



S3 REST APIを使用する

StorageGRID 11.8

NetApp
March 19, 2024

目次

S3 REST APIを使用する	1
S3 REST APIでサポートされるバージョンと更新	1
クイックリファレンス：サポートされるS3 API要求	3
S3 REST API設定のテスト	23
StorageGRID での S3 REST API の実装	25
Amazon S3 REST APIのサポート	40
StorageGRIDのカスタム処理	89
バケットとグループのアクセスポリシー	110
監査ログで追跡される S3 処理	137

S3 REST APIを使用する

S3 REST APIでサポートされるバージョンと更新

StorageGRID は、 Representational State Transfer (REST) の Web サービスのセットとして実装される Simple Storage Service (S3) をサポートします。

S3 REST APIのサポートにより、S3 Webサービス用に開発されたサービス指向アプリケーションを、StorageGRID システムを使用するオンプレミスのオブジェクトストレージに接続できます。クライアントアプリケーションで現在S3 REST API呼び出しを使用している場合は、変更を最小限に抑える必要があります。

サポートされるバージョン

StorageGRID でサポートしている S3 および HTTP のバージョンは次のとおりです。

項目	バージョン
S3 API仕様	"Amazon Web Services (AWS) ドキュメント : 「 Amazon Simple Storage Service API Reference 」"
HTTP	1.1 HTTP の詳細については、HTTP/1.1 (RFC 7230~7235) を参照してください。 "IETF RFC 2616 : 『 Hypertext Transfer Protocol (HTTP/1.1) 』" • 注 : StorageGRID は、HTTP/1.1 パイプラインをサポートしません。

S3 REST APIのサポートが更新されました

リリース。	コメント
11.8	S3処理の名前がで使用されている名前に更新されました。 "Amazon Web Services (AWS) ドキュメント : 「 Amazon Simple Storage Service API Reference 」" 。

リリース。	コメント
11.7	<ul style="list-style-type: none"> • を追加しました "クイックリファレンス：サポートされるS3 API要求"。 • S3オブジェクトロックでのガバナンスモードの使用のサポートが追加されました。 • StorageGRID固有のサポートが追加されました <code>x-ntap-sg-cgr-replication-status</code> GET Object要求とHEAD Object要求の応答ヘッダー。このヘッダーは、グリッド間レプリケーションのオブジェクトのレプリケーションステータスを示します。 • <code>SelectObjectContent</code>要求でParquetオブジェクトがサポートされるようになりました。
11.6	<ul style="list-style-type: none"> • の使用のサポートが追加されました <code>partNumber</code> GET Object要求とHEAD Object要求のRequestパラメータ。 • S3 オブジェクトロックのデフォルト保持モードとデフォルトの保持期間がバケットレベルでサポートされるようになりました。 • のサポートが追加されました <code>s3:object-lock-remaining-retention-days</code> オブジェクトに許可される保持期間の範囲を設定するためのPolicy Conditionキー。 • 単一のPUT Object処理の<code>maximum_recommended_size</code>を5GiB（5、368、709、120バイト）に変更しました。5GB より大きいオブジェクトがある場合は、マルチパートアップロードを使用してください。
11.5.	<ul style="list-style-type: none"> • バケットの暗号化の管理のサポートが追加されました。 • S3 オブジェクトのロックと廃止された従来の準拠要求のサポートを追加しました。 • バージョン管理されたバケットでの <code>DELETE Multiple Objects</code> の使用のサポートが追加されました。 • <code>Content-MD5</code> 要求ヘッダーが正しくサポートされるようになりました。
11.4	<ul style="list-style-type: none"> • <code>DELETE Bucket tagging</code>、<code>GET Bucket tagging</code>、<code>PUT Bucket tagging</code> のサポートが追加されました。コスト割り当てタグはサポートされていません。 • StorageGRID 11.4 で作成されたバケットでは、オブジェクトキー名がパフォーマンスのベストプラクティスに適合するように制限する必要はなくなりました。 • でバケット通知のサポートが追加されました <code>s3:ObjectRestore:Post</code> イベントタイプ。 • マルチパートのAWS サイズの上限が適用されるようになりました。マルチパートアップロードの各パートのサイズは5MiB から5GiB の間にする必要があります。最後の部分は5MiB より小さくすることができます。 • TLS 1.3のサポートが追加されました

リリース。	コメント
11.3	<ul style="list-style-type: none"> • ユーザ指定のキーによるオブジェクトデータのサーバ側暗号化（SSE-C）がサポートされるようになりました。 • DELETE Bucket lifecycle、GET Bucket lifecycle、PUT Bucket lifecycleの各処理（Expirationアクションのみ）とがサポートされるようになりました x-amz-expiration 応答ヘッダー。 • PUT Object、PUT Object - Copy、Multipart Upload が更新されて、取り込み時に同期配置を使用する ILM ルールの影響を受けるようになりました。 • TLS 1.1 暗号はサポートされなくなりました。
11.2.	<p>クラウドストレージプールで POST Object restore を使用できるようになりました。グループポリシーとバケットポリシーの ARN、ポリシー条件キー、およびポリシー変数で AWS 構文を使用できるようになりました。StorageGRID 構文を使用する既存のグループポリシーとバケットポリシーは引き続きサポートされます。</p> <ul style="list-style-type: none"> • 注：カスタム StorageGRID 機能で使用される ARN やその他の構成 JSON / XML の使用に変更はありませんでした。
11.1.	Cross-Origin Resource Sharing（CORS）、グリッドノードへのS3クライアント接続でのHTTP、バケットでの準拠設定のサポートが追加されました。
11.0	バケットでのプラットフォームサービス（CloudMirror レプリケーション、通知、および Elasticsearch 検索統合）の設定がサポートされるようになりました。また、バケットに対するオブジェクトタギングの場所の制約と「available」の整合性がサポートされるようになりました。
10.4	ILM スキャンのバージョン管理、エンドポイントドメインの名前ページの更新、ポリシーの条件と変数、ポリシーの例、および PutOverwriteObject 権限の変更のサポートが追加されました。
10.3	バージョン管理のサポートが追加されました。
10.2	グループとバケットのアクセスポリシー、およびマルチパートコピー（Upload Part - Copy）のサポートが追加されました。
10.1	マルチパートアップロード、仮想ホスト形式の要求、および v4 認証のサポートが追加されました。
10.0	StorageGRID システムで S3 REST API のサポートが初めて導入されました。現在サポートされているバージョンの _Simple Storage Service API Reference_ is 2006-03-01 。

クイックリファレンス：サポートされる**S3 API**要求

このページでは、StorageGRID がAmazon Simple Storage Service（S3）APIをどのよう

にサポートしているかをまとめます。

このページには、StorageGRID でサポートされるS3処理のみが含まれています。



各処理のAWSドキュメントを参照するには、見出しのリンクを選択します。

一般的なURIクエリパラメータと要求ヘッダー

特に記載がない限り、次の一般的なURIクエリパラメータがサポートされます。

- versionId (オブジェクトの処理に必要な場合)

特に記載がないかぎり、次の一般的な要求ヘッダーがサポートされます。

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

関連情報

- ["S3 REST APIの実装の詳細"](#)
- ["Amazon Simple Storage Service API Reference : Common Request Headers"](#)

"AbortMultipartUpload の略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを指定します。

- uploadId

本文を要求します

なし

StorageGRID のドキュメント

["マルチパートアップロードの処理"](#)

"CompleteMultipartUpload"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを指定します。

- uploadId

本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- CompleteMultipartUpload
- ETag
- Part
- PartNumber

StorageGRID のドキュメント

["CompleteMultipartUpload"](#)

"CopyObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-<metadata-name>

本文を要求します

なし

StorageGRID のドキュメント

"CopyObject"

"CreateBucketを選択します"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- x-amz-bucket-object-lock-enabled

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"バケットの処理"

"CreateMultipartUpload を実行します"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

本文を要求します

なし

StorageGRID のドキュメント

["CreateMultipartUpload を実行します"](#)

"DeleteBucketの場合"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

StorageGRID のドキュメント

["バケットの処理"](#)

"DeleteBucketCors"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"DeleteBucketEncryption"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"DeleteBucketLifecycle"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

- ["バケットの処理"](#)
- ["S3 ライフサイクル設定を作成する"](#)

"DeleteBucketPolicyのようになります"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

["バケットの処理"](#)

"DeleteBucketReplication"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

["バケットの処理"](#)

"DeleteBucketTagging"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

["バケットの処理"](#)

"deleteObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求と追加の要求ヘッダー：

- x-amz-bypass-governance-retention

本文を要求します
なし

StorageGRID のドキュメント

"オブジェクトの処理"

"オブジェクトを削除します"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求と追加の要求ヘッダー：

- x-amz-bypass-governance-retention

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"オブジェクトの処理"

"DeleteObjectTagging の場合"

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

"オブジェクトの処理"

"GetBucketAcl"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

"バケットの処理"

"GetBucketCors"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します
なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketEncryptionの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketLifecycleConfiguration"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

- ["バケットの処理"](#)
- ["S3 ライフサイクル設定を作成する"](#)

"GetBucketLocation"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketNotificationConfigurationを参照してください"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketPolicyのようになります"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketReplicationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketTagging"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetBucketVersioningの各ノードの設定"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"GetObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを使用します。

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

追加の要求ヘッダーは次のとおりです。

- Range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

本文を要求します

なし

StorageGRID のドキュメント

["GetObject"](#)

"GetObjectAcl"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["オブジェクトの処理"](#)

"GetObjectLegalHold"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"GetObjectLockConfigurationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"GetObjectRetentionの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"GetObjectTagging の 2 つの機能を"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["オブジェクトの処理"](#)

"ヘッドバケット"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"HeadObject (ヘッドオブジェクト) "

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

本文を要求します

なし

StorageGRID のドキュメント

["HeadObject \(ヘッドオブジェクト\) "](#)

"ListBuckets"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

なし

StorageGRID のドキュメント

["サービス> ListBucketsの操作"](#)

"ListMultipartUploads"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

本文を要求します

なし

StorageGRID のドキュメント

["ListMultipartUploads"](#)

"ListObjects"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- marker
- max-keys
- prefix

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"ListObjectsV2"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- continuation-token

- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"ListObjectVersions"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

本文を要求します

なし

StorageGRID のドキュメント

["バケットの処理"](#)

"ListParts"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次の追加パラメータが含まれます。

- max-parts
- part-number-marker
- uploadId

本文を要求します

なし

StorageGRID のドキュメント

["ListMultipartUploads"](#)

"PutBucketCorsの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

["バケットの処理"](#)

"PutBucketEncryptionの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID のドキュメント

["バケットの処理"](#)

"PutBucketLifecycleConfigurationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker

- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

StorageGRID のドキュメント

- ["バケットの処理"](#)
- ["S3 ライフサイクル設定を作成する"](#)

"PutBucketNotificationConfigurationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文XMLタグを要求します

StorageGRID は、次の要求本文XMLタグをサポートしています。

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

StorageGRID のドキュメント

["バケットの処理"](#)

"PutBucketPolicyのように指定します"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされているJSON本文フィールドの詳細については、[を参照してください "バケットとグループのアクセスポリシーを使用"](#)。

"PutBucketReplicationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文XMLタグを要求します

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

StorageGRID のドキュメント

["バケットの処理"](#)

"PutBucketTaggingの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

["バケットの処理"](#)

"PutBucketVersioning"の各ノードの設定"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文パラメータを要求します

StorageGRID は、次の要求本文パラメータをサポートしています。

- VersioningConfiguration
- Status

StorageGRID のドキュメント

["バケットの処理"](#)

"PutObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加え、次のヘッダーが追加されています。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

本文を要求します

- オブジェクトのバイナリデータ

StorageGRID のドキュメント

["PutObject"](#)

"PutObjectLegalHold"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"PutObjectLockConfigurationの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"PutObjectRetentionの略"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求とこの追加ヘッダー：

- `x-amz-bypass-governance-retention`

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

"PutObjectTagging の 2 つのグループが"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

StorageGRID は、実装時にAmazon S3 REST APIで定義されたすべての要求本文パラメータをサポートします。

StorageGRID のドキュメント

"オブジェクトの処理"

"RestoreObject"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされている本文フィールドの詳細については、[を参照してください](#)。 "RestoreObject"。

"SelectObjectContent の順に選択します"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求のために。

本文を要求します

サポートされている本文フィールドの詳細については、[以下を参照してください](#)。

- ["S3 Select を使用する"](#)
- ["SelectObjectContent の順に選択します"](#)

"UploadPart のアップロード"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを使用します。

- partNumber
- uploadId

追加の要求ヘッダーは次のとおりです。

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5

本文を要求します

- 部品のバイナリデータ

StorageGRID のドキュメント

["UploadPart のアップロード"](#)

"UploadPartCopyをクリックします"

URIクエリパラメータと要求ヘッダー

StorageGRID はすべてをサポートします [共通のパラメータとヘッダー](#) この要求に加えて、次の追加のURIクエリパラメータを使用します。

- partNumber
- uploadId

追加の要求ヘッダーは次のとおりです。

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

本文を要求します

なし

StorageGRID のドキュメント

["UploadPartCopyをクリックします"](#)

S3 REST API設定のテスト

Amazon Web Servicesコマンドラインインターフェイス (AWS CLI) を使用して、システムへの接続をテストし、オブジェクトの読み取りと書き込みが可能であることを確認できます。

作業を開始する前に

- AWS CLI をからダウンロードしてインストールしておきます ["aws.amazon.com/cli"](#)。
- 必要に応じて、["ロードバランサエンドポイントを作成しました"](#)。それ以外の場合は、接続するストレージノードのIPアドレスと使用するポート番号がわかっている必要があります。を参照してください ["クライアント接続用のIPアドレスとポート"](#)。
- これで完了です ["S3テナントアカウントが作成されました"](#)。
- テナントにサインインし、["アクセスキーの作成"](#)。

これらの手順の詳細については、を参照してください ["クライアント接続を設定します"](#)。

手順

1. StorageGRID システムで作成したアカウントを使用するようにAWS CLIを設定します。
 - a. コンフィギュレーションモードを開始します。 `aws configure`
 - b. 作成したアカウントのアクセスキーIDを入力します。
 - c. 作成したアカウントのシークレットアクセスキーを入力します。
 - d. 使用するデフォルトのリージョンを入力します。例： `us-east-1`。
 - e. 使用するデフォルトの出力形式を入力するか、 `* Enter *` キーを押して `JSON` を選択します。
2. バケットを作成する。

この例では、IPアドレス10.96.101.17とポート10443を使用するようにロードバランサエンドポイントが設定されていると想定しています。

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

バケットの作成が完了すると、次の例のようにバケットの場所が返されます。

```
"Location": "/testbucket"
```

3. オブジェクトをアップロードします。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

オブジェクトのアップロードが完了すると、オブジェクトデータのハッシュである `Etag` が返されます。

4. バケットの内容をリストして、オブジェクトがアップロードされたことを確認します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. オブジェクトを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. バケットを削除します。

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

StorageGRID での S3 REST API の実装

競合するクライアント要求です

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。

「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

整合性の値

整合性では、オブジェクトの可用性と、異なるストレージノードおよびサイト間でのオブジェクトの整合性のバランスが維持されます。アプリケーションの必要に応じて整合性を変更できます。

StorageGRID では、デフォルトで、新しく作成したオブジェクトのリードアフターライト整合性が保証されます。正常に完了した PUT に続く GET では、新しく書き込まれたデータを読み取ることができます。既存のオブジェクトの上書き、メタデータの更新、および削除の整合性レベルは、結果整合性です。上書きは通常、数秒から数分で反映されますが、最大で 15 日かかることがあります。

別の整合性でオブジェクトの処理を実行する場合は、次の操作を実行できます。

- 整合性の指定 [各バケット](#)。
- 整合性の指定 [各API処理](#)。
- 次のいずれかのタスクを実行して、グリッド全体のデフォルトの整合性を変更します。
 - Grid Managerで、**[設定]>*>[ストレージ設定]>[デフォルトの整合性]***の順に選択します。
 - 。



グリッド全体の整合性に対する変更は、設定の変更後に作成されたバケットにのみ適用されます。変更の詳細を確認するには、次の場所にある監査ログを参照してください。
`/var/local/log (* consistencyLevel *を検索)。`

整合性の値

整合性は、StorageGRIDがオブジェクトの追跡に使用するメタデータがノード間でどのように分散されるかに影響し、その結果、クライアント要求に対するオブジェクトの可用性にも影響します。

バケットまたはAPI処理の整合性は、次のいずれかの値に設定できます。

- `* all *`：すべてのノードがすぐにデータを受信しないと、要求は失敗します。

- *** strong-global *** : すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
- ***strong-site *** : サイト内のすべてのクライアント要求に対してリードアフターライト整合性が保証されま
す。
- *** Read-after-new-write *** : (デフォルト) 新規オブジェクトにはリードアフターライト整合性を提供し、
オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほ
とんどの場合に推奨されます。
- *** available *** : 新しいオブジェクトとオブジェクトの更新の両方について、結果整合性を提供します。S3
バケットの場合は、必要な場合にのみ使用します (読み取り頻度の低いログ値を含むバケットや、存在し
ないキーに対するHEAD処理やGET処理など)。S3 FabricPool バケットではサポートされません。

「Read-after-new-write」整合性と「available」整合性を使用

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されている場合、StorageGRIDは次のよ
うに複数の手順で検索を実行します。

- まず、低い整合性レベルを使用してオブジェクトを検索します。
- そのルックアップが失敗すると、次の整合性値でルックアップが繰り返され、strong-globalの動作と同等
の整合性が得られるようになります。

HEAD処理またはGET処理で「Read-after-new-write」整合性が使用されているが、オブジェクトが存在しな
い場合、オブジェクト検索の整合性は常にstrong-globalの動作と同じになります。この整合性のためには、オ
ブジェクトメタデータのコピーが各サイトで複数ある必要があるため、同じサイトで使用できないストレージ
ノードが複数ある場合に「500 Internal Server Error」が大量に発生する可能性があります。

Amazon S3と同様の整合性の保証が必要ないかぎり、整合性を「available」に設定することで、HEAD処理
とGET処理でのこれらのエラーを回避できます。HEAD処理またはGET処理で「available」整合性が使用さ
れている場合、StorageGRIDでは結果整合性のみが提供されます。整合性が向上しても失敗した処理が再試
行されることはないため、オブジェクトメタデータのコピーが複数ある必要はありません。

[api-operation-consistency-control]] API処理の整合性を指定します。

個々のAPI処理に対して整合性を設定するには、処理でサポートされている整合性の値を要求ヘッダーで指
定する必要があります。この例では、GetObject処理の整合性を「strong-site」に設定しています。

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



PutObject処理とGetObject処理では、同じ整合性を使用する必要があります。

バケットの整合性を指定する

バケットの整合性を設定するには、StorageGRID "PUT Bucket consistency" リクエスト。または "[バケットの整合性を変更する](#)" Tenant Managerから削除します。

バケットに整合性を設定する場合は、次の点に注意してください。

- バケットに整合性を設定することで、バケット内のオブジェクトまたはバケット設定に対して実行されるS3処理に使用する整合性が決まります。バケット自体に対する処理には影響しません。
- 個々のAPI処理の整合性がバケットの整合性よりも優先されます。
- 通常、バケットではデフォルト整合性の「Read-after-new-write」を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

整合性とILMルールの相互作用によるデータ保護への影響

選択した整合性とILMルールは、どちらもオブジェクトの保護方法に影響します。これらの設定は対話的に操作できます。

たとえば、オブジェクトの格納時に使用される整合性はオブジェクトメタデータの初期配置に影響し、ILMルールで選択された取り込み動作はオブジェクトコピーの初期配置に影響します。StorageGRIDでは、クライアント要求に対応するためにオブジェクトのメタデータとそのデータの両方にアクセスするため、整合性と取り込み動作で同じ保護レベルを選択すると、初期データ保護が向上し、システム応答の予測性が向上します。

次のようになります **"取り込みオプション"** ILMルールで使用できます。

デュアルコミット

StorageGRIDはオブジェクトの中間コピーをただちに作成し、クライアントに成功を返します。可能な場合は、ILMルールで指定されたコピーが作成されます。

strict

クライアントに成功が返される前に、ILMルールで指定されたすべてのコピーが作成されている必要があります。

中間 (Balanced)

StorageGRIDは、取り込み時にILMルールで指定されたすべてのコピーの作成を試みます。作成できない場合は中間コピーが作成され、クライアントに成功が返されます。可能な場合は、ILMルールで指定されたコピーが作成されます。

整合性とILMルールの相互作用の例

2サイトのグリッドで次のILMルールと整合性が設定されているとします。

- * ILM ルール * : ローカルサイトとリモートサイトに1つずつ、2つのオブジェクトコピーを作成します。取り込み動作はStrictを使用します。
- * consistency * : strong-global (オブジェクトメタデータがすべてのサイトに即座に分散されます)。

クライアントがオブジェクトをグリッドに格納すると、StorageGRIDは両方のオブジェクトをコピーし、両方のサイトにメタデータを分散してからクライアントに成功を返します。

オブジェクトは、取り込みが成功したことを示すメッセージが表示された時点で損失から完全に保護されます。たとえば、取り込み直後にローカルサイトが失われた場合、オブジェクトデータとオブジェクトメタデータの両方のコピーがリモートサイトに残っています。オブジェクトを完全に読み出し可能にしている。

同じILMルールでstrong-site整合性を使用した場合、オブジェクトデータがリモートサイトにレプリケートされたあと、オブジェクトメタデータが分散される前にクライアントに成功メッセージが返されることがあります。この場合、オブジェクトメタデータの保護レベルがオブジェクトデータの保護レベルと一致しません。取り込み直後にローカルサイトが失われると、オブジェクトメタデータが失われます。オブジェクトを取得できません。

整合性ルールとILMルールの関係は複雑になる可能性があります。サポートが必要な場合は、NetAppにお問い合わせください。

オブジェクトのバージョン管理

各オブジェクトの複数のバージョンを保持する場合は、バケットのバージョン管理状態を設定できます。バケットのバージョン管理を有効にすると、オブジェクトが誤って削除されないように保護したり、以前のバージョンのオブジェクトを読み出してリストアしたりできます。

StorageGRID システムでは、バージョン管理のほとんどの機能をサポートしていますが、いくつかの制限事項があります。StorageGRID では、オブジェクトごとに最大 1、000 個のバージョンをサポートしていません。

オブジェクトのバージョン管理は、StorageGRID の情報ライフサイクル管理 (ILM) または S3 バケットのライフサイクル設定と組み合わせることができます。バージョン管理はバケットごとに明示的に有効にする必要があります。バケットでバージョン管理を有効にすると、バケットに追加される各オブジェクトにバージョンIDが割り当てられ、このIDがStorageGRIDシステムによって生成されます。

MFA (多要素認証) Delete の使用はサポートされていません。



バージョン管理は、StorageGRID バージョン 10.3 以降で作成されたバケットでのみ有効にすることができます。

ILM とバージョン管理

ILM ポリシーはオブジェクトの各バージョンに適用されます。ILM のスキャン処理では、すべてのオブジェクトが継続的にスキャンされ、現在の ILM ポリシーに照らして再評価されます。ILM ポリシーに対する変更は、それまでに取り込まれたすべてのオブジェクトに適用されます。バージョン管理が有効になっている場合は、それまでに取り込まれたバージョンも対象にILM のスキャン処理により、過去に取り込まれたオブジェクトに変更後の新しい ILM の内容が適用さ

バージョン管理が有効なバケット内のS3オブジェクトについては、バージョン管理のサポートにより、参照時間に「noncurrent time」を使用するILMルールを作成できます (質問、「Apply this rule to older object versions only?」に対して* Yes *を選択します)。イン "[ILMルール作成ウィザードのステップ1](#)")。オブジェクトが更新されると、それまでのバージョンは noncurrent になります。「noncurrent time」フィルタを使用すると、以前のバージョンのオブジェクトによるストレージへの影響を軽減するポリシーを作成できます。



マルチパートアップロード処理を使用してオブジェクトの新しいバージョンをアップロードすると、オブジェクトの元のバージョンの noncurrent の時間には、マルチパートアップロードの完了時ではなく、新しいバージョンのマルチパートアップロードが作成された時点が反映されます。ただし、オリジナルバージョンの最新でない時間は、現行バージョンの時間よりも数時間 ~ 数日早い場合があります。

関連情報

- "S3 バージョン管理オブジェクトの削除方法"
- "S3 バージョン管理オブジェクトの ILM ルールとポリシー (例 4) "。

S3 REST APIを使用してS3オブジェクトロックを設定します

StorageGRID システムでS3オブジェクトロックのグローバル設定が有効になっている場合は、S3オブジェクトロックを有効にしてバケットを作成できます。デフォルトの保持設定はバケットごとに指定することも、オブジェクトバージョンごとに指定することもできます。

バケットでS3オブジェクトロックを有効にする方法

StorageGRID システムでグローバルな S3 オブジェクトのロック設定が有効になっている場合は、各バケットの作成時に S3 オブジェクトのロックを必要に応じて有効にすることができます。

S3オブジェクトロックは永続的な設定で、バケットの作成時にのみ有効にできます。バケットの作成後にS3オブジェクトロックを追加または無効にすることはできません。

バケットでS3オブジェクトロックを有効にするには、次のいずれかの方法を使用します。

- Tenant Manager を使用してバケットを作成します。を参照してください "[S3 バケットを作成する](#)"。
- CreateBucket要求を使用してバケットを作成します。 `x-amz-bucket-object-lock-enabled` 要求ヘッダー。を参照してください "[バケットの処理](#)"。

S3オブジェクトロックにはバケットのバージョン管理が必要です。バージョン管理はバケットの作成時に自動的に有効になります。バケットのバージョン管理を一時停止することはできません。を参照してください "[オブジェクトのバージョン管理](#)"。

バケットのデフォルトの保持設定

バケットでS3オブジェクトロックが有効になっている場合は、必要に応じてバケットのデフォルトの保持を有効にし、デフォルトの保持モードとデフォルトの保持期間を指定できます。

デフォルトの保持モード

- コンプライアンスモードの場合：
 - `retain-until-date`に達するまで、オブジェクトを削除できません。
 - オブジェクトの`retain-until-date`は増やすことはできますが、減らすことはできません。
 - オブジェクトの`retain-until-date`は、その日付に達するまで削除できません。
- ガバナンスモードの場合：
 - を使用するユーザ `s3:BypassGovernanceRetention` 権限はを使用できます `x-amz-bypass-governance-retention: true` 保持設定をバイパスする要求ヘッダー。
 - これらのユーザは、`retain-until-date`に達する前にオブジェクトバージョンを削除できます。
 - これらのユーザは、オブジェクトの`retain-until-date`を増減、または削除できます。

デフォルトの保持期間

各バケットのデフォルトの保持期間は、年または日数で指定できます。

バケットのデフォルトの保持期間を設定する方法

バケットのデフォルトの保持期間を設定するには、次のいずれかの方法を使用します。

- Tenant Managerからバケット設定を管理します。を参照してください ["S3 バケットを作成します。"](#) および ["S3オブジェクトロックのデフォルトの保持期間の更新"](#)。
- 問題デフォルトのモードとデフォルトの日数または年数を指定するための、バケットに対するPutObjectLockConfiguration要求。

PutObjectLockConfigurationの略

PutObjectLockConfiguration要求を使用すると、S3オブジェクトロックが有効になっているバケットに対して、デフォルトの保持モードとデフォルトの保持期間を設定および変更できます。以前に設定したデフォルトの保持設定を削除することもできます。

新しいオブジェクトバージョンがバケットに取り込まれると、にデフォルトの保持モードが適用されます `x-amz-object-lock-mode` および `x-amz-object-lock-retain-until-date` は指定されていません。デフォルトの保持期間は、`retain-until-date`の計算に使用されます `x-amz-object-lock-retain-until-date` が指定されていません。

オブジェクトバージョンの取り込み後にデフォルトの保持期間が変更された場合、オブジェクトバージョンの `retain-until` はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。

を用意しておく必要があります `s3:PutBucketObjectLockConfiguration` この処理を完了するための権限 (rootアカウント)。

。 `Content-MD5` PUT要求に要求ヘッダーを指定する必要があります。

要求例

この例では、バケットでS3オブジェクトロックを有効にし、デフォルトの保持モードを準拠に設定し、デフォルトの保持期間を6年に設定しています。


```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

バケットのデフォルトの保持期間を確認する方法

バケットでS3オブジェクトロックが有効になっているかどうかを確認し、デフォルトの保持モードと保持期間を確認するには、次のいずれかの方法を使用します。

- Tenant Managerでバケットを表示します。を参照してください "[S3バケットを表示します](#)"。
- 問題 `GetObjectLockConfiguration` 要求。

`GetObjectLockConfiguration`の略

`GetObjectLockConfiguration` 要求を使用すると、S3 Object Lockがバケットで有効になっているかどうかを確認できます。有効になっている場合は、バケットにデフォルトの保持モードと保持期間が設定されているかどうかを確認できます。

新しいオブジェクトバージョンがバケットに取り込まれると、にデフォルトの保持モードが適用されます `x-amz-object-lock-mode` が指定されていません。デフォルトの保持期間は、の `retain-until-date` の計算に使用されます `x-amz-object-lock-retain-until-date` が指定されていません。

を用意しておく必要があります `s3:GetBucketObjectLockConfiguration` この処理を完了するための権限 (rootアカウント)。

要求例

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

応答例

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

オブジェクトの保持設定を指定する方法

S3オブジェクトロックが有効なバケットには、S3オブジェクトロックの保持設定の有無に関係なく、オブジェクトを組み合わせて含めることができます。

オブジェクトレベルの保持設定は、S3 REST APIを使用して指定します。オブジェクトの保持設定は、バケットのデフォルトの保持設定よりも優先されます。

オブジェクトごとに次の設定を指定できます。

- 保持モード：コンプライアンスまたはガバナンスのいずれか。
- * retain-until-date *：StorageGRID がオブジェクトバージョンを保持する期間を指定する日付。
 - コンプライアンスモードでは、retain-until-dateが将来の日付の場合、オブジェクトを読み出すことは

できますが、変更や削除はできません。retain-until-dateは増やすことができますが、この日付を減らすことも削除することもできません。

- ガバナンスモードでは、特別な権限を持つユーザーは、retain-until-date設定をバイパスできます。保持期間が経過する前にオブジェクトバージョンを削除できます。また、retain-until-dateを増減したり、削除したりすることもできます。

- *リーガルホールド*：オブジェクトバージョンにリーガルホールドを適用すると、そのオブジェクトがただちにロックされます。たとえば、調査または法的紛争に関連するオブジェクトにリーガルホールドを設定する必要がある場合があります。リーガルホールドには有効期限はありませんが、明示的に削除されるまで保持されます。

オブジェクトのリーガルホールド設定は、保持モードやretain-until-dateとは関係ありません。オブジェクトのバージョンがリーガルホールドの対象になっている場合、そのバージョンは誰も削除できません。

バケットにオブジェクトバージョンを追加するときにS3オブジェクトロックの設定を指定するには、問題Aを実行します **"PutObject"**、**"CopyObject"**または **"CreateMultipartUpload を実行します"** リクエスト。

次のものを使用できます。

- `x-amz-object-lock-mode` コンプライアンスまたはガバナンス（大文字と小文字が区別されます）。



を指定する場合 x-amz-object-lock-mode、も指定する必要があります x-amz-object-lock-retain-until-date。

- x-amz-object-lock-retain-until-date
 - retain-une-dateの値は、の形式で指定する必要があります 2020-08-10T21:46:00Z。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。その他のISO 8601形式は使用できません。
 - retain-une-date は将来の日付にする必要があります。
- x-amz-object-lock-legal-legal

リーガルホールドがオン（大文字と小文字が区別される）の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドがオフの場合、リーガルホールドは適用されません。それ以外の値を指定すると、400 Bad Request（InvalidArgument）エラーが発生します。

次のいずれかの要求ヘッダーを使用する場合は、次の制限事項に注意してください。

- Content-MD5 要求ヘッダーがある場合は必須です x-amz-object-lock-* 要求ヘッダーがPutObject要求に存在します。Content-MD5 CopyObjectまたはCreateMultipartUploadには必要ありません。
- バケットでS3オブジェクトロックが有効になっていない場合は、とをクリックします x-amz-object-lock-* 要求ヘッダーが存在し、400 Bad Request（InvalidRequest）エラーが返されます。
- PutObject要求は、次の使用をサポートします。x-amz-storage-class: REDUCED_REDUNDANCY AWSの動作に合わせて調整できます。ただし、S3 オブジェクトのロックが有効になっているバケットにオブジェクトが取り込まれると、StorageGRID は常にデュアルコミットの取り込みを実行します。
- 後続のGETまたはHeadObjectバージョンの応答には、ヘッダーが含まれます。x-amz-object-lock-mode、x-amz-object-lock-retain-until-date`および `x-amz-object-lock-legal-legal` が設定されている場合、および要求の送信者が正しいかどうか `s3:Get*` 権限：

を使用できます `s3:object-lock-remaining-retention-days` オブジェクトの最小保持期間と最大保持期間を制限するポリシー条件キー。

オブジェクトの保持設定を更新する方法

既存のオブジェクトのバージョンのリーガルホールドや保持の設定を更新する必要がある場合、次のオブジェクトサブリソース処理を実行できます。

- `PutObjectLegalHold`

新しいリーガルホールドの値が `on` の場合、オブジェクトはリーガルホールドの対象になります。リーガルホールドの値が `off` の場合、リーガルホールドは解除されます。

- `PutObjectRetention`

- `mode` 値は `compliance` または `governance` です（大文字と小文字が区別されます）。
- `retain-une-date` の値は、の形式で指定する必要があります `2020-08-10T21:46:00Z`。秒数には分数を指定できますが、保持される 10 進数は 3 桁（ミリ秒単位）だけです。その他の ISO 8601 形式は使用できません。
- オブジェクトバージョンに既存の `retain-until` がある場合は、オブジェクトバージョンを増やすことはできますが、増やすことはできません。新しい値は将来の必要があります。

ガバナンスモードの使用方法

を持つユーザ `s3:BypassGovernanceRetention` 権限は、ガバナンスモードを使用するオブジェクトのアクティブな保持設定をバイパスできます。DELETE 処理または `PutObjectRetention` 処理には、`x-amz-bypass-governance-retention:true` 要求ヘッダー。これらのユーザは、次の追加操作を実行できます。

- 保持期間が経過する前にオブジェクトバージョンを削除するには、`DeleteObject` 処理または `DeleteObjects` 処理を実行します。

リーガルホールドの対象になっているオブジェクトは削除できません。リーガルホールドをオフにする必要があります。

- オブジェクトの保持期間が経過する前にオブジェクトバージョンのモードをガバナンスからコンプライアンスに変更する `PutObjectRetention` 処理を実行します。

コンプライアンスモードからガバナンスモードに変更することはできません。

- `PutObjectRetention` 処理を実行して、オブジェクトバージョンの保持期間を増減、または削除します。

関連情報

- ["S3 オブジェクトロックでオブジェクトを管理します"](#)
- ["S3 オブジェクトロックを使用してオブジェクトを保持します"](#)
- ["Amazon Simple Storage Service User Guide : Using S3 Object Lock"](#)

S3 ライフサイクル設定を作成する

S3 ライフサイクル設定を作成して、特定のオブジェクトが StorageGRID システムから

削除されるタイミングを制御できます。

このセクションの簡単な例では、S3 ライフサイクル設定で特定のオブジェクトが特定の S3 バケットから削除（期限切れ）されるタイミングを制御する方法を示します。このセクションの例は、説明のみを目的としています。S3 ライフサイクル設定の作成の詳細については、を参照してください ["Amazon Simple Storage Service ユーザーガイド：オブジェクトのライフサイクル管理"](#)。StorageGRID では、Expiration アクションのみがサポートされ、移行アクションはサポートされません。

ライフサイクル構成とは

ライフサイクル設定は、特定の S3 バケット内のオブジェクトに適用される一連のルールです。各ルールは、影響を受けるオブジェクトと、それらのオブジェクトの有効期限（特定の日付または日数後）を指定します。

StorageGRID では、1 つのライフサイクル設定で最大 1、000 個のライフサイクルルールがサポートされます。各ルールには、次の XML 要素を含めることができます。

- Expiration：指定した日付に達した場合、またはオブジェクトが取り込まれたときから指定した日数に達した場合にオブジェクトを削除します。
- NoncurrentVersionExpiration：指定した日数に達したオブジェクトを削除します。これは、オブジェクトが最新でなくなったときからです。
- フィルタ（プレフィックス、タグ）
- ステータス
- ID

各オブジェクトは、S3バケットライフサイクルまたはILMポリシーの保持設定に従います。S3バケットライフサイクルが設定されている場合は、バケットライフサイクルフィルタに一致するオブジェクトのILMポリシーがライフサイクル有効期限のアクションで上書きされます。バケットライフサイクルフィルタに一致しないオブジェクトには、ILMポリシーの保持設定が使用されます。オブジェクトがバケットライフサイクルフィルタに一致し、有効期限の操作が明示的に指定されていない場合、ILMポリシーの保持設定は使用されず、オブジェクトのバージョンが無期限に保持されることが暗黙的に示されます。を参照してください ["S3バケットライフサイクルとILMポリシーの優先度の例"](#)。

そのため、ILM ルールの配置手順がオブジェクトに引き続き適用されていても、オブジェクトがグリッドから削除されることがあります。あるいは、ILM 配置手順がすべて終了したあとも、オブジェクトがグリッドに保持される場合があります。詳細については、を参照してください ["オブジェクトのライフサイクル全体にわたる ILM の動作"](#)。



バケットライフサイクル設定は S3 オブジェクトロックが有効になっているバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

StorageGRID では、次のバケット処理を使用してライフサイクル設定を管理できます。

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfigurationの略

ライフサイクル構成を作成します

ライフサイクル設定を作成するための最初の手順として、1 つ以上のルールを含む JSON ファイルを作成します。たとえば、この JSON ファイルには次の 3 つのルールが含まれています。

1. ルール1は、プレフィックスに一致するオブジェクトにのみ適用されます。category1/とそれにはがあります key2 の値 tag2。Expiration パラメータは、フィルタに一致するオブジェクトの有効期限が2020年8月22日の午前0時に切れるように指定します。
2. ルール2は、プレフィックスに一致するオブジェクトにのみ適用されます。category2/。Expiration パラメータは、フィルタに一致するオブジェクトの取り込みから100日後に期限切れにするを指定します。



日数を指定するルールは、オブジェクトが取り込まれた時点を基準とした相対的なルールです。現在の日付が取り込み日と日数を超えている場合は、ライフサイクル設定の適用後すぐに一部のオブジェクトがバケットから削除される可能性があります。

3. ルール3は、プレフィックスに一致するオブジェクトにのみ適用されます。category3/。Expiration パラメータは、最新でないバージョンの一致オブジェクトが最新でなくなったあと50日で期限切れになるように指定します。

```

{
  "Rules": [
    {
      "ID": "rule1",
      "Filter": {
        "And": {
          "Prefix": "category1/",
          "Tags": [
            {
              "Key": "key2",
              "Value": "tag2"
            }
          ]
        }
      },
      "Expiration": {
        "Date": "2020-08-22T00:00:00Z"
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule2",
      "Filter": {
        "Prefix": "category2/"
      },
      "Expiration": {
        "Days": 100
      },
      "Status": "Enabled"
    },
    {
      "ID": "rule3",
      "Filter": {
        "Prefix": "category3/"
      },
      "NoncurrentVersionExpiration": {
        "NoncurrentDays": 50
      },
      "Status": "Enabled"
    }
  ]
}

```

バケットにライフサイクル設定を適用

ライフサイクル設定ファイルを作成したら、PutBucketLifecycleConfiguration要求を発行してバケットに適用します。

次の要求は、サンプルファイル内のライフサイクル設定を、という名前のバケット内のオブジェクトに適用します testbucket。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

ライフサイクル設定がバケットに正常に適用されたことを確認するには、GetBucketLifecycleConfiguration要求を問題します。例：

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

成功応答には、適用したライフサイクル設定が表示されます。

バケットライフサイクルの有効期限が環境 オブジェクトであることを検証します

PutObject、HeadObject、またはGetObjectのいずれか環境の要求を発行するときに、ライフサイクル設定の有効期限ルールが特定のオブジェクトであるかどうかを確認できます。ルールが適用される場合、応答にはが含まれます Expiration オブジェクトの有効期限と一致する有効期限を示すパラメータ。



バケットライフサイクルはILMよりも優先されるため、を参照してください expiry-date 表示されているのは、オブジェクトが削除される実際の日付です。詳細については、を参照してください ["オブジェクト保持期間の決定方法"](#)。

たとえば、このPutObject要求は2020年6月22日に発行され、オブジェクトを testbucket バケット。

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

成功の応答は、オブジェクトの有効期限が 100 日（2020年10月1日）に切れ、ライフサイクル設定のルール 2 に一致したことを示します。

```
{
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\"", rule-
id=\"rule2\"",
  ETag: "\"9762f8a803bc34f5340579d4446076f7\""
}
```


たとえば、次のHeadObject要求を使用して、testbucketバケット内の同じオブジェクトのメタデータを取得しました。

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

成功の応答にはオブジェクトのメタデータが含まれ、オブジェクトが 100 日で期限切れになり、ルール 2 に一致したことが示されます。

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



バージョン管理が有効なバケットの場合は、x-amz-expiration 応答ヘッダーは、現在のバージョンのオブジェクトにのみ適用されます。

S3 REST API を実装する際の推奨事項

StorageGRID で使用するために S3 REST API を実装する場合は、次の推奨事項を考慮してください。

存在しないオブジェクトに対する HEAD の推奨事項

オブジェクトが実際に存在するとは思わないパスにオブジェクトが存在するかどうかをアプリケーションが定期的にチェックする場合は、「available」を使用する必要があります。「**一貫性**」。たとえば、アプリケーションがPUTを実行する前に特定の場所に移動する場合は、「available」整合性を使用する必要があります。

そうしないと、同じサイトに複数のストレージノードが使用できない場合やリモートサイトに到達できない場合に、HEAD処理でオブジェクトが見つからないと「500 Internal Server Error」が大量に返されることがあります。

バケットごとに「available」整合性を設定するには、「**PUT Bucket consistency**」または、個々のAPI処理の要求ヘッダーで整合性を指定できます。

オブジェクトキーの推奨事項

オブジェクトキー名については、バケットが最初に作成された日時に基づいて次の推奨事項に従ってください。

StorageGRID 11.4以前で作成されたバケット

- オブジェクトキーの最初の4文字にランダムな値を使用しないでください。これは、AWS が以前に推奨していたキープレフィックスの推奨事項とは異なります。代わりに、など、ランダムではなく一意ではないプレフィックスを使用します image。
- 以前のAWSの推奨事項に従ってキープレフィックスにランダムな一意の文字を使用する場合は、オブジェクトキーの前にディレクトリ名を付けます。つまり、次の形式を使用します。

```
mybucket/mydir/f8e3-image3132.jpg
```

次の形式は使用しないでください。

```
mybucket/f8e3-image3132.jpg
```

StorageGRID 11.4以降で作成されたバケット

パフォーマンスのベストプラクティスに合わせてオブジェクトキー名を制限する必要はありません。ほとんどの場合、オブジェクトキー名の最初の4文字にはランダムな値を使用できます。



ただし、短期間ですべてのオブジェクトを継続的に削除するS3ワークロードは例外です。このユースケースのパフォーマンスへの影響を最小限に抑えるには、キー名の先頭部分を数千個のオブジェクトごとに、日付などの値を変更します。たとえば、S3クライアントが1秒あたり2、000個のオブジェクトを書き込むのが一般的で、ILMまたはバケットライフサイクルポリシーで3日後にすべてのオブジェクトが削除されるとします。パフォーマンスへの影響を最小限に抑えるには、次のようなパターンを使用してキーに名前を付けます。

```
/mybucket/mydir/yyyyymmddhhmmss-random_UUID.jpg
```

「範囲読み取り」に関する推奨事項

状況に応じて **"格納オブジェクトを圧縮するグローバルオプション"** が有効になっている場合は、S3クライアントアプリケーションで返されるバイト数の範囲を指定するGetObject処理を実行しないでください。これらの「範囲読み取り」処理は効率的ではありません。StorageGRIDでは、要求されたバイトにアクセスするためにオブジェクトの圧縮を実質的に解除する必要があるためです。非常に大きなオブジェクトから小さい範囲のバイト数を要求するGetObject処理は特に非効率的です。たとえば、50GBの圧縮オブジェクトから10MBの範囲を読み取る処理は非効率的です。

圧縮オブジェクトから範囲を読み取ると、クライアント要求がタイムアウトする可能性があります。



オブジェクトを圧縮する必要があり、クライアントアプリケーションが範囲読み取りを使用する必要がある場合は、アプリケーションの読み取りタイムアウトを増やしてください。

Amazon S3 REST APIのサポート

S3 REST APIの実装の詳細

StorageGRID システムは Simple Storage Service API (API バージョン 2006-03-01) を実装しており、ほとんどの処理をサポートしていますが、いくつかの制限事項があります。S3 REST API クライアントアプリケーションを統合するときは、実装の詳細を理解しておく必要があります。

StorageGRID システムでは、仮想ホスト形式の要求とパス形式の要求の両方がサポートされます。

日付の処理

S3 REST API の StorageGRID 実装では、有効な HTTP の日付形式のみをサポートしています。

StorageGRID システムでは、日付の値を設定できるすべてのヘッダーで、有効な HTTP の日付形式のみがサポートされます。日付の時刻の部分は、Greenwich Mean Time (GMT ; グリニッジ標準時) の形式で指定するか、タイムゾーンのオフセットなし (+0000 を指定) の Universal Coordinated Time (UTC ; 協定世界時) の形式で指定できます。を指定する場合は x-amz-date 要求のヘッダー。Date要求ヘッダーで指定された値を上書きします。AWS署名バージョン4を使用している場合は、を参照してください x-amz-date 日付ヘッダーがサポートされていないため、署名済み要求にヘッダーが含まれている必要があります。

代表的な要求ヘッダー

StorageGRID システムは、で定義されている共通の要求ヘッダーをサポートします "[Amazon Simple Storage Service API Reference : Common Request Headers](#)"1 つの例外を除いて。

要求ヘッダー	実装
承認	AWS 署名バージョン 2 は完全にサポートされます AWS 署名バージョン 4 は次の例外を除いてサポートされます。 <ul style="list-style-type: none">• 要求の本文の SHA256 の値は計算されません。ユーザが送信した値は、値の場合と同様に、検証なしで受け入れられます UNSIGNED-PAYLOAD は用に提供されていた x-amz-content-sha256 ヘッダー。
x-amz-security-token を指定します	実装されていませんを返します XNotImplemented。

共通の応答ヘッダー

StorageGRID システムでは、以下の例外を除き、_Simple Storage Service API Reference_で 定義されている共通の応答ヘッダーがすべてサポートされます。

応答ヘッダー	実装
x-amz-id-2	使用されません

要求を認証します

StorageGRID システムでは、 S3 API を使用したオブジェクトへのアクセスについて、認証アクセスと匿名アクセスの両方をサポートしています。

S3 API では、 S3 API 要求の認証で署名バージョン 2 と署名バージョン 4 がサポートされます。

認証された要求は、アクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。

StorageGRID システムでは、HTTPという2つの認証方式がサポートされています Authorization ヘッダーを使用し、クエリパラメータを使用する。

HTTP Authorization ヘッダーを使用します

HTTP Authorization ヘッダーは、バケットポリシーで許可された匿名の要求を除き、すべてのS3 API処理で使用されます。。 Authorization ヘッダーには、要求の認証に必要なすべての署名情報が含まれています。

クエリパラメータを使用します

クエリパラメータを使用すると、URL に認証情報を追加できます。これは署名付き URL と呼ばれ、特定のリソースへの一時的なアクセスを許可する場合に使用できます。指定されたURLを持つユーザは、リソースにアクセスする際にシークレットアクセスキーを知っている必要はありません。これにより、リソースへのサードパーティの制限付きアクセスを提供できます。

サービスの処理

StorageGRID システムでは、サービスに対して次の処理をサポートしています。

操作	実装
ListBuckets (以前の名前はGET Service)	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
GET Storage Usage の略	StorageGRID "GET Storage Usage の略" [Request]には、アカウントで使用されているストレージの合計容量と、アカウントに関連付けられている各バケットについての情報が表示されます。これは、パス/とカスタムクエリパラメータを使用したサービスに対する処理です (?x-ntap-sg-usage)が追加されました
オプション /	クライアントアプリケーションは問題を 実行できます OPTIONS / S3 認証クレデンシャルを入力せずにストレージノード上のS3ポートに要求し、ストレージノードが使用可能かどうかを確認します。この要求は監視に使用できるほか、外部のロードバランサがストレージノードの停止を特定する目的でも使用できます。

バケットの処理

StorageGRID システムでは、 S3 テナントアカウントあたり最大 1、000 個のバケットがサポートされます。

バケット名にはAWS US Standardリージョンの制限事項が適用されますが、S3仮想ホスト形式の要求をサポートするためにDNSの命名規則にも制限する必要があります。

詳細については、次を参照してください。

- "Amazon Simple Storage Serviceユーザガイド：『Bucket Restrictions and Limitations』"
- "S3エンドポイントのドメイン名を設定"

ListObjects (GET Bucket) 処理とListObjectVersions (GET Bucketオブジェクトバージョン) 処理でStorageGRIDがサポートされるようになりました。 "整合性の値"。

最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認することができます。を参照してください ["GET Bucket last access time の場合"](#)。

次の表に、StorageGRID での S3 REST API バケット処理の実装方法を示します。これらの処理を実行するには、アカウントに必要なアクセスクレデンシャルが付与されている必要があります。

操作	実装
CreateBucketを選択します	<p>新しいバケットを作成します。バケットを作成すると、そのバケットの所有者になります。</p> <ul style="list-style-type: none"> • バケット名は次のルールを満たす必要があります。 <ul style="list-style-type: none"> ◦ StorageGRID システム全体で（テナントアカウント内だけでなく）一意である必要があります。 ◦ DNS に準拠している必要があります。 ◦ 3 文字以上 63 文字以下にする必要があります。 ◦ 1 つ以上のラベルを連続して指定できます。隣接するラベルはピリオドで区切ります。各ラベルの先頭と末尾の文字は小文字のアルファベットか数字にする必要があります、使用できる文字は小文字のアルファベット、数字、ハイフンのみです。 ◦ テキスト形式の IP アドレスのようにはできません。 ◦ 仮想ホスト形式の要求でピリオドを使用しないでください。ピリオドを使用すると、サーバワイルドカード証明書の検証で原因の問題が発生します。 • デフォルトでは、バケットは作成されます us-east-1 リージョン。ただし、を使用することはできません LocationConstraint 別のリージョンを指定するように要求本文内の要求要素。を使用する場合 LocationConstraint 要素：Grid Managerまたはグリッド管理APIを使用して定義されているリージョンの正確な名前を指定する必要があります。使用するリージョン名がわからない場合は、システム管理者にお問い合わせください。 <p>注：CreateBucket要求がStorageGRIDで定義されていないリージョンを使用すると、エラーが発生します。</p> <ul style="list-style-type: none"> • を含めることができます x-amz-bucket-object-lock-enabled S3オブジェクトのロックを有効にしてバケットを作成する要求ヘッダー。を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します"。 <p>バケットの作成時に S3 オブジェクトのロックを有効にする必要があります。バケットの作成後にS3オブジェクトロックを追加または無効にすることはできません。S3 オブジェクトロックにはバケットのバージョン管理が必要です。バケットの作成時に自動的に有効になります。</p>
DeleteBucketの場合	バケットを削除します。
DeleteBucketCors	バケットのCORS設定を削除します。

操作	実装
DeleteBucketEncryption	バケットからデフォルトの暗号化を削除します。既存の暗号化オブジェクトは暗号化されたままですが、バケットに追加された新しいオブジェクトは暗号化されません。
DeleteBucketLifecycle	バケットからライフサイクル設定を削除します。を参照してください "S3 ライフサイクル設定を作成する" 。
DeleteBucketPolicyのようになります	バケットに関連付けられているポリシーを削除します。
DeleteBucketReplication	バケットに関連付けられているレプリケーション設定を削除します。
DeleteBucketTagging	<p>を使用します tagging サブリソース：バケットからすべてのタグを削除します。</p> <p>注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、NTAP-SG-ILM-BUCKET-TAG 値が割り当てられたバケットタグ。DeleteBucketTagging要求がある場合は問題を実行しない NTAP-SG-ILM-BUCKET-TAG バケットタグ。代わりに、問題でPutBucketTagging要求を実行し、NTAP-SG-ILM-BUCKET-TAG 他のすべてのタグをバケットから削除するには、タグとその割り当て値を使用します。を変更または削除しないでください。NTAP-SG-ILM-BUCKET-TAG バケットタグ。</p>
GetBucketAcl	バケットの所有者にバケットへのフルアクセスがあることを示す応答が返され、所有者のID、表示名、および権限が表示されます。
GetBucketCors	を返します。 cors バケットの設定。
GetBucketEncryptionの略	バケットのデフォルトの暗号化設定を返します。
GetBucketLifecycleConfiguration (以前のGET Bucket lifecycle)	バケットのライフサイクル設定を返します。を参照してください "S3 ライフサイクル設定を作成する" 。
GetBucketLocation	を使用して設定されたリージョンを返します。 LocationConstraint CreateBucket要求の要素。バケットのリージョンがの場合 `us-east-1`を指定すると、リージョンに対して空の文字列が返されます。
GetBucketNotificationConfigurationを参照してください (以前の名前のGET Bucket notification)	バケットに関連付けられている通知設定を返します。

操作	実装
GetBucketPolicyのように なります	バケットに関連付けられているポリシーを返します。
GetBucketReplicationの略	バケットに関連付けられているレプリケーション設定を返します。
GetBucketTagging	<p>を使用します tagging サブリソース：バケットのすべてのタグを返す</p> <p>注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、NTAP-SG-ILM-BUCKET-TAG 値が割り当てられたバケットタグ。このタグを変更または削除しないでください。</p>
GetBucketVersioningの各 ノードの設定	<p>この実装ではを使用します versioning サブリソース：バケットのバージョン管理の状態を返します。</p> <ul style="list-style-type: none"> • <i>blank</i>：バージョン管理が一度も有効になっていない（バケットは「バージョン管理されていない」） • 有効：バージョン管理が有効になっています • 中断：バージョン管理は以前有効になっていて、中断されています
GetObjectLockConfigurati onの略	<p>バケットのデフォルトの保持モードとデフォルトの保持期間（設定されている場合）を返します。</p> <p>を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します"。</p>
ヘッドバケット	<p>バケットが存在し、そのバケットにアクセスする権限があるかどうかを確認します。</p> <p>この処理から返される情報は次の</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>：バケットのUUID（UUID形式）。 • <code>x-ntap-sg-trace-id</code>：関連付けられた要求の一意的トレースID。

操作	実装
<p>listObjectsおよびListObjectsV2</p> <p>(以前の名前はGET Bucket)</p>	<p>バケット内のオブジェクトの一部またはすべて (最大1,000) を返します。を使用してオブジェクトを取り込んだ場合でも、オブジェクトのストレージクラスには2つの値が設定されます REDUCED_REDUNDANCY ストレージクラスのオプション:</p> <ul style="list-style-type: none"> ・`STANDARD`を指定します。このオブジェクトは、ストレージノードで構成されるストレージプールに格納されます。 ・`GLACIER`を指定します。このオブジェクトは、クラウドストレージプールで指定された外部バケットに移動されています。 <p>バケットに同じプレフィックスを持つ削除済みキーが多数含まれている場合、応答に一部のキーが含まれることがあります CommonPrefixes 鍵が入っていないものです</p>
<p>ListObjectVersions</p> <p>(以前のGET Bucket Object versions)</p>	<p>バケットに対する読み取りアクセスが許可されている場合、versions サブリソースには、バケット内のオブジェクトのすべてのバージョンのメタデータが表示されます。</p>
<p>PutBucketCorsの略</p>	<p>クロスオリジン要求を処理できるように、バケットのCORS設定を設定します。Cross-Origin Resource Sharing (CORS) は、あるドメインのクライアント Web アプリケーションが別のドメインのリソースにアクセスできるようにするセキュリティ機能です。たとえば、というS3バケットを使用するとします images グラフィックを保存します。のCORS設定を指定します images バケットを使用すると、そのバケット内の画像をWebサイトに表示できます http://www.example.com</p>
<p>PutBucketEncryptionの略</p>	<p>既存のバケットのデフォルトの暗号化状態を設定します。バケットレベルの暗号化が有効な場合は、バケットに追加されたすべての新しいオブジェクトが暗号化されます。StorageGRID では、StorageGRID で管理されるキーによるサーバ側の暗号化がサポートされます。サーバ側の暗号化設定ルールを指定する場合は、を設定します SSEAlgorithm パラメータの値 AES256`を使用しないでください `KMSMasterKeyID` パラメータ</p> <p>バケットのデフォルトの暗号化設定は、オブジェクトのアップロード要求ですすでに暗号化が指定されている場合 (要求にが含まれている場合) は無視されます x-amz-server-side-encryption-* 要求ヘッダー)。</p>

操作	実装
PutBucketLifecycleConfigurationの略 (以前のPUT Bucket lifecycle)	<p>バケットの新しいライフサイクル設定を作成するか、既存のライフサイクル設定と置き換えます。StorageGRID では、1つのライフサイクル設定で最大1、000個のライフサイクルルールがサポートされます。各ルールには、次のXML要素を含めることができます。</p> <ul style="list-style-type: none"> • 有効期限 (日数、日付、ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions、NoncurrentDays) • フィルタ (プレフィックス、タグ) • ステータス • ID <p>StorageGRID では、次のアクションはサポートされません。</p> <ul style="list-style-type: none"> • AbortIncompleteMultipartUpload の略 • 移行 <p>を参照してください "S3 ライフサイクル設定を作成する"。バケットライフサイクルのExpirationアクションとILMの配置手順の相互作用については、を参照してください "オブジェクトのライフサイクル全体にわたる ILM の動作"。</p> <ul style="list-style-type: none"> • 注：バケットライフサイクル設定は S3 オブジェクトロックが有効なバケットで使用できますが、従来の準拠バケットではバケットライフサイクル設定がサポートされません。

操作	実装
<p>PutBucketNotificationConfigurationの略</p> <p>(以前の名前のPUT Bucket通知)</p>	<p>要求の本文に含まれる通知設定XMLを使用してバケットの通知を設定します。実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> • StorageGRIDでは、Amazon Simple Notification Service (Amazon SNS) またはKafkaトピックがデスティネーションとしてサポートされます。Simple Queue Service (SQS) またはAmazon Lambdaエンドポイントはサポートされていません。 • 通知のデスティネーションは、StorageGRID エンドポイントの URN として指定する必要があります。エンドポイントは、Tenant Manager またはテナント管理 API を使用して作成できます。 <p>通知設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、400 Bad Request エラーがコードとともに返されます InvalidArgument。</p> <ul style="list-style-type: none"> • 次のイベントタイプに対して通知を設定することはできません。これらのイベントタイプは * サポートされていません。 <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • StorageGRID から送信されるイベント通知は標準のJSON形式を使用しますが、次のリストに示すように、一部のキーが含まれず、他のキーには特定の値が使用されます。 <ul style="list-style-type: none"> ◦ * eventSource* <pre>sgws:s3</pre> ◦ * awsRegion * <p>含まれません</p> ◦ * x-amz-id-2 * <p>含まれません</p> ◦ * arn * <pre>urn:sgws:s3:::bucket_name</pre>
<p>PutBucketPolicyのように指定します</p>	<p>バケットに関連付けられたポリシーを設定します。を参照してください "バケットとグループのアクセスポリシーを使用"。</p>

操作	実装
PutBucketReplicationの略	<p>構成 "StorageGRID CloudMirrorレプリケーション" (バケット用)。要求の本文に含まれるレプリケーション設定XMLを使用します。CloudMirror レプリケーションについては、実装に関する次の詳細事項に注意してください。</p> <ul style="list-style-type: none"> StorageGRID では、V1 のレプリケーション設定のみがサポートされます。つまり、StorageGRID では、の使用はサポートされていません Filter ルールのエレメント。V1の規則に従ってオブジェクトバージョンを削除します。詳細については、を参照してください "Amazon Simple Storage Serviceユーザガイド：レプリケーションの設定"。 バケットレプリケーションは、バージョン管理されているバケットでもバージョン管理されていないバケットでも設定でき レプリケーション設定 XML の各ルールで異なるデスティネーションバケットを指定できます。1つのソースバケットを複数のデスティネーションバケットにレプリケートできます。 デスティネーションバケットは、テナントマネージャまたはテナント管理 API で指定された StorageGRID エンドポイントの URN として指定する必要があります。を参照してください "CloudMirror レプリケーションを設定します"。 <p>レプリケーション設定が機能するためには、エンドポイントが存在している必要があります。エンドポイントが存在しない場合は、として要求が失敗します 400 Bad Request。エラーメッセージ：Unable to save the replication policy. The specified endpoint URN does not exist: URN.</p> <ul style="list-style-type: none"> を指定する必要はありません Role 設定XMLを使用します。この値は StorageGRID では使用されず、送信されても無視されます。 設定XMLでストレージクラスを省略した場合、StorageGRID ではを使用します STANDARD デフォルトのストレージクラス。 ソースバケットからオブジェクトを削除する場合、またはソースバケット自体を削除する場合、クロスリージョンレプリケーションは次のように動作します。 <ul style="list-style-type: none"> レプリケートの前にオブジェクトまたはバケットを削除した場合、オブジェクトまたはバケットはレプリケートされず、通知も送信されません。 レプリケートのあとにオブジェクトまたはバケットを削除すると、StorageGRID は、V1 のクロスリージョンレプリケーションに対する Amazon S3 の通常の削除動作に従います。

操作	実装
PutBucketTaggingの略	<p>を使用します tagging サブリソース：バケットの一連のタグを追加または更新できます。バケットタグを追加する場合は、次の制限事項に注意してください。</p> <ul style="list-style-type: none"> StorageGRID と Amazon S3 はどちらもバケットごとに最大 50 個のタグをサポートします。 バケットに関連付けられているタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで使用できます。 タグ値には、Unicode 文字を 256 文字以内で指定します。 キーと値では大文字と小文字が区別されます。 <p>注意：このバケットにデフォルト以外のILMポリシータグが設定されている場合、NTAP-SG-ILM-BUCKET-TAG 値が割り当てられたバケットタグ。次のことを確認します。NTAP-SG-ILM-BUCKET-TAG バケットタグは、すべてのPutBucketTagging要求で割り当てられた値に含まれます。このタグを変更または削除しないでください。</p> <p>注：この処理を実行すると、バケットにすでに設定されている現在のタグが上書きされます。セットから既存のタグを省略すると、それらのタグはバケットから削除されます。</p>
PutBucketVersioningの各ノードの設定	<p>を使用します versioning サブリソース：既存のバケットのバージョン管理の状態を設定できます。バージョン管理の状態は、次のいずれかの値に設定できます。</p> <ul style="list-style-type: none"> Enabled：バケット内のオブジェクトに対してバージョン管理を有効にします。バケットに追加されるすべてのオブジェクトに、一意のバージョン ID が割り当てられます。 Suspended：バケット内のオブジェクトに対してバージョン管理を無効にします。バケットに追加されるすべてのオブジェクトに、バージョンIDが割り当てられます null。
PutObjectLockConfigurationの略	<p>バケットのデフォルトの保持モードとデフォルトの保持期間を設定または削除します。</p> <p>デフォルトの保持期間を変更した場合、既存のオブジェクトバージョンの retain-until はそのまま残り、新しいデフォルトの保持期間を使用して再計算されることはありません。</p> <p>を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します" を参照してください。</p>

オブジェクトの処理

オブジェクトの処理

このセクションでは、StorageGRID システムでオブジェクトの S3 REST API 処理を実

装する方法について説明します。

すべてのオブジェクトの処理に次の条件が適用されます。

- StorageGRID "整合性の値" オブジェクトに対するすべての操作でサポートされます。ただし、次の操作はサポートされません。
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetentionの略
 - SelectObjectContent の順に選択します
- 同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。
- StorageGRID バケット内のオブジェクトは、匿名ユーザまたは別のアカウントが作成したオブジェクトも含めて、すべてバケット所有者によって所有されます。
- Swiftを使用してStorageGRID システムに取り込まれたデータオブジェクトにS3を使用してアクセスすることはできません。

次の表に、StorageGRID での S3 REST API オブジェクト処理の実装方法を示します。

操作	実装
deleteObject	<p>多要素認証 (MFA) と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>DeleteObject要求を処理すると、StorageGRIDはすべての格納場所からオブジェクトのすべてのコピーをただちに削除しようとします。成功すると、StorageGRID はただちにクライアントに応答を返します。30秒以内にすべてのコピーを削除できない場合（場所が一時的に使用できない場合など）、StorageGRID は削除対象のコピーをキューに登録し、クライアントに成功を通知します。</p> <p>バージョン管理</p> <p>特定のバージョンを削除するには、バケットの所有者を要求元にしてを使用する必要があります <code>versionId</code> サブリソース：このサブリソースを使用すると、バージョンが完全に削除されます。状況に応じて <code>versionId</code> 削除マーカー、応答ヘッダーに対応します <code>x-amz-delete-marker</code> はに設定されています <code>true</code>。</p> <ul style="list-style-type: none"> • を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが有効になっているバケットのサブリソースが表示されると、削除マーカーが生成されます。。 <code>versionId</code> 削除マーカーの場合は、を使用して戻ります <code>x-amz-version-id</code> 応答ヘッダー、および <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 • を使用せずにオブジェクトが削除された場合 <code>versionId</code> バージョンが一時停止中のバケットについて、既存の「null」バージョンまたは「null」削除マーカーが完全に削除され、新しい「null」削除マーカーが生成されます。。 <code>x-amz-delete-marker</code> 応答ヘッダーがに設定されて返されます <code>true</code>。 • 注 * : 特定の場合、1つのオブジェクトに複数の削除マーカーが存在することがあります。 <p>を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します" ガバナンスモードでオブジェクトバージョンを削除する方法については、を参照してください。</p>
<p>オブジェクトを削除します</p> <p>(以前の名前はDELETE Multiple Objects)</p>	<p>多要素認証 (MFA) と応答ヘッダー <code>x-amz-mfa</code> はサポートされていません。</p> <p>同じ要求メッセージで複数のオブジェクトを削除できます。</p> <p>を参照してください "S3 REST APIを使用してS3オブジェクトロックを設定します" ガバナンスモードでオブジェクトバージョンを削除する方法については、を参照してください。</p>

操作	実装
DeleteObjectTagging の場合	<p>を使用します tagging サブリソース：オブジェクトからすべてのタグを削除します。</p> <p>バージョン管理</p> <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが削除されます。オブジェクトの現在のバージョンが削除マーカの場合、「MethodNotAllowed」ステータスが返され、x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
GetObject	"GetObject"
GetObjectAcl	アカウントに必要なアクセスクレデンシャルがある場合、オブジェクトの所有者にオブジェクトに対するフルアクセスがあることを示す応答が返され、所有者の ID、表示名、および権限が表示されます。
GetObjectLegalHold	"S3 REST APIを使用してS3オブジェクトロックを設定します"
GetObjectRetentionの略	"S3 REST APIを使用してS3オブジェクトロックを設定します"
GetObjectTagging の 2 つの機能を	<p>を使用します tagging サブリソース：オブジェクトのすべてのタグを返すために使用します。</p> <p>バージョン管理</p> <p>状況に応じて versionId クエリパラメータが要求で指定されていない場合、バージョン管理されたバケット内のオブジェクトの最新バージョンからすべてのタグが返されます。オブジェクトの現在のバージョンが削除マーカの場合、「MethodNotAllowed」ステータスが返され、x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
HeadObject (ヘッドオブジェクト)	"HeadObject (ヘッドオブジェクト) "
RestoreObject	"RestoreObject"
PutObject	"PutObject"
CopyObject (以前の名前はPUT Object - Copy)	"CopyObject"
PutObjectLegalHold	"S3 REST APIを使用してS3オブジェクトロックを設定します"

操作	実装
PutObjectRetentionの略	"S3 REST APIを使用してS3オブジェクトロックを設定します"
PutObjectTagging の 2 つのグループが	<p>を使用します tagging サブリソース：既存のオブジェクトに一連のタグを追加します。</p> <p>オブジェクトタグの制限</p> <p>タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。</p> <p>タグの更新と取り込み動作</p> <p>PutObjectTaggingを使用してオブジェクトのタグを更新した場合、StorageGRIDはオブジェクトを再取り込みしません。これは、一致する ILM ルールで指定されている取り込み動作が使用されないことを意味します。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価される時に実施されます。</p> <p>つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。</p> <p>競合の解決</p> <p>同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。</p> <p>バージョン管理</p> <p>状況に応じて versionId クエリパラメータが要求で指定されていません。処理は、バージョン管理されたバケット内のオブジェクトの最新バージョンにタグを追加します。オブジェクトの現在のバージョンが削除マーカの場合、「MethodNotAllowed」ステータスが返され、x-amz-delete-marker 応答ヘッダーをに設定しました true。</p>
SelectObjectContent の順に選択します	"SelectObjectContent の順に選択します"

S3 Select を使用する

StorageGRID は、で次のAmazon S3 Select句、データ型、および演算子をサポートしています "[SelectObjectContent コマンド](#)"。



リストされていない項目はサポートされていません。

構文については、を参照してください "[SelectObjectContent の順に選択します](#)"。S3 Select の詳細については、を参照してください "[S3 Select に関する AWS のドキュメント](#)"。

問題 SelectObjectContent クエリを実行できるのは、S3 Select が有効になっているテナントアカウントのみです。を参照してください "[S3 Select を使用する際の考慮事項と要件](#)"。

句

- リストを選択します
- FROM 句
- WHERE 句
- Limit 句

データ型

- ブール値
- 整数
- 文字列
- 浮動小数点
- 10 進数、数値
- タイムスタンプ

演算子

論理演算子

- および
- ありません
- または

比較演算子

- <
- >
- <=
- >=
- =

- =
- <>
- !=
- 間 (Between)
- インチ

パターンマッチング演算子

- いいね
- _
- %

単一の演算子

- は NULL です
- は NULL ではありません

数学演算子

- [+]
- -
- *
- /
- %

StorageGRID はAmazon S3 Selectオペレータの優先順位に従います。

集合関数

- 平均 ()
- カウント (*)
- 最大 ()
- 最小 ()
- 合計 ()

条件付き関数

- ケース
- 集合体
- NULLIF

変換関数

- CAST (サポートされているデータタイプ用)

日付関数

- date_add
- DATE_DIFF
- 抽出 (Extract)
- 文字列まで (_STRING)
- 終了タイムスタンプ
- UTCNOW

文字列関数

- char_length、character_length
- 低い
- サブストリング
- トリム (Trim)
- 上限

サーバ側の暗号化を使用します

サーバ側の暗号化を使用して、保存中のオブジェクトデータを保護できます。StorageGRID は、オブジェクトを書き込む際にデータを暗号化し、ユーザがオブジェクトにアクセスする際にデータを復号化します。

サーバ側の暗号化を使用する場合は、暗号化キーの管理方法に基づいて、次の 2 つのオプションを同時に選択できます。

- * SSE (StorageGRID で管理されるキーによるサーバ側の暗号化) * : オブジェクトを格納する S3 要求を問題 で暗号化すると、StorageGRID は一意のキーでオブジェクトを暗号化します。オブジェクトを読み出す S3 要求を問題 で実行すると、StorageGRID は格納されているキーを使用してオブジェクトを復号化します。
- * SSE-C (ユーザ指定のキーによるサーバ側の暗号化) * : オブジェクトを格納する S3 要求を問題 で処理するときに、独自の暗号化キーを指定します。オブジェクトを読み出すときは、同じ暗号化キーを要求に指定します。2 つの暗号化キーが一致すると、オブジェクトが復号化されてオブジェクトデータが返されます。

オブジェクトの暗号化処理と復号化処理はすべて StorageGRID で管理されますが、指定する暗号化キーはユーザが管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。



SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

SSE を使用します

StorageGRID で管理される一意のキーでオブジェクトを暗号化する場合は、次の要求ヘッダーを使用します。

x-amz-server-side-encryption

SSE 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "PutObject"
- "CopyObject"
- "CreateMultipartUpload を実行します"

SSE-C を使用します

ユーザが管理する一意のキーでオブジェクトを暗号化する場合は、次の 3 つの要求ヘッダーを使用します。

要求ヘッダー	説明
x-amz-server-side-encryption-customer-algorithm	暗号化アルゴリズムを指定します。ヘッダー値はである必要があります AES256。
x-amz-server-side-encryption-customer-key	オブジェクトの暗号化と復号化に使用する暗号化キーを指定します。キーの値は、Base64 でエンコードされた 256 ビットであることが必要です。
x-amz-server-side-encryption-customer-key-MD5	RFC 1321 に従って暗号化キーの MD5 ダイジェストを指定します。これは、暗号化キーがエラーなしで送信されたことを確認するために使用されます。MD5 ダイジェストの値は、Base64 でエンコードされた 128 ビットであることが必要です。

SSE-C 要求ヘッダーは、次のオブジェクト処理でサポートされます。

- "GetObject"
- "HeadObject (ヘッドオブジェクト)"
- "PutObject"
- "CopyObject"
- "CreateMultipartUpload を実行します"
- "UploadPart のアップロード"
- "UploadPartCopyをクリックします"

ユーザ指定のキーによるサーバ側の暗号化 (SSE-C) を使用する場合は考慮事項

SSE-C を使用する場合は、次の考慮事項に注意してください。

- HTTPS を使用する必要があります。



SSE-C を使用すると、http 経由の要求が StorageGRID ですべて拒否されますセキュリティ上の理由から、誤って http を使用して送信したキーは漏洩する可能性があります。キーを破棄し、必要に応じてローテーションします。

- 応答内の ETag は、オブジェクトデータの MD5 ではありません。
- 暗号化キーとオブジェクトの対応関係を管理する必要があります。StorageGRID では暗号化キーは格納されません。各オブジェクトに対して指定した暗号化キーを管理する責任はユーザにあります。
- バケットのバージョン管理が有効になっている場合は、オブジェクトのバージョンごとに固有の暗号化キーが必要です。各オブジェクトバージョンで使用される暗号化キーを管理する責任はユーザにあります。
- 暗号化キーはクライアント側で管理するため、キーローテーションなどの追加の防護策もクライアント側で管理する必要があります。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。

- バケットにクロスグリッドレプリケーションまたはCloudMirrorレプリケーションが設定されている場合は、SSE-Cオブジェクトを取り込むことはできません。取り込み処理は失敗します。

関連情報

["Amazon S3ユーザガイド：ユーザ指定のキーによるサーバ側の暗号化（SSE-C）の使用"](#)

CopyObject

S3 CopyObject要求を使用して、すでにS3に格納されているオブジェクトのコピーを作成できます。CopyObject操作は、GetObjectを実行してからPutObjectを実行する操作と同じです。

競合を解決します

同じキーに書き込む2つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングで行われます。

オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB（5、368、709、120バイト）です。5GiBを超えるオブジェクトがある場合は、["マルチパートアップロード"](#)代わりに、

1回のPutObject処理のmaximum_supported_sizeは5TiB（5、497、558、138、880バイト）です。



StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとする、S3 PUT Object size too largeアラートがトリガーされません。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない） UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、要求は正常に実行されません。
- StorageGRID から返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- ``x-amz-meta-`` をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します
- `x-amz-metadata-directive`: デフォルト値は `COPY` をクリックすると、オブジェクトおよび関連するメタデータをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のメタデータを上書きする場合、またはオブジェクトメタデータを更新する場合。

- `x-amz-storage-class`
- `x-amz-tagging-directive`: デフォルト値は `COPY` をクリックすると、オブジェクトとすべてのタグをコピーできます。

を指定できます `REPLACE` オブジェクトのコピー時に既存のタグを上書きする場合、またはタグを更新する場合。

- S3 オブジェクトロック要求のヘッダー：

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードと `retain-until-date` が計算されます。を参照してください ["S3 REST API を使用して S3 オブジェクトロックを設定します"](#)。

- SSE 要求ヘッダー：

- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

を参照してください [\[サーバ側の暗号化を行うための要求ヘッダー\]](#)

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-website-redirect-location

ストレージクラスのオプション

◦ x-amz-storage-class 要求ヘッダーがサポートされ、一致するILMルールでDual commitまたはBalancedが使用されている場合にStorageGRIDで作成されるオブジェクトコピーの数に影響します。"[取り込みオプション](#)"。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

CopyObjectでのx-amz-copy-sourceの使用

ソースのバケットとキーの場合は、で指定します x-amz-copy-source ヘッダーはデスティネーションのバケットおよびキーとは異なり、ソースオブジェクトデータのコピーがデスティネーションに書き込まれます。

送信元と宛先が一致している場合は、および x-amz-metadata-directive ヘッダーはのように指定します `REPLACE` では、要求で指定されたメタデータの値に基づいてオブジェクトのメタデータが更新されます。この場合、StorageGRID はオブジェクトを再取り込みしません。これには2つの重要な結果があります。

- CopyObjectを使用して既存のオブジェクトを暗号化したり、既存のオブジェクトの暗号化を変更したりすることはできません。を用意する場合は x-amz-server-side-encryption ヘッダーまたは x-amz-server-side-encryption-customer-algorithm ヘッダー。StorageGRID は要求を拒否し、戻ります XNotImplemented。
- 一致する ILM ルールで指定されている取り込み動作のオプションが使用されません。更新によって発生したオブジェクト配置の変更は、通常のバックグラウンド ILM プロセスで ILM が再評価されるときに実施されます。

つまり、ILMルールの取り込み動作にStrictオプションが使用されている場合、必要なオブジェクト配置を実行できない場合（新たに必要な場所が使用できない場合など）は処理されません。更新されたオブジェクトは、必要な配置を実行可能になるまで現在の配置が維持されます。

サーバ側の暗号化を行うための要求ヘッダー

あなたの場合 "[サーバ側の暗号化を使用する](#)"指定する要求ヘッダーは、ソースオブジェクトが暗号化されているかどうか、およびターゲットオブジェクトを暗号化するかどうかによって異なります。

- ソースオブジェクトがユーザ指定のキーを使用して暗号化されている場合 (SSE-C) は、オブジェクトを復号化してコピーできるように、CopyObject要求に次の3つのヘッダーを含める必要があります。
 - x-amz-copy-source-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-copy-source-server-side-encryption-customer-key:ソースオブジェクトの作成時に指定した暗号化キーを指定します
 - x-amz-copy-source-server-side-encryption-customer-key-MD5:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。
- ユーザが指定および管理する一意のキーでターゲットオブジェクト（コピー）を暗号化する場合は、次の3つのヘッダーを含めます。
 - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-server-side-encryption-customer-key:ターゲットオブジェクトの新しい暗号化キーを指定します
 - x-amz-server-side-encryption-customer-key-MD5:新しい暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "[サーバ側の暗号化を使用する](#)"。

- ターゲットオブジェクト（コピー）をStorageGRID（SSE）で管理される一意のキーで暗号化する場合は、CopyObject要求に次のヘッダーを含めます。

◦ `x-amz-server-side-encryption`



◦ `server-side-encryption` オブジェクトの値を更新できません。代わりに、新しいを使用してコピーを作成します `server-side-encryption` を使用した値 `x-amz-metadata-directive: REPLACE`。

バージョン管理

ソースバケットがバージョン管理に対応している場合は、を使用できます `x-amz-copy-source` オブジェクトの最新バージョンをコピーするヘッダー。オブジェクトの特定のバージョンをコピーするには、を使用してコピーするバージョンを明示的に指定する必要があります `versionId` サブリソース：デスティネーションバケットがバージョン管理に対応している場合は、で生成されたバージョンが返されます `x-amz-version-id` 応答ヘッダー。ターゲットバケットのバージョン管理が一時停止中の場合は、を実行します `x-amz-version-id "null"` 値を返します。

GetObject

S3 GetObject要求を使用すると、S3バケットからオブジェクトを読み出すことができます。

GetObjectオブジェクトとマルチパートオブジェクト

を使用できます `partNumber` マルチパートまたはセグメント化されたオブジェクトの特定の部分を読み出す要求パラメータ。◦ `x-amz-mp-parts-count` response要素は、オブジェクトに含まれるパーツの数を示します。

設定できます `partNumber` セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの場合は1になります。ただし、`x-amz-mp-parts-count` 応答要素は、セグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

ユーザメタデータ内の UTF-8 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義のメタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対する GET 要求で、`x-amz-missing-meta` キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません `XNotImplemented` :

- `x-amz-website-redirect-location`

バージョン管理

の場合 `versionId` サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが `x-amz-delete-marker` 応答ヘッダーをに設定しました `true`。

ユーザ指定の暗号化キーによるサーバ側の暗号化（**SSE-C**）の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、3つのヘッダーをすべて使用します。

- `x-amz-server-side-encryption-customer-algorithm`:指定します AES256。
- `x-amz-server-side-encryption-customer-key`:オブジェクトの暗号化キーを指定します
- `x-amz-server-side-encryption-customer-key-MD5`:オブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "[サーバ側の暗号化を使用します](#)"。

クラウドストレージプールオブジェクトに対する**GetObject**の動作

オブジェクトがに格納されている場合 "[クラウドストレージプール](#)"の場合、GetObject要求の動作はオブジェクトの状態によって異なります。を参照してください "[HeadObject \(ヘッドオブジェクト\)](#)" 詳細：



オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合、GetObject要求はクラウドストレージプールからデータを読み出す前にグリッドからデータを読み出そうとします。

オブジェクトの状態	GetObjectの動作
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK オブジェクトのコピーが読み出されます。
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK オブジェクトのコピーが読み出されます。
オブジェクトを読み出し不可能な状態に移行した	403 Forbidden、 InvalidObjectState を使用します " RestoreObject " 読み出し可能な状態へのオブジェクトのリストア要求。
読み出し不可能な状態からリストア中である	403 Forbidden、 InvalidObjectState RestoreObject要求が完了するまで待ちます。
クラウドストレージプールへのリストアが完了している	200 OK オブジェクトのコピーが読み出されます。

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。GetObject要求が誤って返されることがある 200 OK オブジェクトの一部のパーツがすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部のパーツがまだリストアされていない場合。

このような場合は、次のよう

- GetObject要求から一部のデータが返される場合がありますが、転送の途中で停止することがあります。
- 後続のGetObject要求で次のように返されることがある 403 Forbidden。

GetObjectとグリッド間レプリケーション

使用するポート "[グリッドフェデレーション](#)" および "[グリッド間レプリケーション](#)" バケットで有効になっている場合、S3クライアントはGetObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有の情報が含まれます `x-ntap-sg-cgr-replication-status` 応答ヘッダー。次のいずれかの値が設定されます。

グリッド (Grid)	レプリケーションのステータス
ソース	<ul style="list-style-type: none">• 成功：レプリケーションは成功しました。• * pending*：オブジェクトはまだレプリケートされていません。• failure:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
宛先	replica :オブジェクトはソースグリッドからレプリケートされました。



StorageGRID ではがサポートされません `x-amz-replication-status` ヘッダー。

HeadObject (ヘッドオブジェクト)

S3 HeadObject要求を使用すると、オブジェクト自体を返さずにオブジェクトからメタデータを読み出すことができます。オブジェクトがクラウドストレージプールに格納されている場合は、HeadObjectを使用してオブジェクトの移行状態を確認できます。

HeadObjectオブジェクトとマルチパートオブジェクト

を使用できます `partNumber` マルチパートまたはセグメント化されたオブジェクトの特定の部分のメタデータを読み出す要求パラメータ。 `x-amz-mp-parts-count` response要素は、オブジェクトに含まれるパーツの数を示します。

設定できます `partNumber` セグメント化されたオブジェクト/マルチパートオブジェクトとセグメント化されていないオブジェクト/マルチパート以外のオブジェクトの場合は1になります。ただし、 `x-amz-mp-parts-count` 応答要素は、セグメント化されたオブジェクトまたはマルチパートオブジェクトの場合にのみ返されます。

ユーザメタデータ内の UTF-8 文字

StorageGRID は、ユーザ定義メタデータ内のエスケープされた UTF-8 文字を解析も解釈もしません。ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれているオブジェクトに対する HEAD 要求では、が返されません x-amz-missing-meta キーの名前または値に印刷できない文字が含まれている場合は、ヘッダーを指定します。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません XNotImplemented :

- x-amz-website-redirect-location

バージョン管理

の場合 versionId サブリソースが指定されていません。バージョン管理されたバケット内のオブジェクトの最新バージョンが取得されます。オブジェクトの現在のバージョンが削除マーカーの場合は、「Not Found」ステータスが x-amz-delete-marker 応答ヘッダーをに設定しました true。

ユーザ指定の暗号化キーによるサーバ側の暗号化 (SSE-C) の要求ヘッダー

指定した一意のキーでオブジェクトが暗号化されている場合は、次の 3 つのヘッダーをすべて使用します。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key:オブジェクトの暗号化キーを指定します
- x-amz-server-side-encryption-customer-key-MD5:オブジェクトの暗号化キーの MD5 ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください **"サーバ側の暗号化を使用します"**。

クラウドストレージプールオブジェクトに対する HeadObject 応答

オブジェクトがに格納されている場合 **"クラウドストレージプール"**を指定すると、次の応答ヘッダーが返されます。

- x-amz-storage-class: GLACIER
- x-amz-restore

応答ヘッダーは、オブジェクトがクラウドストレージプールに移動され、必要に応じて読み出し不可能な状態に移行されてリストアされる時の状態に関する情報を提供します。

オブジェクトの状態	HeadObject への応答
StorageGRID に取り込まれているがまだ ILM によって評価されていないオブジェクト、または従来のストレージプールに格納されているオブジェクト、またはイレイジャーコーディングを使用しているオブジェクト	200 OK (特別な応答ヘッダーは返されません)。

オブジェクトの状態	HeadObjectへの応答
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>'x-amz-restore : ongoing-request="false"、expiry-date="2030年7月23日 (土) 00 : 00 : 00 GMT</p> <p>オブジェクトが読み出し不可能な状態に移行されるまでの間、の値 expiry-date は、将来の特定の日に設定されます。移行の正確な時間は、StorageGRID システムでは制御されません。</p>
オブジェクトが読み出し不可能な状態に移行したが、少なくとも1つのコピーがグリッドに存在する	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>'x-amz-restore : ongoing-request="false"、expiry-date="2030年7月23日 (土) 00 : 00 : 00 GMT</p> <p>の値 expiry-date は、将来の特定の日に設定されます。</p> <p>注：グリッド上のコピーを使用できない場合（ストレージノードが停止している場合など）は、問題を実行する必要があります "RestoreObject" オブジェクトを読み出す前にクラウドストレージプールからコピーをリストアする要求。</p>
読み出し不可能な状態に移行しており、グリッドにコピーが存在しない	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
読み出し不可能な状態からリストア中である	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>'x-amz-restore : ongoing-request="true"</p>
クラウドストレージプールへのリストアが完了している	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>'x-amz-restore : ongoing-request="false"、expiry-date="2018年7月23日 (土) 00 : 00 : 00 (GMT) "</p> <p>。 expiry-date クラウドストレージプール内のオブジェクトが読み出し不可能な状態に戻るタイミングを示します。</p>

クラウドストレージプール内のマルチパートオブジェクトまたはセグメント化されたオブジェクト

マルチパートオブジェクトをアップロードした場合や StorageGRID が大きなオブジェクトをセグメントに分割した場合、StorageGRID はオブジェクトのパーツまたはセグメントのサブセットをサンプリングすることでクラウドストレージプール内のオブジェクトが使用可能かどうかを判断します。オブジェクトの一部の部分がすでに読み出し不可能な状態に移行されている場合や、オブジェクトの一部がまだリストアされていない場合、HeadObject要求が誤って「x-amz-restore : ongoing-request="false"」を返すことがあります。

HeadObjectとクロスグリッドレプリケーション

使用するポート "[グリッドフェデレーション](#)" および "[グリッド間レプリケーション](#)" バケットで有効になっている場合、S3クライアントはHeadObject要求を発行してオブジェクトのレプリケーションステータスを確認できます。応答にはStorageGRID固有の情報が含まれます x-ntap-sg-cgr-replication-status 応答ヘッダー。次のいずれかの値が設定されます。

グリッド (Grid)	レプリケーションのステータス
ソース	<ul style="list-style-type: none">成功：レプリケーションは成功しました。* pending* : オブジェクトはまだレプリケートされていません。failure:レプリケーションが永続的なエラーで失敗しました。ユーザーはエラーを解決する必要があります。
宛先	replica :オブジェクトはソースグリッドからレプリケートされました。



StorageGRID ではサポートされません x-amz-replication-status ヘッダー。

PutObject

S3 PutObject要求を使用して、バケットにオブジェクトを追加できます。

競合を解決します

同じキーに書き込む 2 つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3 クライアントが処理を開始するタイミングではなく、StorageGRID システムが特定の要求を完了したタイミングで行われます。

オブジェクトのサイズ

1回のPutObject処理の最大推奨サイズは5GiB (5、368、709、120バイト) です。5GiBを超えるオブジェクトがある場合は、"[マルチパートアップロード](#)" 代わりに、

1回のPutObject処理のmaximum_supported_sizeは5TiB (5、497、558、138、880バイト) です。



StorageGRID 11.6以前からアップグレードした場合、5GiBを超えるオブジェクトをアップロードしようとする、S3 PUT Object size too largeアラートがトリガーされます。StorageGRID 11.7または11.8を新規にインストールした場合、この場合アラートはトリガーされません。ただし、AWS S3標準に準拠するため、StorageGRIDの今後のリリースでは5GiBを超えるオブジェクトのアップロードはサポートされません。

ユーザメタデータのサイズ

Amazon S3 では、各 PUT 要求ヘッダー内のユーザ定義メタデータのサイズが 2KB に制限されます。StorageGRID では、ユーザメタデータが 24KiB に制限されます。ユーザ定義のメタデータのサイズは、各キーと値の UTF-8 エンコードでのバイト数の合計で測定されます。

ユーザメタデータ内の UTF-8 文字

要求のユーザ定義メタデータのキー名または値に（エスケープされていない）UTF-8 文字が含まれている場合、StorageGRID の動作は定義されていません。

ユーザ定義メタデータのキー名または値に含まれているエスケープされた UTF-8 文字は、StorageGRID で解析も解釈もされません。エスケープされた UTF-8 文字は ASCII 文字として扱われます。

- ユーザ定義メタデータにエスケープされた UTF-8 文字が含まれている場合、PutObject、CopyObject、GetObject、および HeadObject の各要求は成功します。
- StorageGRID から返されない `x-amz-missing-meta` キーの名前または値の解釈後の値に印刷不能文字が含まれている場合は、ヘッダー。

オブジェクトタグの制限

タグは、新しいオブジェクトをアップロードするときに追加することも、既存のオブジェクトに追加することもできます。StorageGRID と Amazon S3 はどちらも、オブジェクトごとに最大 10 個のタグをサポートします。オブジェクトに関連付けられたタグには、一意のタグキーが必要です。タグキーには Unicode 文字を 128 文字まで、タグ値には Unicode 文字を 256 文字まで使用できます。キーと値では大文字と小文字が区別されます。

オブジェクトの所有権

StorageGRID では、非所有者アカウントまたは匿名ユーザによって作成されたオブジェクトを含むすべてのオブジェクトが、バケット所有者アカウントによって所有されます。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Cache-Control
- Content-Disposition
- Content-Encoding

を指定する場合 `aws-chunked` の場合 Content-Encoding StorageGRID では、次の項目は検証されません。

- StorageGRID ではが検証されません `chunk-signature` チャンクデータに対して。
- StorageGRID は、ユーザが指定した値を検証しません `x-amz-decoded-content-length` をクリックします。
- Content-Language
- Content-Length
- Content-MD5

- Content-Type
- Expires
- Transfer-Encoding

チャンク転送エンコードは、の場合にサポートされます `aws-chunked` ペイロード署名も使用されます。

- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します。

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-name: value
```

ILMルールの参照時間に*[ユーザ定義の作成時間]*オプションを使用する場合は、を使用する必要があります `creation-time` を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 `creation-time` は、1970年1月1日からの秒数として評価されます。



ILMルールでは、参照時間に*ユーザ定義の作成時間*を使用し、取り込みオプションをBalancedまたはStrictの両方にすることはできません。ILM ルールの作成時にエラーが返されます。

- `x-amz-tagging`
- S3 Object Lock 要求のヘッダー
 - `x-amz-object-lock-mode`
 - `x-amz-object-lock-retain-until-date`
 - `x-amz-object-lock-legal-hold`

これらのヘッダーを指定せずに要求を行うと、バケットのデフォルトの保持設定を使用してオブジェクトバージョンモードと`retain-until-date`が計算されます。を参照してください "[S3 REST APIを使用し、S3オブジェクトロックを設定します](#)"。

- SSE 要求ヘッダー：
 - `x-amz-server-side-encryption`
 - `x-amz-server-side-encryption-customer-key-MD5`
 - `x-amz-server-side-encryption-customer-key`
 - `x-amz-server-side-encryption-customer-algorithm`

を参照してください [\[サーバ側の暗号化を行うための要求ヘッダー\]](#)

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません。

- `x-amz-acl` 要求ヘッダーはサポートされていません。
- `x-amz-website-redirect-location` 要求ヘッダーはサポートされておらず、返されます `XNotImplemented`。

ストレージクラスのオプション

• `x-amz-storage-class` 要求ヘッダーがサポートされています。に送信された値 `x-amz-storage-class StorageGRID` が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrict取り込みオプションが使用されている場合は、`x-amz-storage-class` ヘッダーに影響はありません。

には次の値を使用できます `x-amz-storage-class` :

- STANDARD (デフォルト)
 - * Dual commit * : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み直後にオブジェクトの 2 つ目のコピーが作成されて別のストレージノードに配置されます (デュアルコミット)。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェクトコピーを別の場所に作成し、最初の間コピーを削除しなければならないことがあります。
 - * Balanced * : ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別々のストレージノードに作成します。

StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合 (同期配置) は、を参照してください `x-amz-storage-class` ヘッダーに影響はありません。

- REDUCED_REDUNDANCY
 - * Dual commit * : ILM ルールの取り込み動作が Dual commit オプションに指定されている場合は、オブジェクトの取り込み時に StorageGRID が中間コピーを 1 つ作成します (シングルコミット)。
 - * Balanced * : ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。REDUCED_REDUNDANCY オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが 1 つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。



レプリケートコピーを一定期間に1つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが1つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブなILMポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムでデータが格納される際の冗長性レベルが低下することはありません。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

サーバ側の暗号化を行うための要求ヘッダー

オブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- * SSE * : StorageGRID で管理される一意のキーでオブジェクトを暗号化するには、次のヘッダーを使用します。
 - x-amz-server-side-encryption
- * SSE-C * : ユーザーが指定および管理する一意のキーでオブジェクトを暗号化する場合は、次の3つのヘッダーをすべて使用します。
 - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定します。
 - x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザー指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "[サーバ側の暗号化を使用する](#)"。



SSE または SSE-C で暗号化されたオブジェクトは、バケットレベルまたはグリッドレベルの暗号化設定が無視されます。

バージョン管理

バケットでバージョン管理が有効になっている場合は、一意です versionId は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ versionId は、を使用して応答としても返されます x-amz-version-id 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます versionId また、nullバージョンがすでに存在する場合は上書きされます。

Authorizationヘッダーのシグニチャ計算

を使用する場合 Authorization 要求を認証するためのヘッダー。StorageGRID はAWSと次の点で異なります。

- StorageGRID は必要ありません host に含めるヘッダー CanonicalHeaders。
- StorageGRID は必要ありません Content-Type に含まれています CanonicalHeaders。
- StorageGRID は必要ありません x-amz-* に含めるヘッダー CanonicalHeaders。



一般的なベストプラクティスとして、には常にこれらのヘッダーを含めてください CanonicalHeaders これらのヘッダーが検証されるようにするためですが、これらのヘッダーを除外しても、StorageGRID はエラーを返しません。

詳細については、を参照してください "[Authorizationヘッダーのシグニチャ計算：単一チャンクでのペイロードの転送 \(AWS Signature Version 4\)](#)"。

関連情報

["ILM を使用してオブジェクトを管理する"](#)

RestoreObject

S3 RestoreObject要求を使用して、クラウドストレージプールに格納されているオブジェクトをリストアできます。

サポートされている要求タイプ

StorageGRIDでは、オブジェクトのリストアでRestoreObject要求のみがサポートされます。ではサポートされません SELECT リストアのタイプ。戻り要求を選択してください XNotImplemented。

バージョン管理

必要に応じて、と指定します versionId バージョン管理されたバケット内のオブジェクトの特定のバージョンをリストアする。指定しない場合 `versionId` オブジェクトの最新バージョンがリストアされます

クラウドストレージプールオブジェクトでのRestoreObjectの動作

オブジェクトがに格納されている場合 "[クラウドストレージプール](#)"のRestoreObject要求の動作は、オブジェクトの状態に基づいて次のようになります。を参照してください "[HeadObject \(ヘッドオブジェクト\)](#)" 詳細：



オブジェクトがクラウドストレージプールに格納されていて、そのオブジェクトのコピーがグリッドに1つ以上存在する場合は、RestoreObject要求を実行してオブジェクトをリストアする必要はありません。代わりに、GetObject要求を使用してローカルコピーを直接取得できます。

オブジェクトの状態	RestoreObjectの動作
StorageGRID に取り込まれているがまだ ILM によって評価されていない、またはオブジェクトがクラウドストレージプールにない	403 Forbidden、InvalidObjectState
クラウドストレージプール内にあるが、まだ読み出し不可能な状態に移行していない	200 OK 変更は行われません。 注：オブジェクトが読み出し不可能な状態に移行されるまでは変更できません expiry-date。
オブジェクトを読み出し不可能な状態に移行した	202 Accepted 要求の本文で指定されている日数、オブジェクトの読み出し可能なコピーをクラウドストレージプールにリストアします。この期間が終了すると、オブジェクトは読み出し不可能な状態に戻ります。 必要に応じて、を使用します Tier リストアジョブの完了までにかかる時間を確認するための要求要素 (Expedited、Standard`または`Bulk) 。指定しない場合 Tier、 Standard 階層を使用しています。 重要：オブジェクトがS3 Glacier Deep Archiveに移行された場合、またはクラウドストレージプールがAzure BLOBストレージを使用している場合は、を使用してリストアできません Expedited 階層：次のエラーが返されます 403 Forbidden、InvalidTier: Retrieval option is not supported by this storage class。
読み出し不可能な状態からリストア中である	409 Conflict、RestoreAlreadyInProgress
クラウドストレージプールへのリストアが完了している	200 OK *注：*オブジェクトが読み出し可能な状態にリストアされている場合は、オブジェクトを変更できません expiry-date 新しい値を指定してRestoreObject要求を再発行する Days。要求が実行された日時に基づいてリストア日が更新されます。

SelectObjectContent の順に選択します

S3 SelectObjectContent 要求を使用すると、シンプルな SQL ステートメントに基づいて S3 オブジェクトのコンテンツをフィルタリングできます。

詳細については、を参照してください "[Amazon Simple Storage Service APIリファレンス : SelectObjectContent](#)"。

作業を開始する前に

- テナントアカウントには S3 Select 権限が割り当てられます。
- これで完了です s3:GetObject 照会するオブジェクトの権限。

- 照会するオブジェクトは、次のいずれかの形式である必要があります。
 - * CSV *。そのまま使用することも、GZIPやbzip2のアーカイブに圧縮して使用することもできます。
 - 寄木細工。寄木細工オブジェクトの追加要件：
 - S3 Selectでは、GZIPまたはSnappyを使用したカラム圧縮のみがサポートされます。S3 Selectでは、寄木細工オブジェクトのオブジェクト全体の圧縮はサポートされません。
 - S3 Selectは寄木細工の出力をサポートしていません。出力形式はCSVまたはJSONで指定する必要があります。
 - 圧縮されていない行グループの最大サイズは512MBです。
 - オブジェクトのスキーマで指定されているデータ型を使用する必要があります。
 - interval、json、list、time、またはUUID論理型は使用できません。
- SQL 式の最大長は 256KB です。
- 入力または結果のすべてのレコードの最大長は 1MiB です。

CSV要求の構文例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

寄木リクエスト構文の例

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

SQL クエリの例

このクエリは、州名、2010年人口、2015年推定人口、米国の人口調査データからの変化率を取得します。状態でないファイル内のレコードは無視されます。

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

照会するファイルの最初の数行 `SUB-EST2020_ALL.csv` 次ようになります。

```
SUMLEV, STATE, COUNTY, PLACE, COUSUB, CONCIT, PRIMGEO_FLAG, FUNCSTAT, NAME, STNAME,
CENSUS2010POP,
ESTIMATESBASE2010, POPESTIMATE2010, POPESTIMATE2011, POPESTIMATE2012, POPESTIM
ATE2013, POPESTIMATE2014,
POPESTIMATE2015, POPESTIMATE2016, POPESTIMATE2017, POPESTIMATE2018, POPESTIMAT
E2019, POPESTIMATE042020,
POPESTIMATE2020
040, 01, 000, 00000, 00000, 00000, 0, A, Alabama, Alabama, 4779736, 4780118, 4785514, 4
799642, 4816632, 4831586,
4843737, 4854803, 4866824, 4877989, 4891628, 4907965, 4920706, 4921532
162, 01, 000, 00124, 00000, 00000, 0, A, Abbeville
city, Alabama, 2688, 2705, 2699, 2694, 2645, 2629, 2610, 2602,
2587, 2578, 2565, 2555, 2555, 2553
162, 01, 000, 00460, 00000, 00000, 0, A, Adamsville
city, Alabama, 4522, 4487, 4481, 4474, 4453, 4430, 4399, 4371,
4335, 4304, 4285, 4254, 4224, 4211
162, 01, 000, 00484, 00000, 00000, 0, A, Addison
town, Alabama, 758, 754, 751, 750, 745, 744, 742, 734, 734, 728,
725, 723, 719, 717
```

AWS-CLIの使用例 (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

出力ファイルの最初の数行 `changes.csv` 次のようになります。

```
Alabama, 4779736, 4854803, 1.5705260708959658022953568983726297854
Alaska, 710231, 738430, 3.9703983633493891424057806544631253775
Arizona, 6392017, 6832810, 6.8959922978928247531256565807005832431
Arkansas, 2915918, 2979732, 2.1884703204959810255295244928012378949
California, 37253956, 38904296, 4.4299724839960620557988526104449148971
Colorado, 5029196, 5454328, 8.4532796097030221132761578590295546246
```



```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}' --output-serialization
'{"CSV":{}}' changes.csv
```

出力ファイルの最初のいくつかの行は、.csvを変更します。次のようになります。

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

マルチパートアップロードの処理

マルチパートアップロードの処理：概要

このセクションでは、StorageGRID でのマルチパートアップロードの処理のサポートについて説明します。

マルチパートアップロードのすべての処理に、次の条件と注意事項が適用されます。

- 1つのバケットに対して同時に実行するマルチパートアップロードの数が1,000を超えないようにしてください。そのバケットに対するListMultipartUploadsのクエリで不完全な結果が返されることがあります。
- StorageGRID は、マルチパートに AWS のサイズ制限を適用します。S3 クライアントは次のガイドラインに従う必要があります。
 - マルチパートアップロードの各パートのサイズは 5MiB（5、242、880 バイト）と 5GiB（5、368、709、120 バイト）の間にする必要があります。
 - 最後の部分は 5MiB（5,242,880 バイト）より小さくできます。
 - 一般に、パーツサイズはできるだけ大きくする必要があります。たとえば、100GiB オブジェクトの場合、5GB のパートサイズを使用します。各パートは固有のオブジェクトとみなされるため、大きなパートサイズを使用するとStorageGRID メタデータのオーバーヘッドが削減されます。
 - 5GB 未満のオブジェクトでは、マルチパートではないアップロードの使用を検討してください。
- ILMルールでBalancedまたはStrictが使用されている場合は、マルチパートオブジェクトの各パートの取り込み時にILMが評価され、マルチパートアップロードの完了時にオブジェクト全体に対してILMが評価されます。["取り込みオプション"](#)。これがオブジェクトとパートの配置にどのように影響するかに注意する必要があります。

- S3マルチパートアップロードの実行中にILMが変更されると、マルチパートアップロードの完了時にオブジェクトの一部の部分が現在のILM要件を満たしていない可能性があります。正しく配置されていないパートはILMルールによる再評価の対象としてキューに登録され、あとで正しい場所に移動されます。
- パートに対して ILM を評価する際、StorageGRID はオブジェクトのサイズではなくパートのサイズでフィルタリングします。つまり、オブジェクト全体のILM要件を満たしていない場所にオブジェクトの一部を格納できます。たとえば、10GB以上のオブジェクトをすべてDC1に格納し、それより小さいオブジェクトをすべてDC2に格納するルールの場合、10パートのマルチパートアップロードの1GBの各パートは取り込み時にDC2に格納されます。ただし、オブジェクト全体に対してILMが評価されると、オブジェクトのすべての部分がDC1に移動されます。
- マルチパートアップロードのすべての処理でStorageGRIDがサポートされます。 **"整合性の値"**。
- 必要に応じて、 **"サーバ側の暗号化"** マルチパートアップロードの場合：SSE（StorageGRIDで管理されるキーによるサーバ側の暗号化）を使用するには、を指定します `x-amz-server-side-encryption` CreateMultipartUpload要求の要求ヘッダーのみ。SSE-C（ユーザ指定のキーによるサーバ側の暗号化）を使用するには、CreateMultipartUpload要求と後続の各UploadPart要求に同じ3つの暗号化キー要求ヘッダーを指定します。

操作	実装
AbortMultipartUpload の略	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
CompleteMultipartUpload	を参照してください "CompleteMultipartUpload"
CreateMultipartUpload を実行します (以前の名前はInitiate Multipart Upload)	を参照してください "CreateMultipartUpload を実行します"
ListMultipartUploads	を参照してください "ListMultipartUploads"
ListParts	Amazon S3 REST API のすべての動作が実装されています。予告なく変更される場合があります。
UploadPart のアップロード	を参照してください "UploadPart のアップロード"
UploadPartCopyをクリックします	を参照してください "UploadPartCopyをクリックします"

CompleteMultipartUpload

CompleteMultipartUpload処理は、以前にアップロードされたパートをアSEMBルして、オブジェクトのマルチパートアップロードを完了します。

競合を解決します

同じキーに書き込む2つのクライアントなど、競合するクライアント要求は、「latest-wins」ベースで解決されます。「latest-wins」評価は、S3クライアントが処理を開始するタイミングではなく、StorageGRIDシステムが特定の要求を完了したタイミングで行われます。

要求ヘッダー

。 `x-amz-storage-class` 要求ヘッダーがサポートされ、一致するILMルールでDual commitまたはBalancedに指定されている場合にStorageGRIDで作成されるオブジェクトコピーの数の影響します。"取り込みオプション"。

- STANDARD

(デフォルト) ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、デュアルコミットの取り込み処理を指定します。

- REDUCED_REDUNDANCY

ILM ルールで Dual commit オプションが使用されている場合、または Balanced オプションによって中間コピーが作成される場合に、シングルコミットの取り込み処理を指定します。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。



マルチパートアップロードが 15 日以内に完了しないと、非アクティブな処理としてマークされ、関連するすべてのデータがシステムから削除されます。



。 ETag 返される値はデータのMD5サムではなく、のAmazon S3 APIの実装に従います ETag マルチパートオブジェクトの値。

バージョン管理

マルチパートアップロードは、この処理で完了します。バケットでバージョン管理が有効になっている場合は、マルチパートアップロードの完了後にオブジェクトのバージョンが作成されます。

バケットでバージョン管理が有効になっている場合は、一意です `versionId` は、格納されているオブジェクトのバージョンに対して自動的に生成されます。これ `versionId` は、を使用して応答としても返されます `x-amz-version-id` 応答ヘッダー。

バージョン管理が一時停止中の場合は、オブジェクトバージョンはnullで格納されます `versionId` また、nullバージョンがすでに存在する場合は上書きされます。



バケットでバージョン管理が有効になっているときは、同じオブジェクトキーで同時に複数のマルチパートアップロードが実行されている場合でも、マルチパートアップロードが完了するたびに常に新しいバージョンが作成されます。バケットでバージョン管理が有効になっていないときは、マルチパートアップロードの開始後に、同じオブジェクトキーで別のマルチパートアップロードが開始されて先に完了することがあります。バージョン管理が有効になっていないバケットでは、最後に完了したマルチパートアップロードが優先されます。

レプリケーション、通知、またはメタデータ通知に失敗しました

マルチパートアップロードが行われるバケットでプラットフォームサービスが設定されている場合、関連するレプリケーション操作や通知操作が失敗してもマルチパートアップロードは正常に実行されます。

この状況が発生すると、Total Events (SMTT) のアラームがグリッドマネージャで生成されます。通知に失敗した最後のオブジェクトについて、[Last Event]メッセージに「Failed to publish notifications for bucket-nameobject key」と表示されます。(このメッセージを表示するには、* nodes * > * _Storage Node_ * > * Events * を選択します。表の一番上にLast Eventが表示されます)。イベントメッセージは、にも表示されず /var/local/log/bycast-err.log。

テナントでは、オブジェクトのメタデータまたはタグを更新することで、失敗したレプリケーションまたは通知をトリガーできます。テナントでは、既存の値を再送信し、不要な変更を回避できます。

CreateMultipartUpload を実行します

CreateMultipartUpload (以前のInitiate Multipart Upload) 処理は、オブジェクトのマルチパートアップロードを開始し、アップロードIDを返します。

。 x-amz-storage-class 要求ヘッダーがサポートされています。に送信された値 x-amz-storage-class StorageGRID が取り込み中にオブジェクトデータを保護する方法に影響し、StorageGRID システム (ILMで決定) に格納されるオブジェクトの永続的コピーの数には影響しません。

取り込まれたオブジェクトに一致するILMルールでStrictが使用されている場合 "取り込みオプション"、 x-amz-storage-class ヘッダーに影響はありません。

には次の値を使用できます x-amz-storage-class :

- STANDARD (デフォルト)

- * Dual commit * : ILMルールでDual commit取り込みオプションが指定されている場合は、オブジェクトが取り込まれるとすぐにそのオブジェクトの2つ目のコピーが作成されて別のストレージノードに分散されます (デュアルコミット)。ILMが評価されると、StorageGRID はこれらの初期中間コピーがルールの配置手順を満たしているかどうかを判断します。作成されていない場合は、新しいオブジェクトコピーを別の場所に作成し、最初の間コピーを削除しなければならないことがあります。
- * Balanced * : ILMルールでBalancedオプションが指定されていて、ルールで指定されたすべてのコピーをStorageGRID がすぐに作成できない場合、StorageGRID は2つの中間コピーを別々のストレージノードに作成します。

StorageGRID がILMルールに指定されたすべてのオブジェクトコピーをただちに作成できる場合 (同期配置) は、を参照してください x-amz-storage-class ヘッダーに影響はありません。

- REDUCED_REDUNDANCY

- * Dual commit * : ILMルールでDual commitオプションが指定されている場合、StorageGRIDはオブジェクトの取り込み時に中間コピーを1つ作成します (シングルコミット)。
- * Balanced * : ILMルールでBalancedオプションが指定されている場合、StorageGRID は、ルールで指定されたすべてのコピーをただちに作成できない場合にのみ中間コピーを1つ作成します。StorageGRID で同期配置を実行できる場合、このヘッダーは効果がありません。 REDUCED_REDUNDANCY オプションは、オブジェクトに一致するILMルールで単一のレプリケートコピーが作成される場合に最適です。この場合は、を使用します REDUCED_REDUNDANCY 取り込み処理のたびに追加のオブジェクトコピーを不要に作成および削除する必要がなくなります。

を使用する REDUCED_REDUNDANCY それ以外の場合は、このオプションは推奨されません。

REDUCED_REDUNDANCY 取り込み中にオブジェクトデータが失われるリスクが高まります。たとえば、ILM 評価の前にコピーが1つだけ格納されていたストレージノードに障害が発生すると、データが失われる可能性があります。



レプリケートコピーを一定期間に1つだけ作成すると、データが永続的に失われるリスクがあります。オブジェクトのレプリケートコピーが1つしかない場合、ストレージノードに障害が発生したり、重大なエラーが発生すると、そのオブジェクトは失われます。また、アップグレードなどのメンテナンス作業中は、オブジェクトへのアクセスが一時的に失われます。

を指定します REDUCED_REDUNDANCY オブジェクトの初回取り込み時に作成されるコピー数のみに影響します。オブジェクトがアクティブなILMポリシーで評価される際に作成されるオブジェクトのコピー数には影響せず、StorageGRIDシステムでデータが格納される際の冗長性レベルが低下することはありません。



S3オブジェクトロックを有効にしてオブジェクトをバケットに取り込む場合は、を使用します REDUCED_REDUNDANCY オプションは無視されます。古い準拠バケットにオブジェクトを取り込む場合は、を参照してください REDUCED_REDUNDANCY オプションを指定するとエラーが返されます。StorageGRID では、常にデュアルコミットの取り込みが実行され、コンプライアンス要件が満たされます。

次の要求ヘッダーがサポートされています。

- Content-Type
- `x-amz-meta-`をクリックし、続けてユーザ定義のメタデータを含む名前と値のペアを作成します

ユーザ定義メタデータの名前と値のペアを指定する場合、一般的な形式は次のとおりです。

```
x-amz-meta-_name_: `value`
```

ILMルールの参照時間に*[ユーザ定義の作成時間]*オプションを使用する場合は、を使用する必要があります creation-time を、オブジェクトの作成時に記録されたメタデータの名前として指定します。例：

```
x-amz-meta-creation-time: 1443399726
```

の値 creation-time は、1970年1月1日からの秒数として評価されます。



追加中です creation-time レガシー準拠が有効になっているバケットにオブジェクトを追加する場合、ユーザ定義メタデータは許可されません。エラーが返されます。

- S3 オブジェクトロック要求のヘッダー：

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold

これらのヘッダーがない状態で要求を送信した場合、バケットのデフォルトの保持設定を使用して、オブジェクトバージョンの retain-date が計算されます。

["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)

- SSE 要求ヘッダー：

- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

[サーバ側の暗号化を行うための要求ヘッダー]



StorageGRIDでのUTF-8文字の処理方法については、を参照してください。"PutObject"。

サーバ側の暗号化を行うための要求ヘッダー

マルチパートオブジェクトをサーバ側の暗号化で暗号化するには、次の要求ヘッダーを使用します。SSE オプションと SSE-C オプションを同時に指定することはできません。

- **SSE:** StorageGRIDによって管理される一意のキーでオブジェクトを暗号化する場合は、CreateMultipartUpload要求で次のヘッダーを使用します。UploadPart要求でこのヘッダーを指定しないでください。
 - x-amz-server-side-encryption
- *** SSE-C *:** 指定および管理する一意のキーでオブジェクトを暗号化する場合は、CreateMultipartUpload 要求（および後続の各UploadPart要求）でこれら3つのヘッダーをすべて使用します。
 - x-amz-server-side-encryption-customer-algorithm:指定します AES256。
 - x-amz-server-side-encryption-customer-key:新しいオブジェクトの暗号化キーを指定します。
 - x-amz-server-side-encryption-customer-key-MD5:新しいオブジェクトの暗号化キーのMD5 ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください "[サーバ側の暗号化を使用する](#)"。

サポートされない要求ヘッダーです

次の要求ヘッダーはサポートされていません XNotImplemented

- x-amz-website-redirect-location

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

ListMultipartUploads

ListMultipartUploads処理を実行すると、バケットで実行中のマルチパートアップロード

がリストされます。

次の要求パラメータがサポートされています。

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker
- Host
- Date
- Authorization

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

UploadPart のアップロード

UploadPart処理は、オブジェクトのマルチパートアップロード内のパートをアップロードします。

サポートされる要求ヘッダー

次の要求ヘッダーがサポートされています。

- Content-Length
- Content-MD5

サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPart要求に次の要求ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key : CreateMultipartUpload要求で指定したのと同じ暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5 : CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください ["サーバ側の暗号化を使用します"](#)。

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

UploadPartCopyをクリックします

UploadPartCopy操作は、データソースとして既存のオブジェクトからデータをコピーすることによって、オブジェクトの一部をアップロードします。

UploadPartCopy処理は、Amazon S3 REST APIのすべての動作で実装されます。予告なく変更される場合があります。

この要求は、で指定されたオブジェクトデータの読み取りと書き込みを行います x-amz-copy-source-range StorageGRID システム内で実行する。

次の要求ヘッダーがサポートされています。

- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since

サーバ側の暗号化を行うための要求ヘッダー

CreateMultipartUpload要求にSSE-C暗号化を指定した場合は、各UploadPartCopy要求に次の要求ヘッダーも含める必要があります。

- x-amz-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-server-side-encryption-customer-key: CreateMultipartUpload要求で指定したのと同じ暗号化キーを指定します。
- x-amz-server-side-encryption-customer-key-MD5: CreateMultipartUpload要求で指定したMD5ダイジェストと同じMD5ダイジェストを指定します。

ソースオブジェクトがユーザ指定のキー（SSE-C）を使用して暗号化されている場合は、オブジェクトを復号化してコピーできるように、UploadPartCopy要求に次の3つのヘッダーを含める必要があります。

- x-amz-copy-source-server-side-encryption-customer-algorithm:指定します AES256。
- x-amz-copy-source-server-side-encryption-customer-key:ソースオブジェクトの作成時に指定した暗号化キーを指定します
- x-amz-copy-source-server-side-encryption-customer-key-MD5:ソースオブジェクトの作成時に指定したMD5ダイジェストを指定します。



指定した暗号化キーが格納されることはありません。暗号化キーを紛失すると、対応するオブジェクトが失われます。ユーザ指定のキーを使用してオブジェクトデータを保護する前に、の考慮事項を確認してください **"サーバ側の暗号化を使用します"**。

バージョン管理

マルチパートアップロードは、アップロードの開始、アップロードのリストの表示、パートのアップロード、アップロードしたパートのアセンブル、およびアップロードの完了の個別の処理に分けられます。CompleteMultipartUpload処理が実行されると、オブジェクトが作成されます（該当する場合はバージョン管理されます）。

エラー応答

StorageGRID システムでは、該当する S3 REST API の標準のエラー応答をすべてサポートしています。また、StorageGRID の実装では、カスタム応答もいくつか追加されています。

サポートされている **S3 API** のエラーコード

名前	HTTPステータス
アクセスが拒否されました	403 禁止
BadDigest の略	400 不正な要求です
BucketAlreadyExists のようになりました	409 競合
BucketNotEmpty のように入力します	409 競合
IncompleteBody	400 不正な要求です
内部エラー	500 Internal Server Error（内部サーバエラー）
InvalidAccessKeyId	403 禁止
アンヴァリッドドキュメント	400 不正な要求です
InvalidBucketName の略	400 不正な要求です
InvalidBucketState の場合	409 競合
InvalidDigest の略	400 不正な要求です
InvalidEncryptionAlgorithmError	400 不正な要求です
InvalidPart	400 不正な要求です
InvalidPartOrder	400 不正な要求です

名前	HTTPステータス
InvalidRange : 無効な範囲	416 リクエストされた範囲が適合しません
InvalidRequest	400 不正な要求です
InvalidStorageClass	400 不正な要求です
InvalidTag	400 不正な要求です
InvalidURI	400 不正な要求です
KeyTooLong の 2 つのグループがあります	400 不正な要求です
MalformedXML の場合	400 不正な要求です
MetadataTooLarge	400 不正な要求です
MethodNotAllowed のように入力します	405 メソッドは許可されていません
MissingContentLength (MissingContentLength)	411 長さが必要です
MissingRequestBodyError	400 不正な要求です
MissingSecurityHeader	400 不正な要求です
NoSuchBucket	404 が見つかりません
NoSuchKey	404 が見つかりません
NoSuchUpload	404 が見つかりません
実装なし	501 は実装されていません
NoSuchBucketPolicy のようになります	404 が見つかりません
ObjectLockConfigurationNotFoundError	404 が見つかりません
PreconditionalFailed	412 事前条件が失敗しました
RequestTimeTooSkewed	403 禁止
サービスを利用できません	503 Service Unavailable (503 サービスが利用でき

名前	HTTPステータス
SignatureDoesNotMatch のように指定します	403 禁止
TooManyBuckets	400 不正な要求です
UserKeyMustBeSpecified	400 不正な要求です

StorageGRID カスタムのエラーコード

名前	説明	HTTPステータス
XBucketLifecycleNotAllowed のようになり ました	バケットライフサイクル設定は従来の準拠 バケットには適用されません	400 不正な要求です
XBucketPolicyParseException	受信したバケットポリシー JSON を解析 できませんでした。	400 不正な要求です
XCompliConflict	準拠設定が古いため、処理が拒否されま した。	403 禁止
XCompliReducedRedundancyForbidden	レガシー準拠バケットでは冗長性の低下は 許可されません	400 不正な要求です
XMaxBucketPolicyLengthExceeded (XMaxBucketLengthExceeded)	ポリシーが許容される最大バケットポリシ ー長を超えています。	400 不正な要求です
XMissingInternalRequestHeader	内部要求のヘッダーがありません。	400 不正な要求です
XNoSuchBucketCompliance です	指定したバケットで従来の準拠が有効にな っていません。	404 が見つかりませ ん
XNotAcceptable	要求に含まれている Accept ヘッダーの 1 つ以上を満たすことができませんでした。	406 は許容されませ ん
XNotImplemented	指定した要求の処理には、実装されていな い機能が含まれます。	501 は実装されてい ません

StorageGRIDのカスタム処理

StorageGRIDのカスタム処理：概要

StorageGRIDシステムでは、S3 REST APIに追加されるカスタム処理をサポートしています。

次の表に、StorageGRIDでサポートされるカスタム処理を示します。

操作	説明
"GET Bucket consistency"	特定のバケットに適用されている整合性を返します。
"PUT Bucket consistency"	特定のバケットに適用する整合性を設定します。
"GET Bucket last access time の場合"	特定のバケットで最終アクセス時間の更新が有効になっているか無効になっているかを返します。
"PUT Bucket last access time のように指定します"	特定のバケットの最終アクセス時間の更新を有効または無効にできます。
"バケットのメタデータ通知設定を削除します"	特定のバケットに関連付けられているメタデータ通知設定 XML を削除します。
"GET Bucket metadata notification configuration"	特定のバケットに関連付けられているメタデータ通知設定 XML を返します。
"PUT Bucket metadata notification configuration のコマンドです"	バケットのメタデータ通知サービスを設定します。
"GET Storage Usage の略"	アカウントおよびアカウントに関連付けられている各バケットで使用されているストレージの総容量が表示されます。
"廃止予定：準拠設定を使用してCreateBucket"	廃止およびサポート終了：準拠を有効にした新しいバケットを作成できなくなりました。
"廃止予定：バケット準拠を取得します"	廃止されましたがサポートされています：既存の古い準拠バケットに対して現在有効な準拠設定を返します。
"廃止予定：PUT Bucket compliance"	廃止されましたがサポートされています：既存の古い準拠バケットの準拠設定を変更できます。

GET Bucket consistency

GET Bucket consistency要求を使用すると、特定のバケットに適用されている整合性を確認できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されません。

この処理を完了するには、s3: GetBucketConsistency権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

応答XMLで、<Consistency> は次のいずれかの値を返します。

整合性	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	(デフォルト) 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

応答例

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

PUT Bucket consistency

PUT Bucket consistency要求では、バケットで実行される処理に適用する整合性を指定できます。

デフォルトの整合性は、新規作成されたオブジェクトのリードアフターライトを保証するように設定されます。

作業を開始する前に

この処理を完了するには、s3:PutBucketConsistency権限またはrootアカウントが必要です。

リクエスト

。 x-ntap-sg-consistency パラメータには次のいずれかの値を指定する必要があります。

整合性	説明
すべて	すべてのノードが即座にデータを受け取り、受け取れない場合は要求が失敗します。
strong-global	すべてのサイトのすべてのクライアント要求について、リードアフターライト整合性が保証されます。
strong-site	1つのサイト内のすべてのクライアント要求について、リードアフターライト整合性が保証されます。
read-after-new-write の場合	(デフォルト) 新規オブジェクトにはリードアフターライト整合性を、オブジェクトの更新には結果整合性を提供します。高可用性が確保され、データ保護が保証されます。ほとんどの場合に推奨されます。
利用可能	新規オブジェクトとオブジェクトの更新の両方について結果整合性を提供します。S3バケットの場合は、必要な場合にのみ使用します（読み取り頻度の低いログ値を含むバケットや、存在しないキーに対するHEAD処理やGET処理など）。S3 FabricPool バケットではサポートされません。

*注：*一般に、「Read-after-new-write」整合性を使用する必要があります。要求が正しく動作しない場合は、可能であればアプリケーションクライアントの動作を変更します。または、API要求ごとに整合性を指定するようにクライアントを設定します。バケットレベルの整合性は最後の手段として設定してください。

要求例

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

関連情報

["整合性の値"](#)

GET Bucket last access time の場合

GET Bucket last access time 要求を使用すると、最終アクセス時間の更新が個々のバケットで有効になっているか無効になっているかを確認できます。

この処理を完了するには、s3:GetBucketLastAccessTime権限またはrootアカウントが必要です。

要求例

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

次の例では、バケットの最終アクセス時間の更新が有効になっています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket last access time のように指定します

PUT Bucket last access time 要求を使用すると、最終アクセス時間の更新を個々のバケットで有効または無効にできます。最終アクセス時間の更新を無効にするとパフォーマンスが向上します。バージョン 10.3.0 以降で作成されたバケットに対しては、いずれも

デフォルトで無効になります。

この処理を完了するには、バケットのs3:PutBucketLastAccessTime権限またはrootアカウントが必要です。



StorageGRID バージョン 10.3 以降では、すべての新規バケットで最終アクセス時間の更新がデフォルトで無効になります。以前のバージョンの StorageGRID で作成されたバケットにこの新たなデフォルトの動作を適用する場合は、対象となるバケットごとに最終アクセス時間の更新を無効にする必要があります。最終アクセス時間の更新を有効または無効にするには、PUT Bucket last access time要求を使用するか、Tenant Managerのバケットの詳細ページを使用します。を参照してください "[最終アクセス日時の更新を有効または無効にします](#)"。

バケットで最終アクセス時間の更新が無効になっている場合、バケットの処理の動作は次のようになります。

- GetObject、GetObjectAcl、GetObjectTagging、HeadObjectの各要求では、最終アクセス時間は更新されません。オブジェクトは、情報ライフサイクル管理（ILM）評価のキューに追加されません。
- メタデータのみを更新するCopyObject要求とPutObjectTagging要求では、最終アクセス時間も更新されません。オブジェクトは ILM 評価のキューに追加されます。
- ソースバケットで最終アクセス時間の更新が無効になっている場合、CopyObject要求でソースバケットの最終アクセス時間が更新されません。コピーされたオブジェクトは、ソースバケットの ILM 評価のキューに追加されません。ただし、デスティネーションについては、CopyObject要求で常に最終アクセス時間が更新されます。オブジェクトのコピーは、ILM 評価のキューに追加されます。
- CompleteMultipartUpload要求で最終アクセス時間が更新されます。完了したオブジェクトは、ILM 評価のキューに追加されます。

例をリクエストする

この例では、バケットの最終アクセス時間を有効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

この例では、バケットの最終アクセス時間を無効にしています。

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

バケットのメタデータ通知設定を削除します

DELETE Bucket metadata notification configuration 要求では、設定 XML を削除することで、個々のバケットで検索統合サービスを無効化できます。

この処理を完了するには、バケットのs3:DeleteBucketMetadataNotification権限またはrootアカウントが必要

です。

要求例

次の例は、バケットの検索統合サービスを無効にする方法を示しています。

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

GET Bucket metadata notification configuration

GET Bucket metadata notification configuration 要求では、個々のバケットで検索統合を設定するために使用する設定 XML を読み出すことができます。

この処理を完了するには、s3: GetBucketMetadataNotification権限またはrootアカウントが必要です。

要求例

次の要求は、というバケットのメタデータ通知設定を読み出します bucket。

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答

応答の本文には、バケットのメタデータ通知設定が含まれます。メタデータ通知設定では、バケットでの検索統合の設定を確認できます。つまり、どのオブジェクトにインデックスが付けられ、そのオブジェクトメタデータがどのエンドポイントに送信されるかを確認できます。

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

各メタデータ通知設定には、1つ以上のルールが含まれています。各ルールは、環境がオブジェクトを指定し、StorageGRIDがオブジェクトメタデータを送信するデスティネーションを指定します。デスティネーションは、StorageGRIDエンドポイントのURNを使用して指定する必要があります。

名前	説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。 1つ以上の Rule 要素を含みます。	はい。
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。 プレフィックスが重複しているルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれています。	はい。
ID	ルールの一意的識別子。 Rule 要素に含まれています。	いいえ
ステータス	Status には「Enabled」または「Disabled」を指定できます。無効になっているルールについては操作が実行されません。 Rule 要素に含まれています。	はい。

名前	説明	必須
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのコンテナタグ。</p> <p>Rule 要素に含まれています。</p>	はい。
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> • es 3番目のエレメントである必要があります。 • URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります <code>domain-name/myindex/mytype</code>。 <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

応答例

間に含まれるXML

<MetadataNotificationConfiguration></MetadataNotificationConfiguration> タグは、バケットに対して検索統合エンドポイントとの統合がどのように設定されているかを示します。次の例では、という名前のElasticsearchインデックスにオブジェクトメタデータが送信されています `current` と入力します `2017` という名前のAWSドメインでホストされている `records`。

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml
```

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:33333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

["テナントアカウントを使用する"](#)

PUT Bucket metadata notification configuration のコマンドです

PUT Bucket metadata notification configuration 要求を使用すると、個々のバケットで検索統合サービスを有効化できます。要求の本文に含めるメタデータ通知設定 XML では、デスティネーション検索インデックスにメタデータを送信するオブジェクトを指定します。

この処理を完了するには、バケットのs3:PutBucketMetadataNotification権限またはrootアカウントが必要です。

リクエスト

要求の本文にメタデータ通知設定が含まれている必要があります。各メタデータ通知設定には、1つ以上のルールが含まれています。各ルールは、環境がオブジェクトを指定し、StorageGRIDがオブジェクトメタデータを送信するデスティネーションを指定します。

オブジェクトはオブジェクト名のプレフィックスでフィルタリングできます。たとえば、というプレフィックスのオブジェクトのメタデータを送信できます /images を1つのデスティネーションに、プレフィックスがのオブジェクトに追加します /videos 別のノードに移動します

プレフィックスが重複している設定は有効ではなく、送信時に拒否されます。たとえば、プレフィックスがのオブジェクト用のルールを1つ含む設定などです test プレフィックスが付いたオブジェクトの2番目のルールです test2 許可されません。

デスティネーションは、StorageGRID エンドポイントの URN を使用して指定する必要があります。エンドポイントは、メタデータ通知設定が送信されたときに存在している必要があります。存在していない場合、要求がとして失敗します 400 Bad Request。エラーメッセージ：Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

次の表に、メタデータ通知設定 XML の要素を示します。

名前	説明	必須
MetadataNotificationConfiguration のページです	メタデータ通知でオブジェクトとデスティネーションの指定に使用されるルール用のコンテナタグ。 1 つ以上の Rule 要素を含みます。	はい。
ルール	指定したインデックスにメタデータを追加する必要があるオブジェクトを特定するルール用のコンテナタグ。 プレフィックスが重複しているルールは拒否され ます。 MetadataNotificationConfiguration 要素に含まれて います。	はい。
ID	ルールの一意的識別子。 Rule 要素に含まれています。	いいえ

名前	説明	必須
ステータス	<p>Status には「Enabled」または「Disabled」を指定できます。無効になっているルールについては操作が実行されません。</p> <p>Rule 要素に含まれています。</p>	はい。
プレフィックス	<p>プレフィックスと一致するオブジェクトにルールが適用され、そのメタデータが指定したデスティネーションに送信されます。</p> <p>すべてのオブジェクトを照合するには、空のプレフィックスを指定します。</p> <p>Rule 要素に含まれています。</p>	はい。
宛先	<p>ルールのデスティネーションのテナントタグ。</p> <p>Rule 要素に含まれています。</p>	はい。
URN	<p>オブジェクトメタデータが送信されるデスティネーションの URN。次のプロパティを持つ StorageGRID エンドポイントの URN を指定する必要があります。</p> <ul style="list-style-type: none"> • es 3番目のエレメントである必要があります。 • URNの末尾に、メタデータが格納されるインデックスとタイプを、の形式で指定する必要があります <code>domain-name/myindex/mytype</code>。 <p>エンドポイントは、Tenant Manager またはテナント管理 API を使用して設定します。形式は次のとおりです。</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>エンドポイントは設定 XML を送信する前に設定する必要があります。そうしないと、404 エラーで設定が失敗します。</p> <p>Urn は Destination 要素に含まれています。</p>	はい。

例をリクエストする

次の例は、バケットの検索統合を有効にする方法を示しています。この例では、すべてのオブジェクトのオブジェクトメタデータが同じデスティネーションに送信されます。

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

この例では、プレフィックスに一致するオブジェクトのオブジェクトメタデータを指定します。/images が1つのデスティネーションに送信され、プレフィックスに一致するオブジェクトのオブジェクトメタデータが送信されます。/videos 2番目の送信先に送信されます。

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

検索統合サービスで生成される JSON

バケットで検索統合サービスを有効にすると、オブジェクトのメタデータまたはタグの追加、更新、削除が行われるたびに、JSON ドキュメントが生成されてデスティネーションエンドポイントに送信されます。

次の例は、キーを含むオブジェクトの場合に生成されるJSONを示しています。SGWS/Tagging.txt は、という名前のバケットに作成されます test。 test バケットはバージョン管理されていないため、を使用します versionId タグが空です。


```

{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}

```

メタデータ通知に含まれているオブジェクトメタデータ

次の表に、検索統合が有効になっている場合にデスティネーションエンドポイントに送信される JSON ドキュメント内のすべてのフィールドを示します。

ドキュメント名には、バケット名、オブジェクト名、バージョン ID（存在する場合）が含まれます。

を入力します	項目名	説明
バケットとオブジェクトの情報	バケット	バケットの名前
バケットとオブジェクトの情報	キーを押します	オブジェクトキーの名前
バケットとオブジェクトの情報	versionId	バージョン管理されたバケット内のオブジェクトのオブジェクトバージョン
バケットとオブジェクトの情報	リージョン	たとえば、バケットのリージョンのように指定します us-east-1
システムメタデータ	サイズ	HTTP クライアントから認識できるオブジェクトのサイズ（バイト）
システムメタデータ	MD5	オブジェクトのハッシュ
ユーザメタデータ	メタデータ <i>key:value</i>	オブジェクトのすべてのユーザメタデータをキーと値のペアとして格納

を入力します	項目名	説明
タグ	タグ <i>key:value</i>	オブジェクトに対して定義されたすべてのオブジェクトタグをキーと値のペアとして使用します



タグとユーザメタデータの場合、StorageGRID は文字列または S3 イベント通知として Elasticsearch に日付と番号を渡します。これらの文字列を日付または数値として解釈するように Elasticsearch を設定するには、動的フィールドマッピングおよびマッピング日付形式に関する Elasticsearch の手順に従ってください。検索統合サービスを設定する前に、インデックスの動的フィールドマッピングを有効にする必要があります。ドキュメントのインデックス作成後は、インデックス内のドキュメントのフィールドタイプを編集することはできません。

関連情報

["テナントアカウントを使用する"](#)

GET Storage Usage 要求の略

GET Storage Usage 要求を使用すると、アカウントで使用しているストレージの総容量とアカウントに関連付けられているバケットごとの使用容量を確認できます。

アカウントとそのバケットで使用されているストレージの容量は、`x-ntap-sg-usage` クエリパラメータ。バケットによるストレージの使用量は、システムで処理される PUT 要求や DELETE 要求とは別に追跡されません。特にシステムの負荷が高い場合などは、使用量の値が要求の処理に基づく想定値と同じになるまでに少し時間がかかることがあります。

デフォルトでは、StorageGRID は strong-global 整合性を使用して、使用状況の情報を取得します。strong-global 整合性を達成できない場合、StorageGRID は strong-site 整合性で使用状況情報を取得しようとします。

この処理を完了するには、`s3:ListAllMyBuckets` 権限または root アカウントが必要です。

要求例

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

次の例は、2つのバケットに4つのオブジェクトと12バイトのデータが格納されたアカウントです。各バケットには、2つのオブジェクトと6バイトのデータが格納されています。

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

バージョン管理

には、格納されているすべてのオブジェクトバージョンが関連します ObjectCount および DataBytes 応答の値。削除マーカには追加されません ObjectCount 合計。

関連情報

["整合性の値"](#)

従来の準拠のためのバケット要求が廃止されました

従来の準拠のためのバケット要求が廃止されました

従来の準拠機能で作成されたバケットの管理には、StorageGRID S3 REST API の使用が必要になる場合があります。

コンプライアンス機能は廃止されました

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。

グローバル準拠設定を有効にしている場合は、StorageGRID 11.6 でグローバル S3 オブジェクトロック設定が有効になっています。準拠を有効にした新しいバケットは作成できなくなりました。ただし、必要に応じて、StorageGRID S3 REST API を使用して、従来の準拠バケットを管理できます。

- ["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)
- ["ILM を使用してオブジェクトを管理する"](#)
- ["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

廃止された準拠要求：

- ["DEPRECATED - PUT Bucket request modifications for compliance"](#)

SGCompliance XML 要素は廃止されました。これまでは、この StorageGRID カスタム要素を PUT Bucket 要求のオプションの XML 要求の本文に含めて準拠バケットを作成できました。

- ["廃止予定- GET Bucket compliance"](#)

GET Bucket compliance要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

- ["廃止されました。PUT Bucket compliance"](#)

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

廃止予定：準拠のための**CreateBucket**要求の変更

SGCompliance XML 要素は廃止されました。以前は、このStorageGRIDカスタム要素をCreateBucket要求のオプションのXML要求本文に含めて、準拠バケットを作成できました。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。



- ["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)
- ["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

準拠を有効にした新しいバケットを作成することはできなくなりました。準拠のためにCreateBucket要求の変更を使用して新しい準拠バケットを作成しようとすると、次のエラーメッセージが返されます。

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

廃止予定：GET Bucket compliance要求

GET Bucket compliance要求は廃止されました。ただし、既存のレガシー準拠バケットに対して現在有効な準拠設定を引き続き確認することができます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。



- ["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)
- ["ネットアップのナレッジベース：StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

この処理を完了するには、s3：GetBucketCompliance権限またはrootアカウントが必要です。

要求例

次の要求例では、という名前のバケットの準拠設定を確認できます mybucket。

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

応答例

応答XMLで、<SGCompliance>バケットで有効な準拠設定が表示されます。次の応答例では、バケットの準拠設定が示されており、各オブジェクトはグリッドに取り込まれてから1年間（525、600分）保持されます。このバケットには現在リーガルホールドはありません。各オブジェクトは1年後に自動的に削除されません。

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>
```

名前	説明
RetentionPeriodMinutes です	このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。
LegalHold のようになります	<ul style="list-style-type: none"> • True : このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。 • False : このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。
自動削除	<ul style="list-style-type: none"> • True : このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false : このバケット内のオブジェクトは、保持期間が過ぎても自動的に削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。

エラー応答

バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found`を返します `XNoSuchBucketCompliance。

廃止予定： PUT Bucket compliance 要求

PUT Bucket compliance 要求は廃止されました。ただし、この要求を引き続き使用して、既存のレガシー準拠バケットの準拠設定を変更できます。たとえば、既存のバケットをリーガルホールドの対象にしたり、バケットの保持期間を長くしたりできます。

以前のバージョンの StorageGRID で提供されていた StorageGRID 準拠機能は廃止され、S3 オブジェクトロックに置き換えられました。詳細については、次を参照してください。



- ["S3 REST APIを使用してS3オブジェクトロックを設定します"](#)
- ["ネットアップのナレッジベース： StorageGRID 11.5 でレガシー準拠バケットを管理する方法"](#)

この処理を完了するには、s3:PutBucketCompliance権限またはrootアカウントが必要です。

PUT Bucket compliance 要求を発行する際は、準拠設定のすべてのフィールドに値を指定する必要があります。

要求例

次の要求例では、という名前のバケットの準拠設定を変更します mybucket。この例では、のオブジェクトが表示されています mybucket オブジェクトがグリッドに取り込まれてから1年間ではなく2年間（1、051、200分）保持されます。このバケットにリーガルホールドはありません。各オブジェクトは2年後に自動的に削除されます。

```

PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>

```

名前	説明
RetentionPeriodMinutes です	<p>このバケットに追加されたオブジェクトの保持期間を分で指定します。保持期間は、オブジェクトがグリッドに取り込まれたときからの期間です。</p> <p>重要 RetentionPeriodMinutesに新しい値を指定する場合は、バケットの現在の保持期間以上の値を指定する必要があります。バケットの保持期間の設定後は、その値を減らすことはできず、増やすことしかできません。</p>
LegalHold のようになります	<ul style="list-style-type: none"> • True : このバケットは、現在リーガルホールドの対象です。このバケット内のオブジェクトは、保持期間が過ぎても、リーガルホールドが解除されるまで削除できません。 • False : このバケットは、現在リーガルホールドの対象ではありません。このバケット内のオブジェクトは、保持期間が過ぎたら削除できます。
自動削除	<ul style="list-style-type: none"> • True : このバケット内のオブジェクトは、バケットがリーガルホールドの対象である場合を除き、保持期間が過ぎると自動的に削除されます。 • false : このバケット内のオブジェクトは、保持期間が過ぎても自動的に削除されません。これらのオブジェクトを削除する必要がある場合は、手動で削除する必要があります。

準拠設定の整合性

PUT Bucket compliance 要求によって S3 バケットの準拠設定を更新すると、StorageGRID は、グリッド全体のバケットのメタデータを更新しようとします。デフォルトでは、StorageGRIDは* strong-global *整合性を使用して、バケットのメタデータを含むすべてのデータセンターサイトとストレージノードで、変更された準拠設定のリードアフターライト整合性を保証します。

データセンターサイトまたはサイトの複数のストレージノードが利用できないために、StorageGRIDが* strong-global *整合性を達成できない場合、応答のHTTPステータスコードは次のようになります。 503 Service Unavailable.

この応答を受け取った場合は、必要なストレージサービスをできるだけ早く利用可能にするために、グリッド管理者に問い合わせる必要があります。グリッド管理者が各サイトで十分な数のストレージノードを利用可能にできない場合、テクニカルサポートから* strong-site *整合性を強制的に適用して、失敗した要求を再試行するよう指示されることがあります。



テクニカルサポートから指示され、このレベルを使用した場合の潜在的な影響を理解している場合を除き、PUT bucket complianceで* strong-site *整合性を強制的に実行しないでください。

整合性を* strong-site *に減らすと、StorageGRIDは、サイト内のクライアント要求についてのみ、更新された準拠設定のリードアフターライト整合性を保証します。そのため、すべてのサイトおよびストレージノードが利用可能になるまでの間、StorageGRID システムにはこのバケットに対して複数の異なる設定が一時的に存在することになる場合があります。整合性のない設定を使用すると、予期せぬ望ましくない動作が生じる可能性がありますたとえば、バケットをリーガルホールドの対象にする場合に、より低い整合性を強制的に適用すると、一部のデータセンターサイトでバケットの以前の準拠設定（リーガルホールドのオフ）が引き続き有効になることがあります。したがって、リーガルホールドの対象と思われるオブジェクトは、保持期間が経過すると、ユーザによって削除される場合と、AutoDelete によって削除される場合があります。

strong-site *整合性を強制的に使用するには、PUT Bucket compliance要求を再実行し、Consistency-Control HTTP要求ヘッダー。

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

エラー応答

- バケットが準拠バケットとして作成されていない場合、応答のHTTPステータスコードはになります 404 Not Found。
- 状況 RetentionPeriodMinutes 要求がバケットの現在の保持期間よりも短い場合、HTTPステータスコードはになります 400 Bad Request。

関連情報

["廃止：準拠のための PUT Bucket 要求の変更"](#)

バケットとグループのアクセスポリシー

バケットとグループのアクセスポリシーを使用

StorageGRID では、Amazon Web Services（AWS）ポリシー言語を使用して、S3 テナントによるバケットおよびバケット内のオブジェクトへのアクセスを制御できます。StorageGRID システムには、S3 REST API ポリシー言語のサブセットが実装されています。S3 API のアクセスポリシーは JSON 形式で記述されます。

アクセスポリシーの概要

StorageGRID では 2 種類のアクセスポリシーがサポートされています。

- バケットポリシー。S3 APIのGetBucketPolicy、PutBucketPolicy、およびDeleteBucketPolicyの各処理を使

用して管理されます。バケットポリシーはバケットに関連付けられ、バケットとそのオブジェクトへのバケット所有者アカウントやその他のアカウントのユーザによるアクセスを制御するために使用されます。バケットポリシー環境は1つのバケットのみで、場合によっては複数のグループに分かれています。

- * グループポリシー *。Tenant Manager またはテナント管理 API を使用して設定します。グループポリシーはアカウントのグループに関連付けられ、そのアカウントが所有する特定のリソースにそのグループがアクセスできるように設定されます。グループポリシー環境は1つのグループに限定され、場合によっては複数のバケットに適用されます。



グループポリシーとバケットポリシーの優先度に違いはありません。

StorageGRID のバケットとグループのポリシーは、Amazon が定義している特定の文法に従って記述されます。各ポリシーは一連のステートメントからなり、各ステートメントは次の要素で構成されます。

- ステートメント ID (SID) (オプション)
- 効果
- プリンシパル / NotPrincipal
- リソース / メモリソース
- アクション / NotAction
- Condition (オプション)

次の構造を使用して、権限を指定するポリシーステートメントが構築されます。 <Effect> を付与して、 <Condition> に該当する場合に <Principal> に <Resource> に対する <Action> の実行を許可または拒否します。

各ポリシー要素は、特定の機能に使用されます。

要素 (Element)	説明
SID	Sid 要素はオプションです。SID は、ユーザの概要としてのみ使用されます。StorageGRID システムに格納はされますが、システムで解釈されません。
効果	Effect 要素では、指定した処理を許可するか拒否するかを指定します。Action 要素でサポートされるキーワードを使用して、バケットやオブジェクトで許可 (または拒否) する処理を指定する必要があります。
プリンシパル / NotPrincipal	ユーザ、グループ、およびアカウントに特定のリソースへのアクセスと特定の操作の実行を許可できます。要求に S3 の署名が含まれていない場合は、ワイルドカード文字 (*) をプリンシパルとして指定することで匿名アクセスが許可されます。デフォルトでは、アカウントが所有するリソースへのアクセスは root アカウントにのみ許可されます。 Principal 要素を指定する必要があるのはバケットポリシーだけです。グループポリシーの場合は、ポリシーが関連付けられたグループが暗黙的にプリンシパルになります。

要素 (Element)	説明
リソース / メモリソース	Resource 要素では、バケットとオブジェクトを指定します。Amazon リソースネーム (ARN) を使用してリソースを指定し、バケットやオブジェクトに対する権限を許可または拒否することができます。
アクション / NotAction	権限は Action 要素と Effect 要素の 2 つで構成されます。グループがリソースを要求すると、リソースへのアクセスが許可または拒否されます。権限を明示的に割り当てていないかぎりアクセスは拒否されますが、明示的な拒否を使用して別のポリシーで付与された権限を上書きすることもできます。
条件	Condition 要素はオプションです。条件を使用すると、ポリシーを適用する条件を示す式を作成できます。

Action 要素では、ワイルドカード文字 (*) を使用してすべての処理または処理のサブセットを指定できます。たとえば、次の Action の値は、s3 : GetObject、s3 : PutObject、s3 : DeleteObject などの権限に一致します。

```
s3:*Object
```

Resource 要素では、ワイルドカード文字 (*) および (?) を使用できます。アスタリスク (*) は 0 文字以上の文字に一致し、疑問符 (?) は 0 文字以上の文字に一致します。任意の 1 文字に一致します。

Principal要素では、匿名アクセスを設定してすべてのユーザに権限を付与する場合を除き、ワイルドカード文字はサポートされません。たとえば、Principal の値としてワイルドカード (*) を設定します。

```
"Principal": "*"

```

```
"Principal":{"AWS":"*"

```

次の例では、Effect、Principal、Action、および Resource の各要素を使用して記述します。次の例は、「許可」の効果を使用してプリンシパル、adminグループを指定したバケットポリシーのステートメントを示しています federated-group/admin 財務グループなどです federated-group/finance、アクションを実行する権限 s3:ListBucket をバケットにインストールします mybucket そしてアクション s3:GetObject そのバケット内のすべてのオブジェクト。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3::mybucket",
        "arn:aws:iam:s3::mybucket/*"
      ]
    }
  ]
}

```

バケットポリシーのサイズの上限は 20、480 バイトで、グループポリシーのサイズの上限は 5、120 バイトです。

ポリシーノセイクウセイ

デフォルトでは、グループポリシーに対するすべての更新の整合性レベルは結果整合性です。グループポリシーの整合性が取れた場合、ポリシーキャッシュのために変更が有効になるまでにさらに15分かかることがあります。デフォルトでは、バケットポリシーに対する更新の整合性は非常に高くなります。

バケットポリシーの更新の整合性保証は必要に応じて変更できます。たとえば、サイトが停止しているときにバケットポリシーを変更できるようにすることができます。

この場合は、を設定できます `Consistency-Control PutBucketPolicy`要求のヘッダー、またはPUT Bucket `consistency`要求を使用できます。バケットポリシーの整合性が確保されると、ポリシーキャッシュのために変更が有効になるまでにさらに8秒かかることがあります。



一時的な状況を回避するために整合性の値を別の値に設定する場合は、完了後にバケットレベルの設定を元の値に戻してください。そうしないと、以降のすべてのバケット要求で変更後の設定が使用されます。

ポリシーステートメントでは **ARN** を使用します

ポリシーステートメントでは、Principal 要素と Resource 要素で ARN を使用します。

- S3 リソースの ARN の指定には次の構文を使用します。

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- アイデンティティリソースの ARN（ユーザおよびグループ）の指定には次の構文を使用します。

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

その他の考慮事項：

- オブジェクトキーの一部にワイルドカードとしてアスタリスク（*）を使用すると、0文字以上の文字に一致します。
- オブジェクトキーで指定できる国際文字は、JSON UTF-8 形式または JSON \u エスケープシーケンスを使用してエンコードする必要があります。パーセントエンコーディングはサポートされていません。

"RFC 2141 の URN 構文"

PutBucketPolicy処理のHTTP要求の本文は、charset=UTF-8でエンコードする必要があります。

ポリシー内のリソースを指定します

ポリシーステートメントでは、Resource 要素を使用して、権限を許可または拒否するバケットやオブジェクトを指定できます。

- Resource 要素はポリシーの各ステートメントに必要です。ポリシーでは、リソースは要素で示されます Resource または、`NotResource` 除外のため。
- リソースは S3 リソースの ARN で指定します。例：

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- オブジェクトキーの内部でポリシー変数を使用することもできます。例：

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- グループポリシーの作成時は、まだ存在しないバケットもリソースの値で指定することができます。

ポリシーでプリンシパルを指定します

ポリシーステートメントでリソースへのアクセスを許可または拒否するユーザ、グループ、またはテナントアカウントを指定するには、Principal 要素を使用します。

- バケットポリシーの各ポリシーステートメントには、Principal 要素を含める必要があります。グループはプリンシパルとみなされるため、グループポリシーのポリシーステートメントではPrincipal要素は必要ありません。
- ポリシーでは、「Principal」要素または「NotPrincipal」要素（除外の場合）でプリンシパルを指定します。
- ID または ARN を使用してアカウントベースのアイデンティティを指定する必要があります。

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- 次の例では、テナントアカウント ID 27233906934684427525 を使用しています。この場合、root アカウントとそのすべてのユーザが含まれます。

```
"Principal": { "AWS": "27233906934684427525" }
```

- root アカウントのみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- 特定のフェデレーテッドユーザ（「Alex」）を指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- 特定のフェデレーテッドグループ（「Managers」）のみを指定する場合は次のようになります。

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- 匿名プリンシパルを指定する場合は次のようになります。

```
"Principal": "*" 
```

- あいまいさを排除するために、ユーザ名の代わりに UUID を使用できます。

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-  
eb6b9e546013
```

たとえば、Alexが組織とユーザ名を退職するとします Alex が削除されました。新しいAlexが組織に参加

し、同じが割り当てられている場合 Alex ユーザ名。元のユーザに付与された権限が、新しいユーザに意図せず継承されることがあります。

- バケットポリシーの作成時は、まだ存在しないグループ / ユーザの名前もプリンシパルの値で指定することができます。

ポリシーで権限を指定します

ポリシーでは、Action 要素を使用してリソースに対する権限を許可または拒否します。ポリシーには、「Action」要素で示される一連の権限、または除外する「NotAction」要素で指定できる一連の権限があります。それぞれが特定の S3 REST API 処理に対応しています。

次の表に、バケットに適用される権限とオブジェクトに適用される権限を示します。



Amazon S3では、PutBucketReplicationとDeleteBucketReplicationの両方のアクションにs3 : PutReplicationConfiguration権限が使用されるようになりました。StorageGRID では、元の Amazon S3 仕様に一致する個別の権限が各アクションに使用されます。



DELETEは、PUTを使用して既存の値を上書きした場合に実行されます。

バケットに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : CreateBucket を指定します	CreateBucketを選択します	はい。 注：グループポリシーでのみ使用します。
S3 : DeleteBucket	DeleteBucketの場合	
S3 : DeleteBucketMetadataNotification	バケットのメタデータ通知設定を削除します	はい。
S3 : DeleteBucketPolicy	DeleteBucketPolicyのようになります	
S3 : DeleteReplicationConfiguration	DeleteBucketReplication	○ (PUTとDELETEに別々の権限を設定)
S3 : GetBucketAcl	GetBucketAcl	
S3 : GetBucketCompliance	GET Bucket compliance (廃止)	はい。
S3 : GetBucketConsistency	GET Bucket consistency	はい。

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : GetBucketCORS	GetBucketCors	
S3 : GetEncryptionConfiguration	GetBucketEncryptionの略	
S3 : GetBucketLastAccessTime	GET Bucket last access time の場合	はい。
S3 : GetBucketLocation	GetBucketLocation	
S3 : GetBucketMetadataNotification	GET Bucket metadata notification configuration	はい。
S3 : GetBucketNotification	GetBucketNotificationConfigurationを参照してください	
S3 : GetBucketObjectLockConfiguration	GetObjectLockConfigurationの略	
S3 : GetBucketPolicy	GetBucketPolicyのようになります	
S3 : GetBucketTagging	GetBucketTagging	
S3 : GetBucketVersioning	GetBucketVersioningの各ノードの設定	
S3 : GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
S3 : GetReplicationConfiguration	GetBucketReplicationの略	
S3 : ListAllMyBuckets	<ul style="list-style-type: none"> • ListBuckets • GET Storage Usage の略 	<p>○ (GET Storage Usage) 。</p> <p>注：グループポリシーでのみ使用しません。</p>
S3 : ListBucket	<ul style="list-style-type: none"> • ListObjects • ヘッドバケット • RestoreObject 	
S3 : ListBucketMultipartUploads	<ul style="list-style-type: none"> • ListMultipartUploads • RestoreObject 	
S3 : ListBucketVersions	GET Bucket versions (バケットバージョンの取得)	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutBucketCompliance	PUT Bucket compliance (廃止)	はい。
S3 : PutBucketConsistency	PUT Bucket consistency	はい。
S3 : PutBucketCORS	<ul style="list-style-type: none"> • DeleteBucketCors† • PutBucketCorsの略 	
S3 : PutEncryptionConfiguration	<ul style="list-style-type: none"> • DeleteBucketEncryption • PutBucketEncryptionの略 	
S3 : PutBucketLastAccessTime	PUT Bucket last access time のように指定します	はい。
S3 : PutBucketMetadataNotification	PUT Bucket metadata notification configuration のコマンドです	はい。
S3 : PutBucketNotification	PutBucketNotificationConfigurationの略	
S3 : PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> • を使用してCreateBucketを作成します。 x-amz-bucket-object-lock-enabled: true 要求ヘッダー (s3 : CreateBucket権限も必要) • PutObjectLockConfigurationの略 	
S3 : PutBucketPolicy	PutBucketPolicyのように指定します	
S3 : PutBucketTagging	<ul style="list-style-type: none"> • DeleteBucketTagging† • PutBucketTaggingの略 	
S3 : PutBucketVersioning	PutBucketVersioningの各ノードの設定	
S3 : PutLifecycleConfiguration	<ul style="list-style-type: none"> • DeleteBucketLifecycle† • PutBucketLifecycleConfigurationの略 	
S3 : PutReplicationConfiguration	PutBucketReplicationの略	○ (PUTとDELETEに別々の権限を設定)

オブジェクトに適用される権限

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : AbortMultipartUpload	<ul style="list-style-type: none"> AbortMultipartUpload の略 RestoreObject 	
S3 : Bypassガバナー 保持	<ul style="list-style-type: none"> deleteObject オブジェクトを削除します PutObjectRetentionの略 	
S3 : DeleteObject	<ul style="list-style-type: none"> deleteObject オブジェクトを削除します RestoreObject 	
S3 : DeleteObjectTagging	DeleteObjectTagging の場合	
S3 : DeleteObjectVersionTagging	DeleteObjectTagging (オブジェクトの特定のバージョン)	
S3 : DeleteObjectVersion	deleteObject (オブジェクトの特定のバージョン)	
S3 : GetObject	<ul style="list-style-type: none"> GetObject HeadObject (ヘッドオブジェクト) RestoreObject SelectObjectContent の順に選択します 	
S3 : GetObjectAcl	GetObjectAcl	
S3 : GetObjectLegalHold	GetObjectLegalHold	
S3 : GetObjectRetention	GetObjectRetentionの略	
S3 : GetObjectTagging	GetObjectTagging の 2 つの機能を	
S3 : GetObjectVersionTagging	GetObjectTagging (オブジェクトの特定のバージョン)	
S3 : GetObjectVersion	GetObject (オブジェクトの特定のバージョン)	
S3 : ListMultipartUploadParts	ListParts、RestoreObject	

権限	S3 REST API の処理	StorageGRID のカスタム
S3 : PutObject	<ul style="list-style-type: none"> • PutObject • CopyObject • RestoreObject • CreateMultipartUpload を実行します • CompleteMultipartUpload • UploadPart のアップロード • UploadPartCopyをクリックします 	
S3 : PutObjectLegalHold	PutObjectLegalHold	
S3 : PutObjectRetention	PutObjectRetentionの略	
S3 : PutObjectTagging	PutObjectTagging の 2 つのグループが	
S3 : PutObjectVersionTagging	PutObjectTagging (オブジェクトの特定のバージョン)	
S3 : PutOverwriteObject	<ul style="list-style-type: none"> • PutObject • CopyObject • PutObjectTagging の 2 つのグループが • DeleteObjectTagging の場合 • CompleteMultipartUpload 	はい。
S3 : RestoreObject	RestoreObject	

PutOverwriteObject 権限を使用します

s3 : PutOverwriteObject 権限は、オブジェクトの作成または更新を行う環境 処理のカスタムの StorageGRID 権限です。この権限の設定により、オブジェクトのデータ、ユーザ定義メタデータ、または S3 オブジェクトのタグをクライアントが上書きできるかどうかが決まります。

この権限で可能な設定は次のとおりです。

- * allow * : クライアントはオブジェクトを上書きできます。これがデフォルト設定です。
- **Deny**: クライアントはオブジェクトを上書きできません。PutOverwriteObject 権限が Deny に設定されている場合の動作は次のとおりです。
 - 同じパスで既存のオブジェクトが見つかった場合は、次の手順を実行します。
 - オブジェクトのデータ、ユーザ定義メタデータ、またはS3オブジェクトのタグを上書きすることはできません。
 - 実行中の取り込み処理はすべてキャンセルされ、エラーが返されます。

- S3のバージョン管理が有効になっている場合は、Denyに設定すると、PutObjectTagging処理またはDeleteObjectTagging処理によってオブジェクトとその最新でないバージョンのTagSetが変更されなくなります。
- 既存のオブジェクトが見つからない場合は、この権限の設定は影響しません。
- この権限がない場合、Allow が設定されたものと同じ結果になります。



現在のS3ポリシーで上書きが許可されていて、PutOverwriteObject権限がDenyに設定されている場合、オブジェクトのデータ、ユーザ定義メタデータ、またはオブジェクトのタグをクライアントが上書きすることはできません。また、**[Prevent client modification]***チェックボックスが選択されている場合（configuration > Security settings > Network and objects *）、この設定はPutOverwriteObject権限の設定よりも優先されます。

ポリシーの条件を指定します

条件は、ポリシーが有効になるタイミングを定義します。条件は演算子とキーと値のペアで構成されます。

条件はキーと値のペアを使用して評価されます。Condition 要素には複数の条件を指定でき、各条件には複数のキーと値のペアを含めることができます。条件ブロックの形式は次のとおりです。

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

次の例では、IpAddress 条件で SourceIp 条件キーを使用しています。

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

サポートされる条件演算子は次の

条件演算子は次のように分類されます。

- 文字列
- 数値
- ブール値
- IP アドレス
- Null チェック

条件演算子	説明
StringEquals	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別あり）。
StringNotEquals	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別あり）。
StringEqualsIgnoreCase	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別なし）。
StringNotEqualsIgnoreCase	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別なし）。
StringLike	キーを文字列値と比較し、完全一致であることを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
StringNotLike	キーを文字列値と比較し、不一致であることを確認します（大文字と小文字の区別あり）。含めることができる * と ? ワイルドカード文字を使用できます。
NumericEquals (数値機器)	キーを数値と比較し、完全一致であることを確認します。
NumericNotEquals	キーを数値と比較し、不一致であることを確認します。
NumericGreaterThan	キーを数値と比較し、「より大きい」の一致であるかどうかを確認します。
NumericGreaterThanEquals	キーを数値と比較し、「以上」の一致であるかどうかを確認します。
NumericLessThan	キーを数値と比較し、「より小さい」一致であることを確認します。
NumericLessThanEquals	キーを数値と比較し、「小なり」の一致であることを確認します。
ブール値	キーをブール値と比較し、「trueまたはfalse」の一致であることを確認します。
IP アドレス	キーを IP アドレスまたは IP アドレスの範囲と比較します。
NotIpAddress	キーを IP アドレスまたは IP アドレスの範囲と比較し、不一致であることを確認します。
null	現在の要求コンテキストに条件キーが存在するかどうかを確認します。

サポートされている条件キー

Conditionキー	アクション	説明
AWS : sourceIP	IP 演算子	<p>要求の送信元の IP アドレスと比較します。バケットまたはオブジェクトの処理に使用できます。</p> <ul style="list-style-type: none"> • 注 : S3 要求が管理ノードおよびゲートウェイノード上のロードバランササービスを介して送信された場合は、ロードバランササービスのアップストリームの IP アドレスと比較します。 • 注 * : サードパーティ製の非透過型ロードバランサを使用する場合は、そのロードバランサの IP アドレスと比較します。任意 X-Forwarded-For ヘッダーの有効性を確認できないため、ヘッダーは無視されます。
AWS : ユーザ名	リソース / ID	<p>要求の送信者のユーザ名と比較します。バケットまたはオブジェクトの処理に使用できます。</p>
S3 : デリミタ	<p>S3 : ListBucket と</p> <p>S3 : ListBucketVersions 権限</p>	<p>ListObjects要求またはListObjectVersions要求で指定されたdelimiterパラメータと比較します。</p>

Conditionキー	アクション	説明
S3 : ExistingObjectTag /<tag-key>	<p>S3 : DeleteObjectTagging</p> <p>S3 : DeleteObjectVersionTagging</p> <p>S3 : GetObject</p> <p>S3 : GetObjectAcl</p> <p>S3 : GetObjectTagging</p> <p>S3 : GetObjectVersion</p> <p>S3 : GetObjectVersionAcl</p> <p>S3 : GetObjectVersionTagging</p> <p>S3 : PutObjectAcl</p> <p>S3 : PutObjectTagging</p> <p>S3 : PutObjectVersionAcl</p> <p>S3 : PutObjectVersionTagging</p>	既存のオブジェクトに特定のタグキーと値が必要になります。
S3 : max-keys	<p>S3 : ListBucket と</p> <p>S3 : ListBucketVersions 権限</p>	ListObjects要求またはListObjectVersions要求で指定されたmax-keysパラメータと比較します。
S3 : object-lock-remaining-retention-days	S3 : PutObject	<p>で指定されたretain-until-dateと比較します x-amz-object-lock-retain-until-date 次の要求について、これらの値が許容範囲内であることを確認するために、要求ヘッダーまたはバケットのデフォルト保持期間から計算されます。</p> <ul style="list-style-type: none"> • PutObject • CopyObject • CreateMultipartUpload を実行します
S3 : object-lock-remaining-retention-days	S3 : PutObjectRetention	は、PutObjectRetention要求で指定されたretain-until-dateと比較して、許容範囲内であることを確認します。

Conditionキー	アクション	説明
S3 : プレフィックス	S3 : ListBucket と S3 : ListBucketVersions 権限	ListObjects要求またはListObjectVersions要求で指定されたprefixパラメータと比較します。
S3 : RequestObjectTag /<tag-key>	S3 : PutObject S3 : PutObjectTagging S3 : PutObjectVersionTagging	オブジェクト要求にタグ付けが含まれている場合は、特定のタグキーと値が必要になります。

ポリシーで変数を指定します

ポリシーで変数を使用すると、該当するポリシーの情報を設定できます。でポリシー変数を使用できます Resource の要素と文字列比較 Condition 要素 (Element) :

この例では、変数を使用しています `${aws:username}` はResource要素の一部です。

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

この例では、変数を使用しています `${aws:username}` は、条件ブロックの条件値の一部です。

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

変数 (Variable)	説明
<code>\${aws:SourceIp}</code>	SourceIp キーを指定の変数として使用します。
<code>\${aws:username}</code>	username キーを指定の変数として使用します。
<code>\${s3:prefix}</code>	サービス固有のプレフィックスキーを指定の変数として使用します。
<code>\${s3:max-keys}</code>	サービス固有の max-keys キーを指定の変数として使用します。
<code>\${*}</code>	特殊文字です。文字をリテラル * 文字として使用します。

変数 (Variable)	説明
<code>\${?}</code>	特殊文字です。文字をリテラル文字として使用しますか?を押します。
<code>\${\$}</code>	特殊文字です。文字「\$」をリテラル文字として使用します。

特別な処理を必要とするポリシーを作成します

ポリシーで付与される権限によって、アカウントの root ユーザがロックアウトされるなど、セキュリティや継続的な運用に支障が生じることがあります。StorageGRID の S3 REST API の実装では、ポリシーの検証時の制限は Amazon よりも厳しくありませんが、評価時は同等の制限が適用されます。

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
自身に対し、root アカウントに対するすべての権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ
自身に対しユーザ / グループに対するすべての権限を拒否する	グループ	有効で適用されます	同じ
外部アカウントグループに対し任意の権限を許可します	バケット	無効なプリンシパルです	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます
外部アカウントの root またはユーザに任意の権限を許可します	バケット	有効だが、S3 バケットのすべてのポリシー処理に対する権限をポリシーで許可すると 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザにすべての処理に対する権限を許可します	バケット	有効だが、外部アカウントの root およびユーザについては、S3 バケットのすべてのポリシー処理に対する権限で 405 Method Not Allowed エラーが返されます	同じ
すべてのユーザに対してすべての処理に対する権限を拒否する	バケット	有効で適用されるが、S3 バケットのすべてのポリシー処理に対する権限は引き続き root ユーザアカウントに付与される	同じ

Policy 概要 の略	ポリシータイプ	Amazon の動作	StorageGRID の動作
プリンシパルとして新規のユーザまたはグループを指定します	バケット	無効なプリンシパルです	有効
リソースとして新規の S3 バケットを指定する必要があります	グループ	有効	同じ
プリンシパルとしてローカルグループを指定します	バケット	無効なプリンシパルです	有効
ポリシーは、オブジェクトをPUTするための非所有者アカウント（匿名アカウントを含む）権限を付与します。	バケット	有効。オブジェクトは作成者アカウントによって所有され、バケットポリシーは適用されません。作成者アカウントは、オブジェクトのACLを使用してオブジェクトにアクセス権限を付与する必要があります。	有効。オブジェクトはバケット所有者アカウントによって所有され、バケットポリシーが適用される。

Write-Once-Read-Many（WORM）による保護

データ、ユーザ定義オブジェクトのメタデータ、S3 オブジェクトのタグを保護するために、Write-Once-Read-Many（WORM）バケットを作成することができます。新しいオブジェクトの作成を許可し、既存のコンテンツの上書きや削除を防止するように WORM バケットを設定します。ここで説明するいずれかの方法を使用します。

上書きを常に拒否するには、次の操作を実行します。

- Grid Managerで、* configuration > Security > Security settings > Network and objects の順に選択し、Prevent client modification *チェックボックスを選択します。
- 次のルールと S3 ポリシーを適用します。
 - S3 ポリシーに PutOverwriteObject DENY 処理を追加します。
 - S3 ポリシーに DeleteObject DENY 処理を追加します。
 - S3ポリシーにPutObject Allow処理を追加します。



S3ポリシーでDeleteObjectをDENYに設定しても、「zero copies after 30 days」などのルールが存在する場合はILMによってオブジェクトが削除されます。



これらのルールとポリシーがすべて適用されても、同時書き込みからは保護されません（状況Aを参照）。保護の対象になるのはシーケンシャルな上書きです（状況 B を参照）。

- 状況 A * : 同時書き込み（保護対象外）

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

- 状況 B * : シーケンシャルな上書き (保護対象)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

関連情報

- ["StorageGRID の ILM ルールによるオブジェクトの管理"](#)
- ["バケットポリシーの例"](#)
- ["グループポリシーの例"](#)
- ["ILM を使用してオブジェクトを管理する"](#)
- ["テナントアカウントを使用する"](#)

バケットポリシーの例

このセクションの例を使用して、バケットのStorageGRID アクセスポリシーを作成します。

バケットポリシーでは、そのポリシーが関連付けられたバケットに対するアクセス権限を指定します。バケットポリシーは、S3 PutBucketPolicy API を使用して設定します。を参照してください ["バケットの処理"](#)。

バケットポリシーを設定するには、AWS CLI で次のコマンドを使用します。

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、匿名ユーザを含むすべてのユーザにバケット内のオブジェクトのリストとバケット内のすべてのオブジェクトのGetObject処理を許可しています。それ以外の処理はすべて拒否されます。バケットへの書き込み権限がrootアカウント以外に付与されていないため、このポリシーは特に有用ではない場合があります。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
        ["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

例：あるアカウントのすべてのユーザにフルアクセスを許可し、別のアカウントのすべてのユーザにバケットへの読み取り専用アクセスを許可する

この例では、指定したアカウントのすべてのユーザにバケットへのフルアクセスを許可しています。さらに、アカウントをもう1つ指定し、そのアカウントのすべてのユーザには、で始まるバケットのオブジェクトのList処理とGetObject処理のみを許可しています shared/ オブジェクトキープレフィックス。



StorageGRID では、非所有者アカウント（匿名アカウントを含む）によって作成されたオブジェクトが、バケット所有者アカウントによって所有されます。バケットポリシーで、これらのオブジェクトの環境を設定します。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

例：すべてのユーザにバケットへの読み取り専用アクセスを許可し、指定したグループにフルアクセスを許可する

この例では、グループに属するユーザのみがバケットのList処理とバケット内のすべてのオブジェクトのGetObject処理を実行できるように匿名ユーザを含むすべてのユーザに許可しています。Marketing 指定したアカウントでは、フルアクセスが許可されています。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：クライアントの **IP 範囲** を限定して、すべてのユーザにバケットへの読み取り / 書き込みアクセスを許可する

この例では、指定した IP 範囲（54.240.143.0~54.240.143.255 で 54.240.143.188 を除く）からの要求についてのみ、匿名ユーザを含むすべてのユーザにバケットの List 処理とバケット内のすべてのオブジェクトの全処理を許可しています。それ以外の処理はすべて拒否され、IP 範囲外の要求はすべて拒否されます。

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

例：指定したフェデレーテッドユーザにのみバケットへのフルアクセスを許可します

この例では、フェデレーテッドユーザのAlexがへのフルアクセスを許可しています examplebucket バケットとそのオブジェクト。'root' を含む他のすべてのユーザは 'すべての操作を明示的に拒否されますただし、「root」による Put/Get/DeleteBucketPolicy は拒否されません。

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

例：PutOverwriteObject 権限

この例では、を使用しています Deny PutOverwriteObjectとDeleteObjectの効果は、オブジェクトのデータ、ユーザ定義メタデータ、S3オブジェクトのタグを上書きまたは削除できないようにします。

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

グループポリシーの例

このセクションの例を使用して、グループのStorageGRID アクセスポリシーを作成します。

グループポリシーは、そのポリシーが関連付けられたグループに対するアクセス権限を指定します。はいませんが Principal 要素は暗黙的であるため、ポリシーに含まれます。グループポリシーは Tenant Manager または API を使用して設定します。

例：Tenant Manager を使用してグループポリシーを設定します

Tenant Managerでグループを追加または編集するときに、グループポリシーを選択して、このグループのメンバーに付与するS3アクセス権限を決定できます。を参照してください ["S3 テナント用のグループを作成します"](#)。

- *** No S3 Access ***：デフォルトオプション。バケットポリシーでアクセスが許可されていないかぎり、このグループのユーザはS3リソースにアクセスできません。このオプションを選択すると、デフォルトでは root ユーザにのみ S3 リソースへのアクセスが許可されます。
- *** 読み取り専用アクセス ***：このグループのユーザには、S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。このオプションを選択すると、テキストボックスに読み取り専用グループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- *** フルアクセス ***：このグループのユーザには、バケットを含む S3 リソースへのフルアクセスが許可されます。このオプションを選択すると、テキストボックスにフルアクセスグループポリシーの JSON 文字列が表示されます。この文字列は編集できません。
- **ランサムウェアの軽減**：このサンプルポリシーは、このテナントのすべてのバケットを環境します。このグループのユーザは共通の操作を実行できますが、オブジェクトのバージョン管理が有効になっているバケットからオブジェクトを完全に削除することはできません。

Manage All Buckets権限を持つTenant Managerユーザは、このグループポリシーよりも優先できます。[すべてのバケットを管理]権限を信頼できるユーザに制限し、可能な場合は多要素認証（MFA）を使用します。

- *** カスタム ***：グループ内のユーザーには、テキストボックスで指定した権限が付与されます。

例：グループにすべてのバケットへのフルアクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーにテナントアカウントが所有するすべてのバケットへのフルアクセスが許可されます。

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループにすべてのバケットへの読み取り専用アクセスを許可する

この例では、バケットポリシーで明示的に拒否されている場合を除き、グループのすべてのメンバーに S3 リソースへの読み取り専用アクセスが許可されます。たとえば、オブジェクトをリストして、オブジェクトデータ、メタデータ、タグを読み取ることができます。

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

例：グループメンバーにバケット内の「フォルダ」へのフルアクセスのみを許可する

この例では、指定したバケット内の特定のフォルダ（キープレフィックス）のリストおよびアクセスのみがグループのメンバーに許可されます。これらのフォルダのプライバシー設定を決めるときは、他のグループポリシーやバケットポリシーのアクセス権限を考慮する必要があります。

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

監査ログで追跡される S3 処理

監査メッセージは StorageGRID サービスによって生成され、テキスト形式のログファイルに保存されます。監査ログのS3固有の監査メッセージを確認して、バケットとオブジェクトの処理に関する詳細を確認できます。

監査ログで追跡されるバケットの処理

- CreateBucketを選択します
- DeleteBucketの場合
- DeleteBucketTagging
- オブジェクトを削除します
- GetBucketTagging
- ヘッドバケット
- ListObjects
- ListObjectVersions
- PUT Bucket compliance で確認してください
- PutBucketTaggingの略
- PutBucketVersioningの各ノードの設定

監査ログで追跡されるオブジェクトの処理

- CompleteMultipartUpload
- CopyObject
- deleteObject
- GetObject
- HeadObject (ヘッドオブジェクト)
- PutObject
- RestoreObject
- SelectObject
- UploadPart (ILMルールの取り込みがBalancedまたはStrictの場合)
- UploadPartCopy (ILMルールの取り込みがBalancedまたはStrictの場合)

関連情報

- ["監査ログファイルにアクセスします"](#)
- ["クライアント書き込み監査メッセージ"](#)
- ["クライアント読み取り監査メッセージ"](#)

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。