



S3 プラットフォームサービスを管理します StorageGRID 11.8

NetApp
March 19, 2024

目次

S3 プラットフォームサービスを管理します	1
プラットフォームサービスの管理：概要	1
プラットフォームサービスに関する考慮事項	6
プラットフォームサービスエンドポイントを設定する	9
CloudMirror レプリケーションを設定します	25
イベント通知を設定する	29
検索統合サービスを使用する	33

S3 プラットフォームサービスを管理します

プラットフォームサービスの管理：概要

StorageGRID プラットフォームサービスでは、イベント通知やS3オブジェクトとオブジェクトメタデータのコピーを外部のデスティネーションに送信できるため、ハイブリッドクラウド戦略の実装に役立ちます。

テナントアカウントにプラットフォームサービスの使用が許可されている場合は、S3 バケットに対して次のサービスを設定できます。

CloudMirror レプリケーション

使用 ["StorageGRID CloudMirror レプリケーションサービス"](#) StorageGRID バケットから指定した外部のデスティネーションに特定のオブジェクトをミラーリングする。

たとえば、CloudMirror レプリケーションを使用して特定の顧客レコードを Amazon S3 にミラーリングし、AWS サービスを利用してデータを分析することができます。



ソースバケットで S3 オブジェクトのロックが有効になっている場合、CloudMirror レプリケーションはサポートされません。

通知

使用 ["バケット単位のイベント通知"](#) オブジェクトに対して実行された特定の処理に関する通知を、指定した外部のAmazon Simple Notification Service (Amazon SNS) に送信すること。

たとえば、バケットに追加された各オブジェクトについてアラートが管理者に送信されるように設定できます。この場合、オブジェクトは重大なシステムイベントに関連付けられているログファイルです。



S3 オブジェクトのロックが有効になっているバケットでイベント通知を設定することはできますが、オブジェクトの S3 オブジェクトロックメタデータ (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

検索統合サービス

を使用します ["検索統合サービス"](#) 外部サービスを使用してメタデータを検索または分析できるように、指定されたElasticsearchインデックスにS3オブジェクトメタデータを送信する場合。

たとえば、リモートのElasticsearch サービスに S3 オブジェクトメタデータを送信するようにバケットを設定できます。次に、Elasticsearch を使用してバケット間で検索を実行し、オブジェクトメタデータのターンに対して高度な分析を実行できます。



S3 オブジェクトロックが有効なバケットではElasticsearch 統合を設定できますが、オブジェクトの S3 オブジェクトロックメタデータ (Retain Until Date および Legal Hold のステータスを含む) は通知メッセージに含まれません。

通常、プラットフォームサービスのターゲットは StorageGRID 環境の外部にあるため、プラットフォームサービスを使用することで外部ストレージリソース、通知サービス、検索または分析サービスの機能と柔軟性をデータに対して利用できます。

単一の S3 バケットに対して複数のプラットフォームサービスを組み合わせることで設定できます。たとえば、StorageGRID S3 バケットに対して CloudMirror サービスと通知の両方を設定して、特定のオブジェクトを Amazon Simple Storage Service にミラーリングし、同時に各オブジェクトに関する通知を他社製の監視アプリケーションに送信して AWS の費用を追跡できます。



プラットフォームサービスの使用は、StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用してテナントアカウントごとに有効にする必要があります。

プラットフォームサービスの設定方法

プラットフォームサービスは、を使用して設定した外部エンドポイントと通信します **"Tenant Manager の略"** または **"テナント管理 API"**。各エンドポイントは外部のデスティネーション（StorageGRID S3バケット、Amazon Web Servicesバケット、Amazon SNSトピック、ローカルやAWSなどでホストされるElasticsearchクラスタなど）です。

外部エンドポイントを作成したら、バケットにXML設定を追加してプラットフォームサービスを有効にできます。XML 設定は、バケットが処理を実行するオブジェクト、実行する処理、およびサービスに使用するエンドポイントを特定します。

設定するプラットフォームサービスごとに XML 設定を追加する必要があります。例：

- キーがで始まるすべてのオブジェクトを指定する場合 /images Amazon S3バケットにレプリケートするには、ソースバケットにレプリケーション設定を追加する必要があります。
- これらのオブジェクトがバケットに格納されたときに通知も送信するには、通知設定を追加する必要があります。
- 最後に、これらのオブジェクトのメタデータのインデックスを作成する場合は、検索統合を実装するためのメタデータ通知設定を追加する必要があります。

設定 XML の形式は、StorageGRID プラットフォームサービスの実装に使用する S3 REST API に従います。

プラットフォームサービス	S3 REST API	を参照してください
CloudMirror レプリケーション	<ul style="list-style-type: none"> • GetBucketReplicationの略 • PutBucketReplicationの略 	<ul style="list-style-type: none"> • "CloudMirror レプリケーション" • "バケットの処理"
通知	<ul style="list-style-type: none"> • GetBucketNotificationConfigurationを参照してください • PutBucketNotificationConfigurationの略 	<ul style="list-style-type: none"> • "通知" • "バケットの処理"
検索統合	<ul style="list-style-type: none"> • GET Bucket metadata notification configuration • PUT Bucket metadata notification configuration のコマンドです 	<ul style="list-style-type: none"> • "検索統合" • "StorageGRIDのカスタム処理"

関連情報

["プラットフォームサービスに関する考慮事項"](#)

CloudMirror レプリケーションサービス

StorageGRID で、ある S3 バケットに追加されたオブジェクトを指定して 1 つ以上のデスティネーションバケットにレプリケートする必要がある場合は、そのバケットに対して CloudMirror レプリケーションを有効にすることができます。

CloudMirror レプリケーションは、グリッドのアクティブな ILM ポリシーとは独立して動作します。CloudMirror サービスは、ソースバケットに格納された時点でオブジェクトをレプリケートし、できるだけ早くデスティネーションバケットに配信します。レプリケートオブジェクトの配信は、オブジェクトの取り込みが成功したときにトリガーされます。



CloudMirror レプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点があります。詳細については、[を参照してください](#) "グリッド間レプリケーションと CloudMirror レプリケーションを比較してください"。

既存のバケットに対して CloudMirror レプリケーションを有効にすると、そのバケットに追加された新しいオブジェクトのみがレプリケートされます。バケット内の既存のオブジェクトはレプリケートされません。既存のオブジェクトのレプリケーションを強制的に実行するには、オブジェクトのコピーを実行して既存のオブジェクトのメタデータを更新します。



CloudMirror レプリケーションを使用してオブジェクトを Amazon S3 デスティネーションにコピーする場合は、Amazon S3 で各 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 に制限されることに注意してください。オブジェクトのユーザ定義メタデータが 2KB を超える場合、そのオブジェクトはレプリケートされません。

StorageGRID では、1 つのバケット内のオブジェク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。そのためには、レプリケーション設定 XML で各ルールのデスティネーションを指定します。オブジェクトを複数のバケットに同時にレプリケートすることはできません。

また、バージョン管理に対応している / していないバケットで CloudMirror レプリケーションを設定することもでき、バージョン管理に対応している / していないバケットをデスティネーションとして指定できます。バージョン管理に対応しているバケットとしないバケットを組み合わせで使用することができます。たとえば、バージョン管理に対応しているバケットをバージョン管理に対応していないソースバケットのデスティネーションとして指定することも、その逆を指定することもできます。また、バージョン管理に対応していないバケット間でもレプリケートできます。

CloudMirror レプリケーションサービスの削除は、Amazon S3 が提供する Cross Region Replication (CRR; クロスリージョンレプリケーション) サービスの削除と同様に機能します。つまり、ソースバケット内のオブジェクトを削除してもデスティネーションのレプリケートオブジェクトは削除されません。ソースとデスティネーションの両方のバケットがバージョン管理に対応している場合は、削除マーカーがレプリケートされます。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ない場合は、ソースバケット内のオブジェクトを削除しても削除マーカーはデスティネーションバケットにレプリケートされず、デスティネーションオブジェクトも削除されません。

StorageGRID は、デスティネーションバケットにレプリケートされたオブジェクトを「レプリカ」としてマークします。デスティネーション StorageGRID バケットはレプリカとしてマークされたオブジェクトを再びレプリケートしないため、誤ってレプリケーションがループすることはありません。このレプリカマーキングは StorageGRID の内部処理で、Amazon S3 バケットをデスティネーションとして使用する際に AWS CRR を使用することには支障はありません。



レプリカのマークに使用されるカスタムヘッダーは `x-ntap-sg-replica`。このマーキングは 'カスケード・ミラー' を防止します。StorageGRID では、2つのグリッド間の双方向 CloudMirror がサポートされます。

デスティネーションバケット内のイベントは一意であることや順序が保証されるわけではありません。確実に配信することを目的とした処理の結果として、ソースオブジェクトの同一のコピーが複数デスティネーションに配信されることがあります。まれに、複数の異なる StorageGRID サイトから同じオブジェクトが同時に更新された場合、デスティネーションバケットでの処理の順序がソースバケットでのイベントの順序と一致しないことがあります。

通常、CloudMirror レプリケーションは外部の S3 バケットをデスティネーションとして使用するよう設定します。ただし、他の StorageGRID 環境や任意の S3 互換サービスを使用するようにレプリケーションを設定することもできます。

バケットの通知について理解します

S3バケットのイベント通知を有効にすると、指定したイベントに関する通知をStorageGRIDからデスティネーションKafkaクラスタまたはAmazon Simple Notification Serviceに送信できます。

可能です **"イベント通知を設定する"** 通知設定 XML をソースバケットに関連付けます。通知設定XMLにはS3の規則に従ってバケット通知を設定し、デスティネーションのKafkaまたはAmazon SNSトピックをエンドポイントのURNとして指定します。

イベント通知は通知設定に従ってソースバケットで作成され、デスティネーションに配信されます。オブジェクトに関連付けられているイベントが成功すると、そのイベントに関する通知が作成されて配信のためにキューに登録されます。

通知の一意性と順序は保証されません。確実に配信することを目的とした処理の結果として、1つのイベントに関する通知が複数デスティネーションに配信されることがあります。また配信は非同期で実行されるため、特に異なる StorageGRID サイトで開始された処理の場合、デスティネーションでの通知の時間的順序がソースバケットでのイベントの順序と一致する保証はありません。を使用できます `sequencer Amazon S3` のドキュメントに従って、イベントメッセージを入力して特定のオブジェクトに対するイベントの順序を決定します。

サポートされている通知およびメッセージです

StorageGRID のイベント通知はAmazon S3 APIに従いますが、いくつかの制限事項があります。

- 次のイベントタイプがサポートされています。
 - S3 : ObjectCreated : *
 - S3 : ObjectCreated : PUT
 - S3 : ObjectCreated : Post
 - S3 : ObjectCreated : コピー
 - S3 : ObjectCreated : CompleteMultipartUpload
 - S3 : ObjectRemoved : *
 - S3 : ObjectRemoved : 削除

- S3 : ObjectRemoved : DeleteMarkerCreated
- S3 : ObjectRestore : POSTコマンド
- 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、次の表に示すように、一部のキーを含めずに特定の値を使用するキーもあります。

キー名	StorageGRID 値
eventSource	sgws:s3
awsRegion のようになります	含まれません
x-amz-id-2	含まれません
ARN	urn:sgws:s3:::bucket_name

検索統合サービスについて理解する

オブジェクトメタデータに外部の検索およびデータ分析サービスを使用する必要がある場合は、S3 バケットの検索統合を有効にすることができます。

検索統合サービスはカスタムの StorageGRID サービスです。S3 オブジェクトまたはそのメタデータが更新されるたびに、オブジェクトメタデータを非同期的に自動でデスティネーションエンドポイントに送信します。その後、デスティネーションサービスが提供する高度な検索、データ分析、視覚化、機械学習のツールを使用して、オブジェクトデータを検索、分析し、情報を把握できます。

検索統合サービスはバージョン管理に対応している / していないに関わらずすべてのバケットに対して有効にすることができます。検索統合を設定するには、対象のオブジェクトおよびオブジェクトメタデータのデスティネーションを指定したメタデータ通知設定 XML をバケットに関連付けます。

通知は、という名前の JSON ドキュメントの形式で生成されます。バケット名、オブジェクト名、バージョン ID も必要です。各メタデータ通知には、すべてのオブジェクトのタグとユーザメタデータに加えて、オブジェクトのシステムメタデータの標準セットが含まれています。



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。

通知は次の場合に常に生成され、配信のキューに登録されます

- オブジェクトが作成されます。
- オブジェクトが削除されたとき。グリッドの ILM ポリシーの処理が実行された結果、オブジェクトが削除される場合も含まれます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されたとき。変更された値だけでなく、すべてのメタデータとタグが常に更新時に送信されます。

バケットにメタデータ通知設定 XML を追加すると、新しく作成したオブジェクトや、データ、ユーザメタデータ、またはタグの更新によって変更したオブジェクトに関する通知が送信されます。ただし、バケットにすでに含まれていたオブジェクトについては通知は送信されません。バケットに含まれるすべてのオブジェクトのオブジェクトメタデータを確実にデスティネーションに送信するには、次のいずれかを行う必要があります。

- バケットの作成後、オブジェクトを追加する前に、検索統合サービスを設定する。
- すでにバケットに含まれているすべてのオブジェクトに対して、メタデータ通知メッセージをデスティネーションに送信するトリガーとなる処理を実行する。

StorageGRID 検索統合サービスは、デスティネーションとして Elasticsearch クラスタをサポートします。他のプラットフォームサービスと同様、URN がサービスの設定 XML で使用されているエンドポイントにデスティネーションが指定されます。を使用します ["NetApp Interoperability Matrix Tool で確認できます"](#) サポートされている Elasticsearch のバージョンを確認できます。

関連情報

["検索統合用の XML を設定します"](#)

["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"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスを設定する"](#)

プラットフォームサービスに関する考慮事項

プラットフォームサービスを実装する前に、これらのサービスの使用に関する推奨事項と考慮事項を確認してください。

S3 の詳細については、を参照してください ["S3 REST APIを使用する"](#)。

プラットフォームサービスの使用に関する考慮事項

考慮事項	詳細
デスティネーションエンドポイントの監視	各デスティネーションエンドポイントの可用性を監視する必要があります。長時間にわたってデスティネーションエンドポイントへの接続が失われ、要求のバックログが大量に発生している場合、StorageGRID に対する以降のクライアント要求（PUT 要求など）は失敗します。エンドポイントがアクセス可能になったら、失敗した要求を再試行する必要があります。

考慮事項	詳細
デスティネーションエンドポイントのスロットル	<p>要求が送信されるペースがデスティネーションエンドポイントで要求を受信できるペースを超えると、StorageGRID ソフトウェアはバケットの受信 S3 要求を調整する場合があります。スロットルは、デスティネーションエンドポイントへの送信を待機している要求のバックログが生じている場合にのみ発生します。</p> <p>明らかな影響は、受信 S3 要求の実行時間が長くなることです。パフォーマンスが大幅に低下していることが検出されるようになった場合は、取り込み速度を下げるか、容量の大きいエンドポイントを使用する必要があります。要求のバックログが増え続けると、クライアント S3 処理（PUT 要求など）が失敗します。</p> <p>通常、CloudMirror 要求には、検索統合やイベント通知の要求よりも多くのデータ転送が含まれるため、デスティネーションエンドポイントのパフォーマンスによる影響を受ける可能性が高くなります。</p>
順序保証	<p>StorageGRID では、1 つのサイト内のオブジェクトに対する処理の順序が保証されます。あるオブジェクトに対するすべての処理が同じサイト内で実行されるかぎり、最終的なオブジェクトの（レプリケーションの）状態は常に StorageGRID の状態と同じになります。</p> <p>StorageGRID は、StorageGRID サイト間で処理が行われる場合、最善の順序で要求を処理しようと試みます。たとえば、最初にサイト A にオブジェクトを書き込んだあと、サイト B で同じオブジェクトを上書きした場合、CloudMirror によって最終的にデスティネーションバケットにレプリケートされるオブジェクトが新しいほうのオブジェクトであるとはかぎりません。</p>
ILM ベースのオブジェクト削除	<p>AWS CRRとAmazon Simple Notification Serviceの削除動作と一致するように、StorageGRID ILMルールに基づいてソースバケット内のオブジェクトが削除された場合、CloudMirror要求とイベント通知要求は送信されません。たとえば、ILM ルールによって 14 日後にオブジェクトが削除された場合、CloudMirror 要求やイベント通知要求は送信されません。</p> <p>一方、ILM に基づいてオブジェクトが削除された場合、検索統合要求は送信されます。</p>
Kafkaエンドポイントの使用	<p>Kafkaエンドポイントでは、相互TLSはサポートされていません。その結果、<code>ssl.client.auth</code> をに設定します <code>required</code> Kafkaブローカーの設定では、原因Kafkaエンドポイントの設定に問題がある可能性があります。</p> <p>Kafkaエンドポイントの認証では、次の認証タイプが使用されます。これらのタイプは、Amazon SNSなどの他のエンドポイントの認証に使用されるタイプとは異なり、ユーザ名とパスワードのクレデンシャルが必要です。</p> <ul style="list-style-type: none"> • SASL/プレーン • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>*注：*構成済みのストレージプロキシ設定は、Kafkaプラットフォームサービスエンドポイントには適用されません。</p>

CloudMirror レプリケーションサービスの使用に関する考慮事項

考慮事項	詳細
レプリケーションのステータス	StorageGRID ではサポートされません x-amz-replication-status ヘッダー。
オブジェクトのサイズ	<p>CloudMirror レプリケーションサービスでデスティネーションバケットにレプリケートできるオブジェクトの最大サイズは 5TiB で、maximum_supported_object サイズと同じです。</p> <p>注：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。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。</p>
バケットのバージョン管理とバージョン ID	<p>StorageGRID でソース S3 バケットのバージョン管理を有効にした場合、デスティネーションバケットのバージョン管理も有効にする必要があります。</p> <p>バージョン管理を使用している場合、S3 プロトコルの制限事項により、デスティネーションバケットのオブジェクトバージョンの処理はベストエフォートベースで行われ、CloudMirror サービスによる保証はありません。</p> <p>注：StorageGRID のソースバケットのバージョンIDは、デスティネーションバケットのバージョンIDとは関係ありません。</p>
オブジェクトバージョンのタグ付け	<p>S3プロトコルの制限により、バージョンIDを提供するPutObjectTagging要求やDeleteObjectTagging要求はCloudMirrorサービスではレプリケートされません。ソースとデスティネーションのバージョンIDは関連付けられていないため、特定のバージョンIDへのタグの更新を確実にレプリケートする方法はありません。</p> <p>一方、CloudMirrorサービスでは、バージョンIDを指定しないPutObjectTagging要求またはDeleteObjectTagging要求はレプリケートされません。これらの要求は、最新のキー（バケットがバージョン管理されている場合は最新のバージョン）のタグを更新します。（タグの更新ではなく）タグを使用した通常の取り込みもレプリケートされます。</p>
マルチパートアップロードおよび ETag 値	マルチパートアップロードを使用してアップロードされたオブジェクトをミラーリングした場合、CloudMirror サービスではパートが保持されません。その結果、が表示されます ETag ミラーオブジェクトの値は、とは異なります ETag 元のオブジェクトの値。
SSE-C（ユーザ指定のキーによるサーバ側の暗号化）で暗号化されたオブジェクト	CloudMirror サービスでは、SSE-C で暗号化されたオブジェクトがサポートされませんCloudMirror レプリケーションのソースバケットにオブジェクトを取り込む際に、要求に SSE-C 要求ヘッダーが含まれていると、処理が失敗します。
S3 オブジェクトのロックが有効になっているバケット	CloudMirrorレプリケーションのデスティネーションS3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、バケットのレプリケーションを設定しようとするとAccessDeniedエラーで失敗します。

プラットフォームサービスエンドポイントを設定する

バケットのプラットフォームサービスを設定する前に、少なくとも1つのエンドポイントをプラットフォームサービスのデスティネーションとして設定する必要があります。

プラットフォームサービスへのアクセスは、StorageGRID 管理者がテナント単位で有効にします。プラットフォームサービスエンドポイントを作成または使用するには、ストレージノードが外部のエンドポイントリソースにアクセスできるようネットワークが設定されているグリッドで、Manage EndpointsまたはRoot Access 権限を持つテナントユーザである必要があります。1つのテナントに対して設定できるプラットフォームサービスエンドポイントは最大500個です。詳細については、StorageGRID 管理者にお問い合わせください。

プラットフォームサービスエンドポイントとは何ですか。

プラットフォームサービスエンドポイントを作成するときは、StorageGRID が外部のデスティネーションにアクセスするために必要な情報を指定します。

たとえば、StorageGRID バケットからAmazon S3バケットにオブジェクトをレプリケートする場合は、StorageGRID がAmazonのデスティネーションバケットにアクセスするために必要な情報とクレデンシャルを含むプラットフォームサービスエンドポイントを作成します。

プラットフォームサービスのタイプごとに独自のエンドポイントが必要なため、使用する各プラットフォームサービスについて少なくとも1つのエンドポイントを設定する必要があります。プラットフォームサービスエンドポイントの定義が完了したら、サービスを有効にするための設定XMLでエンドポイントのURNをデスティネーションとして指定します。

同じエンドポイントを複数のソースバケットのデスティネーションとして使用できます。たとえば、複数のバケット間で検索を実行できるように、複数のソースバケットが同じ検索統合エンドポイントにオブジェクトメタデータを送信するように設定できます。複数のエンドポイントをターゲットとして使用するようにソースバケットを設定することもできます。これにより、オブジェクトの作成に関する通知をあるAmazon Simple Notification Service (Amazon SNS) トピックに送信したり、オブジェクトの削除に関する通知を別のAmazon SNSトピックに送信したりできます。

CloudMirror レプリケーション用のエンドポイント

StorageGRID は、S3 バケットを表すレプリケーションエンドポイントをサポートします。このバケットは、Amazon Web Services、同一またはリモートのStorageGRID 環境、あるいは別のサービスでホストされている可能性があります。

通知用のエンドポイント

StorageGRIDは、Amazon SNSおよびKafkaエンドポイントをサポートしています。Simple Queue Service (SQS) またはAWS Lambdaエンドポイントはサポートされていません。

Kafkaエンドポイントでは、相互TLSはサポートされていません。その結果、`ssl.client.auth` をに設定します `required` Kafkaブローカーの設定では、原因Kafkaエンドポイントの設定に問題がある可能性があります。

検索統合サービスのエンドポイント

StorageGRID は、Elasticsearch クラスタを表す検索統合エンドポイントをサポートします。Elasticsearch クラスタは、ローカルデータセンターに配置することも、AWSクラウドなどの別の場所でホストすることも

きます。

検索統合エンドポイントは、Elasticsearch の特定のインデックスとタイプを参照します。StorageGRID でエンドポイントを作成する前に、Elasticsearch でインデックスを作成しておく必要があります。作成していない場合、エンドポイントの作成に失敗します。エンドポイントを作成する前にタイプを作成する必要はありません。StorageGRID は、オブジェクトメタデータをエンドポイントに送信するときに必要に応じてタイプを作成します。

関連情報

["StorageGRID の管理"](#)

プラットフォームサービスのエンドポイントの **URN** を指定してください

プラットフォームサービスエンドポイントを作成するときは、Unique Resource Name (URN) を指定する必要があります。プラットフォームサービスの設定XMLを作成するときは、URNを使用してエンドポイントを参照します。各エンドポイントのURNは一意である必要があります。

プラットフォームサービスエンドポイントは、作成時に StorageGRID で検証されます。プラットフォームサービスエンドポイントを作成する前に、エンドポイントで指定されたリソースが存在し、アクセス可能であることを確認してください。

URN 要素

プラットフォームサービスのエンドポイントのURNは、いずれかで開始する必要があります `arn:aws` または `urn:mystore`、次のようにします。

- サービスがAmazon Web Services (AWS) でホストされている場合は、を使用します `arn:aws`
- サービスがGoogle Cloud Platform (GCP) でホストされている場合は、を使用します `arn:aws`
- サービスがローカルでホストされている場合は、を使用します `urn:mystore`

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合、URNはで始まる可能性があります `urn:sgws`。

URN の次の要素では、次のようにプラットフォームサービスのタイプを指定します。

サービス	を入力します
CloudMirror レプリケーション	s3
通知	sns または kafka
検索統合	es

たとえば、StorageGRID でホストされるCloudMirrorエンドポイントのURNを指定する場合は、と指定します `s3` をダウンロードしてください `urn:sgws:s3`。

URN の最後の要素は、デスティネーション URI の特定のターゲットリソースを識別します。

サービス	特定のリソース
CloudMirror レプリケーション	bucket-name
通知	sns-topic-name または kafka-topic-name
検索統合	domain-name/index-name/type-name <ul style="list-style-type: none"> 注： Elasticsearch クラスタが * NOT * である場合、インデックスを自動的に作成するように設定されているため、エンドポイントを作成する前にインデックスを手動で作成する必要があります。

AWS と GCP でホストされるサービスの URN

AWS と GCP のエンティティの場合、完全な URN は有効な AWS ARN です。例：

- CloudMirror レプリケーション：

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

- 通知：

```
arn:aws:sns:region:account-id:topic-name
```

- 検索統合：

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



AWS検索統合エンドポイントの場合は、を参照してください domain-name リテラル文字列を含める必要があります `domain/` を参照してください。

ローカルでホストされるサービスの URN

クラウド サービス ではなくローカルでホストされるサービスを使用する場合は、URN の 3 番目と最後の必須要素が含まれていて、有効かつ一意な URN が作成されるのであれば、どのような方法で URN を指定してもかまいません。となっている要素はオプションで空白にすることも、リソースを識別して一意な URN の作成に役立つ任意の情報を指定することもできます。例：

- CloudMirror レプリケーション：

```
urn:mystore:s3:optional:optional:bucket-name
```

StorageGRID でホストされるCloudMirrorエンドポイントの場合は、で始まる有効なURNを指定できます

urn:sgws :

```
urn:sgws:s3:optional:optional:bucket-name
```

• 通知 :

Amazon Simple Notification Serviceエンドポイントを指定します。

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Kafkaエンドポイントを指定します。

```
urn:mysite:kafka:optional:optional:kafka-topic-name
```

• 検索統合 :

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```



ローカルでホストされる検索統合エンドポイントの場合は、を参照してください domain-name エンドポイントのURNが一意であるかぎり、Elementには任意の文字列を指定できません。

プラットフォームサービスエンドポイントを作成します

プラットフォームサービスを有効にする前に、正しいタイプのエンドポイントを少なくとも 1 つ作成しておく必要があります。

作業を開始する前に

- Tenant Manager にはを使用してサインインします "サポートされている Web ブラウザ"。
- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- が設定されたユーザグループに属している必要があります "エンドポイントまたはRoot Access権限を管理します"。
- プラットフォームサービスエンドポイントによって参照されるリソースを作成しておきます。
 - CloudMirror レプリケーション : S3 バケット
 - イベント通知 : Amazon Simple Notification Service (Amazon SNS) またはKafkaトピック
 - 検索通知 : インデックスを自動的に作成するようにデスティネーションクラスタが設定されていない場合、Elasticsearch インデックス。
- デスティネーションリソースに関する情報を確認しておきます。
 - Uniform Resource Identifier (URI) のホストとポート



StorageGRID システムでホストされているバケットを CloudMirror レプリケーションのエンドポイントとして使用する場合は、グリッド管理者に問い合わせて入力が必要な値を決定してください。

- Unique Resource Name (URN)

"プラットフォームサービスのエンドポイントの URN を指定してください"

- 認証クレデンシャル (必要な場合) :

AWSケンサクトウコウエントホイント

AWS検索統合エンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key : アクセスキー ID とシークレットアクセスキー
- 基本 HTTP 認証: ユーザ名とパスワード
- CAP (C2S Access Portal) : 一時的なクレデンシャル URL、サーバ証明書とクライアント証明書、クライアントキー、およびオプションのクライアント秘密鍵パスフレーズ。

CloudMirrorレプリケーションと**Amazon SNS**エンドポイント

CloudMirrorレプリケーションエンドポイントとAmazon SNSエンドポイントの場合は、次のクレデンシャルを使用できます。

- Access Key : アクセスキー ID とシークレットアクセスキー
- CAP (C2S Access Portal) : 一時的なクレデンシャル URL、サーバ証明書とクライアント証明書、クライアントキー、およびオプションのクライアント秘密鍵パスフレーズ。

Kafkaエンドポイント

Kafkaエンドポイントの場合は、次のクレデンシャルを使用できます。

- SASL/plain : ユーザ名とパスワード
- SASL/SCRAM-SHA-256 : ユーザ名とパスワード
- SASL/SCRAM-SHA-512 : ユーザ名とパスワード

- セキュリティ証明書 (カスタム CA 証明書を使用する場合)

- Elasticsearchセキュリティ機能が有効になっている場合は、接続テスト用のmonitor cluster権限と、ドキュメント更新用のwrite index権限、またはindex権限とdelete index権限の両方があります。

手順

1. ストレージ (S3) * > * プラットフォームサービスのエンドポイント * を選択します。プラットフォームサービスエンドポイントページが表示されます。
2. [* エンドポイントの作成 *] を選択します。
3. エンドポイントとその目的を簡単に説明する表示名を入力します。

エンドポイントがサポートするプラットフォームサービスのタイプは、[Endpoints]ページのエンドポイント名の横に表示されるため、この情報を名前に含める必要はありません。

4. [* URI*] フィールドに、エンドポイントの Unique Resource Identifier (URI) を指定します。

次のいずれかの形式を使用します。

```
https://host:port  
http://host:port
```

ポートを指定しない場合は、次のデフォルトポートが使用されます。

- HTTPS URIにはポート443、HTTP URIにはポート80（ほとんどのエンドポイント）
- HTTPSおよびHTTP URI用のポート9092（Kafkaエンドポイントのみ）

たとえば、StorageGRID でホストされているバケットの URI は次のようになります。

```
https://s3.example.com:10443
```

この例では、s3.example.com StorageGRID ハイアベイラビリティ (HA) グループの仮想IP (VIP) のDNSエントリ、およびを表します 10443 ロードバランサエンドポイントで定義されたポートを表します。



単一点障害 (Single Point of Failure) を回避するために、可能な限りロードバランシングノードのHAグループに接続する必要があります。

同様に、AWS でホストされているバケットの URI は次のようになります。

```
https://s3-aws-region.amazonaws.com
```



エンドポイントがCloudMirrorレプリケーションサービスに使用される場合は、URIにバケット名を含めないでください。バケット名は「* URN *」フィールドに含める必要があります。

5. エンドポイントの Unique Resource Name (URN) を入力します。



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

6. 「* Continue *」を選択します。

7. [認証タイプ]*の値を選択します。

AWSケンサクトウコウエントポイント

AWS検索統合エンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
アクセスキー	AWS形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none">• アクセスキー ID• シークレットアクセスキー
基本 HTTP	ユーザ名とパスワードを使用して、デスティネーションへの接続を認証します。	<ul style="list-style-type: none">• ユーザ名• パスワード
CAP (C2S Access Portal)	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none">• 一時的な資格情報 URL• サーバ CA 証明書 (PEM ファイルのアップロード)• クライアント証明書 (PEM ファイルのアップロード)• クライアント秘密鍵 (PEM ファイルのアップロード、OpenSSL 暗号化形式、または暗号化されていない秘密鍵形式)• クライアント秘密鍵のパスフレーズ (オプション)

CloudMirrorレプリケーションまたはAmazon SNSエンドポイント

CloudMirrorレプリケーションまたはAmazon SNSエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。

認証タイプ	説明	クレデンシャル
アクセスキー	AWS 形式のクレデンシャルを使用してデスティネーションとの接続を認証します。	<ul style="list-style-type: none"> • アクセスキー ID • シークレットアクセスキー
CAP (C2S Access Portal)	証明書とキーを使用してデスティネーションへの接続を認証します。	<ul style="list-style-type: none"> • 一時的な資格情報 URL • サーバ CA 証明書 (PEM ファイルのアップロード) • クライアント証明書 (PEM ファイルのアップロード) • クライアント秘密鍵 (PEM ファイルのアップロード、OpenSSL 暗号化形式、または暗号化されていない秘密鍵形式) • クライアント秘密鍵のパスフレーズ (オプション)

Kafkaエンドポイント

Kafkaエンドポイントのクレデンシャルを入力またはアップロードします。

指定するクレデンシャルには、デスティネーションリソースに対する書き込み権限が必要です。

認証タイプ	説明	クレデンシャル
匿名	デスティネーションへの匿名アクセスを許可します。セキュリティが無効になっているエンドポイントでのみ機能します。	認証なし。
SASL/プレーン	プレーンテキストのユーザ名とパスワードを使用して、宛先への接続を認証します。	<ul style="list-style-type: none"> • ユーザ名 • パスワード
SASL/SCRAM-SHA-256	チャレンジ応答プロトコルとSHA-256 ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> • ユーザ名 • パスワード
SASL/SCRAM-SHA-512	チャレンジ応答プロトコルとSHA-512 ハッシュを使用してユーザ名とパスワードを使用し、宛先への接続を認証します。	<ul style="list-style-type: none"> • ユーザ名 • パスワード

ユーザ名とパスワードがKafkaクラスタから取得した委任トークンから取得されたものである場合は、* Use delegation taken authentication *を選択します。

8. 「 * Continue * 」を選択します。
9. Verify server * のラジオボタンを選択して、エンドポイントへの TLS 接続の検証方法を選択します。

×

Create endpoint

✓ Enter details
 ✓ Select authentication type Optional
3 Verify server Optional

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abodefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabodefghijklABCD
-----END CERTIFICATE-----
```

Previous
Test and create endpoint

証明書検証のタイプ	説明
カスタム CA 証明書を使用する	カスタムのセキュリティ証明書を使用します。この設定を選択した場合は、カスタムセキュリティ証明書を * CA 証明書 * テキストボックスにコピーして貼り付けます。
オペレーティングシステムの CA 証明書を使用します	オペレーティングシステムにインストールされているデフォルトの Grid CA 証明書を使用して接続を保護します。
証明書を検証しないでください	TLS 接続に使用される証明書は検証されません。このオプションはセキュアではありません。

10. [* テストとエンドポイントの作成 *] を選択します。
 - 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
 - エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、 * エンドポイントの詳細に戻る * を選択して情報を更新します。次に、「 * Test 」を選択し、エンドポイントを作成します。 *



テナントアカウントでプラットフォームサービスが有効になっていないと、エンドポイントの作成が失敗します。StorageGRID 管理者にお問い合わせください。

エンドポイントの設定が完了したら、その URN を使用してプラットフォームサービスを設定できます。

関連情報

["プラットフォームサービスのエンドポイントの URN を指定してください"](#)

["CloudMirror レプリケーションを設定します"](#)

["イベント通知を設定する"](#)

["検索統合サービスを設定する"](#)

プラットフォームサービスエンドポイントの接続をテストします

プラットフォームサービスへの接続が変更された場合は、エンドポイントへの接続をテストして、デスティネーションリソースが存在すること、および指定したクレデンシャルでアクセスできることを確認できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

このタスクについて

StorageGRID は、クレデンシャルに正しい権限があるかどうかを検証しません。

手順

1. ストレージ (S3) * > * [プラットフォームサービスのエンドポイント](#) * を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 接続をテストするエンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

Overview [^](#)

Display name: **my-endpoint-1** [✎](#)

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection **Configuration**

Verify connection [?](#)

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. [接続のテスト *] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの1つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エラーを修正するためにエンドポイントを変更する必要がある場合は、「* Configuration *」を選択して情報を更新します。次に、[テスト] を選択し、変更を保存します。*

プラットフォームサービスエンドポイントを編集します

プラットフォームサービスエンドポイントの設定を編集して、名前、URI、またはその他の詳細を変更できます。たとえば、期限切れのクレデンシャルを更新したり、フェールオーバー用のバックアップ Elasticsearch インデックスを指すように URI を変更したりすることが必要な場合があります。プラットフォームサービスエンドポイントのURN は変更できません。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

手順

1. ストレージ (S3) * > * プラットフォームサービスのエンドポイント * を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints [Create endpoint](#)

[Delete endpoint](#)

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. 編集するエンドポイントを選択します。


エンドポイントの詳細ページが表示されます。

3. 「* Configuration *」を選択します。

4. 必要に応じて、エンドポイントの設定を変更します。



エンドポイントの作成後にエンドポイントのURNを変更することはできません。

a. エンドポイントの表示名を変更するには、編集アイコンを選択します .

b. 必要に応じて、URI を変更します。

c. 必要に応じて、認証タイプを変更します。

- アクセスキー認証の場合は、必要に応じて「* S3 キーの編集」を選択し、新しいアクセスキー ID とシークレットアクセスキーを貼り付けることで、キーを変更します。変更をキャンセルする必要がある場合は、* Revert S3 key edit * を選択します。
- CAP (C2S Access Portal) 認証の場合は、一時的なクレデンシャル URL またはオプションのクライアント秘密鍵パスフレーズを変更し、必要に応じて新しい証明書と鍵ファイルをアップロードします。



クライアント秘密鍵は、OpenSSL 暗号化形式または暗号化されていない秘密鍵形式である必要があります。

d. 必要に応じて、サーバを検証する方法を変更します。

5. [変更のテストと保存 *] を選択します。

- 指定したクレデンシャルを使用してエンドポイントにアクセスできた場合は、成功を伝えるメッセージが表示されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。
- エンドポイントの検証が失敗した場合は、エラーメッセージが表示されます。エンドポイントを変更してエラーを修正し、[変更のテストと保存] を選択します。

プラットフォームサービスエンドポイントを削除します

関連するプラットフォームサービスが不要になった場合は、エンドポイントを削除できます。

作業を開始する前に

- Tenant Manager にはを使用してサインインします ["サポートされている Web ブラウザ"](#)。
- が設定されたユーザグループに属している必要があります ["エンドポイントまたはRoot Access権限を管理します"](#)。

手順

1. ストレージ (S3) * > * プラットフォームサービスのエンドポイント * を選択します。

Platform services Endpoints ページが表示され、設定済みのプラットフォームサービスエンドポイントのリストが表示されます。

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name [?] ↕	Last error [?] ↕	Type [?] ↕	URI [?] ↕	URN [?] ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

- 削除する各エンドポイントのチェックボックスを選択します。



使用中のプラットフォームサービスエンドポイントを削除すると、エンドポイントを使用するすべてのバケットに対して、関連するプラットフォームサービスが無効になります。完了していない要求はすべて破棄されます。新しい要求は、削除された URN を参照しないようにバケット設定を変更するまで、引き続き生成されます。StorageGRID はこれらの要求を回復不能なエラーとして報告します。

- [* アクション * > * エンドポイントの削除 *] を選択します。

確認メッセージが表示されます。

Delete endpoint ✕

Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

Cancel Delete endpoint


4. [* エンドポイントの削除 *] を選択します。

プラットフォームサービスのエンドポイントエラーのトラブルシューティングを行います

StorageGRID がプラットフォームサービスエンドポイントと通信しようとしたときにエラーが発生すると、ダッシュボードにメッセージが表示されます。Platform services Endpoints ページの Last error 列は、エラーが発生してからの時間を示します。エンドポイントのクレデンシャルに関連付けられている権限が正しくない場合は、エラーは表示されません。


エラーが発生したかどうかを確認します

過去7日以内にプラットフォームサービスエンドポイントエラーが発生した場合は、Tenant Managerダッシュボードにアラートメッセージが表示されます。プラットフォームサービスのエンドポイントページに移動して、エラーの詳細を確認できます。

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

ダッシュボードに表示されるのと同じエラーは、[Platform services Endpoints]ページの上にも表示されます。詳細なエラーメッセージを表示するには、次の手順を実行します

手順

1. エンドポイントのリストで、エラーが発生したエンドポイントを選択します。
2. エンドポイントの詳細ページで、* 接続 * を選択します。このタブには、エンドポイントの最新のエラーと、エラーが発生してからの経過時間が表示されます。赤の X アイコンを含むエラー  過去 7 日以内に発生しました。

Overview ^

Display name:	my-endpoint-2
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

エラーがまだ最新であるかどうかを確認します

一部のエラーは、解決後も「* Last error *」列に引き続き表示される場合があります。エラーが現在発生しているかどうかを確認したり、解決済みのエラーをテーブルから強制的に削除したりするには、次の手順を実行します。

手順

1. エンドポイントを選択します。

エンドポイントの詳細ページが表示されます。

2. 接続 > 接続テスト * を選択します。

[接続のテスト *] を選択すると、StorageGRID はプラットフォームサービスエンドポイントが存在すること、および現在のクレデンシャルでアクセスできることを検証します。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

24

エンドポイントエラーの解決

エンドポイントの詳細ページの「* Last error *」メッセージを使用して、エラーの原因を特定できます。一部のエラーでは、問題を解決するためにエンドポイントの編集が必要になります。たとえば、StorageGRID に正しいアクセス権限がないか、アクセスキーが期限切れになっているためにデスティネーションの S3 バケットにアクセスできない場合、CloudMirror のエラーが発生することがあります。メッセージは「Either the endpoint credentials or the destination access needs to be updated」で、詳細は「AccessDenied」または「InvalidAccessKeyId」です。

エラーを解決するためにエンドポイントを編集する必要がある場合は、「* 変更のテストと保存 *」を選択すると、StorageGRID によって更新されたエンドポイントが検証され、現在のクレデンシャルで到達できることが確認されます。エンドポイントへの接続は、各サイトの 1 つのノードから検証されます。

手順

1. エンドポイントを選択します。
2. エンドポイントの詳細ページで、* 構成 * を選択します。
3. 必要に応じてエンドポイントの設定を編集します。
4. 接続 > 接続テスト * を選択します。

必要な権限がないエンドポイントクレデンシャルです

StorageGRID によるプラットフォームサービスエンドポイントの検証では、エンドポイントのクレデンシャルを使用してデスティネーションリソースに接続できること、および基本的な権限チェックを実行できることが確認されます。ただし、StorageGRID では、特定のプラットフォームサービス処理に必要なすべての権限が検証されるわけではありません。そのため、プラットフォームサービスを使用しようとしたときにエラー（「403 Forbidden」など）が表示された場合は、エンドポイントのクレデンシャルに関連付けられている権限を確認してください。

関連情報

- ["StorageGRIDの管理>プラットフォームサービスのトラブルシューティング"](#)
- ["プラットフォームサービスエンドポイントを作成します"](#)
- ["プラットフォームサービスエンドポイントの接続をテストします"](#)
- ["プラットフォームサービスエンドポイントを編集します"](#)

CloudMirror レプリケーションを設定します

。 ["CloudMirror レプリケーションサービス"](#) は、3 つの StorageGRID プラットフォームサービスのうちの 1 つです。CloudMirror レプリケーションを使用すると、外部の S3 バケットにオブジェクトを自動的にレプリケートできます。

作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- レプリケーションソースとして機能するバケットがすでに作成されている。
- CloudMirrorレプリケーションのデスティネーションとして使用するエンドポイントがすでに存在し、そのURNが必要です。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管](#)

理します”。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

CloudMirror レプリケーションでは、ソースバケットからエンドポイントで指定されたデスティネーションバケットにオブジェクトがコピーされます。



CloudMirrorレプリケーションには、クロスグリッドレプリケーション機能と重要な類似点と相違点があります。詳細については、[を参照してください "グリッド間レプリケーションとCloudMirrorレプリケーションを比較してください"](#)。

バケットでCloudMirrorレプリケーションを有効にするには、有効なバケットレプリケーション設定XMLを作成して適用する必要があります。レプリケーション設定 XML では、各デスティネーションとして S3 バケットエンドポイントの URN を使用する必要があります。



S3 オブジェクトロックが有効なソースバケットまたはデスティネーションバケットでは、レプリケーションはサポートされません。

バケットレプリケーションとその設定方法の一般的な情報については、[を参照してください "Amazon Simple Storage Service \(S3\) のドキュメント：「オブジェクトのレプリケート"](#)。StorageGRID でのGetBucketReplication、DeleteBucketReplication、およびPutBucketReplicationの実装方法については、[を参照してください "バケットの処理"](#)。

オブジェクトを含むバケットでCloudMirrorレプリケーションを有効にすると、バケットに追加された新しいオブジェクトがレプリケートされますが、バケット内の既存のオブジェクトはレプリケートされません。レプリケーションをトリガーするには、既存のオブジェクトを更新する必要があります。

レプリケーション設定 XML でストレージクラスを指定した場合は、デスティネーション S3 エンドポイントに対して処理を実行する際に StorageGRID でそのクラスが使用されます。指定したストレージクラスは、デスティネーションエンドポイントでもサポートされている必要があります。デスティネーションシステムのベンダーからの推奨事項がある場合は、それに準拠してください。

手順

1. ソースバケットのレプリケーションを有効にします。

S3 レプリケーション API で指定されているように、レプリケーションを有効にするために必要なレプリケーション設定 XML をテキストエディタで作成します。XML を設定する場合は、次の点に

- 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、レプリケーション設定に関する Amazon のドキュメントを参照してください。
- デスティネーションとして S3 バケットエンドポイントの URN を使用してください。
- 必要に応じてを追加します <StorageClass> エレメントを選択し、次のいずれかを指定します。
 - STANDARD：デフォルトのストレージクラス。オブジェクトをアップロードするときにストレージクラスを指定しない場合は、が表示されます STANDARD ストレージクラスが使用されている。
 - STANDARD_IA：（標準-アクセス頻度の低いアクセス）このストレージクラスは、アクセス頻度は低いが、必要に応じて高速アクセスが必要なデータに使用します。
 - REDUCED_REDUNDANCY：重大度が低く、再現可能で、かつ冗長性に劣る状態で保存可能なデータ

には、このストレージクラスを使用します STANDARD ストレージクラス。

- を指定する場合 Role 設定XMLでは無視されます。この値は StorageGRID では使用されません。

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. ダッシュボードで* View Buckets を選択するか、 storage (S3) > Buckets *を選択します。
3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス * > * レプリケーション * を選択します。
5. [レプリケーションを有効にする]*チェックボックスを選択します。
6. レプリケーション設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。

Bucket options
Bucket access
Platform services

Replication
Disabled
↑

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Save changes



StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. レプリケーションが正しく設定されていることを確認します。
 - a. レプリケーション設定で指定されたレプリケーションの要件を満たすオブジェクトをソースバケットに追加します。

前述の例では、プレフィックス「2020」に一致するオブジェクトがレプリケートされます。
 - b. オブジェクトがデスティネーションバケットにレプリケートされたことを確認します。

サイズの小さいオブジェクトについては、レプリケーションの所要時間が短くなります。

関連情報

["プラットフォームサービスエンドポイントを作成します"](#)

イベント通知を設定する

通知サービスは、3つの StorageGRID プラットフォームサービスのうちの1つです。バケットの通知を有効にすると、指定したイベントに関する情報をAWS Simple Notification Service (Amazon SNS) をサポートするデスティネーションKafkaクラスタまたはサービスに送信できます。

作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- 通知のソースとして機能するバケットを作成しておきます。
- イベント通知のデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

イベント通知を設定すると、ソースバケット内のオブジェクトで指定したイベントが発生するたびに通知が生成され、デスティネーションエンドポイントとして使用されているAmazon SNSまたはKafkaトピックに送信されます。バケットの通知を有効にするには、有効な通知設定 XML を作成して適用する必要があります。通知設定 XML では、各デスティネーションとしてイベント通知エンドポイントの URN を使用する必要があります。

イベント通知とその設定方法の一般的な情報については、Amazonのドキュメントを参照してください。StorageGRIDでS3バケットの通知設定APIを実装する方法については、[を参照してください](#)。"[S3 クライアントアプリケーションを実装するための手順](#)"。

オブジェクトを含むあるバケットのイベント通知を有効にした場合、通知は通知設定の保存後に実行された処理に対してのみ送信されます。

手順

1. ソースバケットの通知を有効にします。
 - イベント通知を有効にするために必要な通知設定 XML を、S3 通知 API で指定されている内容に従ってテキストエディタで作成します。
 - XML を設定するにあたっては、デスティネーショントピックとしてイベント通知エンドポイントの URN を使用します。

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Tenant Manager で、 * Storage (S3) * > * Buckets * を選択します。

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス > イベント通知 * を選択します。

5. [イベント通知を有効にする]*チェックボックスをオンにします。

6. 通知設定 XML をテキストボックスに貼り付け、 * 変更を保存 * を選択します。

Bucket options Bucket access Platform services S3 Console

Replication Disabled

Event notifications Disabled

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS) or a destination Apache Kafka cluster.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

Clear

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
</NotificationConfiguration>
```

Save changes



StorageGRID 管理者がグリッドマネージャまたはグリッド管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. イベント通知が正しく設定されていることを確認します。
 - a. 設定 XML で設定した通知をトリガーする要件を満たす操作をソースバケット内のオブジェクトに対して実行します。

この例では、を使用してオブジェクトが作成されるたびにイベント通知が送信されます images/ プレフィックス。

b. デスティネーションのAmazon SNSまたはKafkaトピックに通知が配信されたことを確認します。

たとえば、デスティネーショントピックがAmazon SNSでホストされている場合は、通知が配信されたときにEメールを送信するようにサービスを設定できます。

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+ デスティネーショントピックに通知が届いた場合は、StorageGRID 通知のソースバケットが正しく設定されています。

["バケットの通知について理解します"](#)

["S3 REST APIを使用する"](#)

["プラットフォームサービスエンドポイントを作成します"](#)

検索統合サービスを使用する

検索統合サービスは、3つの StorageGRID プラットフォームサービスのうちの1つです。このサービスを有効にすると、オブジェクトが作成、削除されたとき、またはそのメタデータやタグが更新されたときに、デスティネーションの検索インデックスにオブジェクトメタデータを送信できます。

テナントマネージャを使用して検索統合を設定し、カスタム StorageGRID 設定 XML をバケットに適用できます。



検索統合サービスではオブジェクトメタデータがデスティネーションに送信されるため、その設定 XML は `_メタデータ通知設定.xml` と呼ばれます。この設定 XML は、イベント通知を有効にするための `_通知設定.xml` とは異なります。

を参照してください ["S3 クライアントアプリケーションを実装するための手順"](#) 次のカスタムの StorageGRID S3 REST API 処理の詳細については、以下を参照してください。

- バケットのメタデータ通知設定を削除します
- GET Bucket metadata notification configuration
- PUT Bucket metadata notification configuration のコマンドです

関連情報

["検索統合用の XML を設定します"](#)

["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"](#)

["検索統合サービスで生成される JSON"](#)

["検索統合サービスを設定する"](#)

["S3 REST APIを使用する"](#)

検索統合用の XML を設定します

検索統合サービスは、内に含まれる一連のルールを使用して設定します

```
<MetadataNotificationConfiguration> および  
</MetadataNotificationConfiguration> タグ。各ルールは、ルール環境で指定されたオブジェクト、および StorageGRID からそのオブジェクトの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、`images` 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

オブジェクトのメタデータに追加します 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、プレフィックスがオブジェクトに対するルールを1つ含む設定です 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 は許可されていません。

デスティネーションは、検索統合サービス用に作成された 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。これらのエンドポイントは、Elasticsearch クラスタ上に定義されているインデックスとタイプを参照します。

```
<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>
```

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」を指定できません。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 domain-name/myindex/mytype。 <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"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <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。

サンプルのメタデータ通知設定 XML を使用して、独自の XML を作成する方法を確認できます。

メタデータ通知設定：環境 のすべてのオブジェクトを対象にした設定です

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。

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

2 つのルールを含むメタデータ通知設定

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。

```
<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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

関連情報

["S3 REST APIを使用する"](#)

"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"

"検索統合サービスで生成される JSON"

"検索統合サービスを設定する"

検索統合サービスを設定します

検索統合サービスでは、オブジェクトが作成、削除、またはそのメタデータ / タグが更新されるたびに、デスティネーションの検索インデックスにオブジェクトメタデータが送信されます。

作業を開始する前に

- テナントアカウントのプラットフォームサービスがStorageGRID 管理者によって有効にされている。
- コンテンツにインデックスを付けるS3バケットを作成しておきます。
- 検索統合サービスのデスティネーションとして使用するエンドポイントがすでに存在し、URNが設定されている必要があります。
- が設定されたユーザグループに属している必要があります ["すべてのバケットまたはRoot Access権限を管理します"](#)。これらの権限は、Tenant Manager を使用してバケットを設定する際にグループポリシーまたはバケットポリシーの権限設定よりも優先されます。

このタスクについて

ソースバケットに対して検索統合サービスを設定した場合、オブジェクトを作成またはオブジェクトのメタデータ / タグを更新すると、オブジェクトメタデータがデスティネーションエンドポイントに送信されます。すでにオブジェクトが含まれているバケットで検索統合サービスを有効にすると、既存のオブジェクトに関するメタデータ通知は自動的に送信されません。既存のオブジェクトのメタデータがデスティネーションの検索インデックスに追加されるようにするには、オブジェクトを更新する必要があります。

手順

1. 検索統合を有効にするために必要なメタデータ通知 XML をテキストエディタで作成します。
 - 検索統合用の設定 XML に関する情報を参照してください。
 - XML を設定するにあたっては、デスティネーションとして検索統合エンドポイントの URN を使用します。

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Tenant Manager で、 * Storage (S3) * > * Buckets * を選択します。

3. ソースバケットの名前を選択します。

バケットの詳細ページが表示されます。

4. プラットフォームサービス > 検索統合 * を選択します

5. [検索統合を有効にする]*チェックボックスをオンにします。

6. テキストボックスにメタデータ通知設定を貼り付け、 * 変更を保存 * を選択します。

The screenshot shows the 'Platform services' tab in the Tenant Manager console. It features three tabs: 'Bucket options', 'Bucket access', and 'Platform services'. Under 'Platform services', there are three sections: 'Replication' (Disabled), 'Event notifications' (Disabled), and 'Search integration' (Disabled). The 'Search integration' section is expanded, showing a description: 'Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.' Below this are three bullet points: 'Platform services must be enabled for your tenant account by a StorageGRID administrator.', 'You must have already configured an endpoint for the search integration service.', and 'You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.' A checkbox labeled 'Enable search integration' is checked. A 'Clear' button is located to the right of the checkbox. Below the checkbox is a text area containing XML configuration code:

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

 A 'Save changes' button is located at the bottom right of the form.



StorageGRID 管理者がグリッドマネージャまたは管理 API を使用して各テナントアカウントのプラットフォームサービスを有効にしておく必要があります。設定 XML の保存時にエラーが発生した場合は、StorageGRID 管理者にお問い合わせください。

7. 検索統合サービスが正しく設定されていることを確認します。
 - a. 設定 XML で指定されたメタデータ通知をトリガーする要件を満たすオブジェクトをソースバケットに追加します。

前述の例では、バケットに追加されたすべてのオブジェクトがメタデータ通知をトリガーします。
 - b. オブジェクトのメタデータとタグを含む JSON ドキュメントが、エンドポイントで指定された検索インデックスに追加されたことを確認します。

完了後

必要に応じて、次のいずれかの方法でバケットの検索統合を無効にできます。

- Storage (S3) > Buckets を選択し、Enable search integration *チェックボックスをオフにします。
- S3 API を直接使用している場合は、DELETE Bucket メタデータ通知要求を使用します。S3 クライアントアプリケーションを実装する手順を参照してください。

関連情報

["検索統合サービスについて理解する"](#)

["検索統合用の XML を設定します"](#)

["S3 REST APIを使用する"](#)

["プラットフォームサービスエンドポイントを作成します"](#)

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	項目名と概要
バケットとオブジェクトの情報	bucket: バケットの名前
key: オブジェクトキー名	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
region: バケットリージョンなど us-east-1	システムメタデータ
size: HTTPクライアントに表示されるオブジェクトのサイズ(バイト単位)	md5: オブジェクトハッシュ
ユーザメタデータ	metadata: 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 key: value

を入力します	項目名と概要
タグ	tags:オブジェクトに定義されている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 key:value



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。

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权を有し、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权については、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。