応しています。このパラメータではワイルドカードを使用できます。
      - * Resources *-アクションを許可または拒否するフォルダまたはファイルのパスを入力するか、デフォルト（バケットのルートディレクトリ）を使用します。

CLI の使用

1. UNIXまたはWindowsクライアント（あるいはその両方）のローカルネームマッピングを作成します。[+] `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` -マッピング評価の優先順位番号。1または2を入力します。
   - `-pattern` - S3ユーザ名または正規表現
   - `-replacement` - WindowsまたはUNIXのユーザ名

例+ `vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1 -replacement win_user_1 vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1 -replacement unix_user_1`

1. クライアントアクセスを許可するバケットポリシーを作成します。[+] `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` -ユーザがアクションを要求したときにアクセスを許可するか拒否するかを指定します。
   - `-action <Action>, …` -許可または拒否されるリソース操作を指定しますオブジェクトストアサーバで現在S3 NASバケットに対してサポートされているリソース処理のセットは、

GetObject、PutObject、DeleteObject、ListBucket、GetBucketAclです。 GetObjectAcl 、GetObjectTagging、PutObjectTagging、DeleteObjectTagging、GetBucketLocation、GetBucketVersioning、PutBucketVersioning、ListBucketVersionsの各メソッドに対応しています。このパラメータではワイルドカードを使用できます。

- `-principal <Objectstore Principal>, …` -オブジェクトストアサーバのユーザまたはグループに対してアクセスを要求するユーザを検証します。
  - オブジェクトストアサーバグループは、グループ名にプレフィックスグループ/を追加することによって指定します。
  - `-principal -`（ハイフン文字）は、すべてのユーザにアクセスを許可します。
- `-resource <text>, …` -許可または拒否の権限を設定するバケット、フォルダ、またはオブジェクトを指定します。このパラメータではワイルドカードを使用できます。
- `[-sid <SID>]` -オブジェクトストアサーバのバケットポリシーステートメントのオプションのテキストコメントを指定します。

例+
```
cluster1::> vserver object-store-server bucket policy add-statement
-bucket testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```