S3 プラットフォーム サービスを管理する

StorageGRID software

NetApp
December 03, 2025

目次

S3 プラットフォーム サービスを管理する

S3 プラットフォームサービス

プラットフォームサービスの概要と考慮事項

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概要と考慮事項を確認してください。

S3の詳細については、"S3 REST APIを使用する" 。

プラットフォームサービスの概要

StorageGRIDプラットフォーム サービスは、イベント通知や S3 オブジェクトおよびオブジェクト メタデータのコピーを外部の宛先に送信できるようにすることで、ハイブリッド クラウド戦略の実装を支援します。

プラットフォーム サービスのターゲットの場所は通常、 StorageGRID展開の外部にあるため、プラットフォーム サービスにより、データの外部ストレージ リソース、通知サービス、検索サービスや分析サービスを使用することで得られるパワーと柔軟性が得られます。

単一の S3 バケットに対して、プラットフォーム サービスの任意の組み合わせを構成できます。たとえば、"CloudMirrorサービス"そして"通知"StorageGRID S3 バケットに作成することで、特定のオブジェクトを Amazon Simple Storage Service (S3) にミラーリングできると同時に、各オブジェクトに関する通知をサードパーティの監視アプリケーションに送信して、AWS 経費を追跡できるようになります。

> プラットフォーム サービスの使用は、Grid Manager または Grid Management API を使用して、 StorageGRID管理者がテナント 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構成方法

プラットフォームサービスは、"Tenant Manager"または"テナント管理API"。各エンドポイントは、StorageGRID S3 バケット、Amazon Web Services バケット、Amazon SNS トピック、ローカル、AWS、またはその他の場所でホストされている Elasticsearch クラスターなどの外部の宛先を表します。

外部エンドポイントを作成した後、バケットに XML 構成を追加して、バケットのプラットフォーム サービスを有効にできます。 XML 構成では、バケットが操作するオブジェクト、バケットが実行するアクション、およびバケットがサービスに使用するエンドポイントが識別されます。

構成するプラットフォーム サービスごとに個別の XML 構成を追加する必要があります。例えば：

- キーが次の文字で始まるすべてのオブジェクトを取得したい場合 `/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保存されたときにも通知を送信する場合は、通知設定を追加する必要があります。
- これらのオブジェクトのメタデータをインデックスする場合は、検索統合を実装するために使用されるメタデータ通知構成を追加する必要があります。

構成 XML の形式は、 StorageGRIDプラットフォーム サービスを実装するために使用される S3 REST API によって管理されます。

プラットフォームサービス	S3 REST API	参照
CloudMirrorレプリケーション	• GetBucketReplication • PutBucketレプリケーション	• "CloudMirrorレプリケーション" • "バケットの操作"
通知	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "通知" • "バケットの操作"
検索統合	• バケットメタデータ通知設定の取得 • PUT バケットメタデータ通知設定	• "検索統合" • "StorageGRIDカスタム操作"

プラットフォームサービスの利用に関する考慮事項

考慮事項	詳細
宛先エンドポイントの監視	各宛先エンドポイントの可用性を監視する必要があります。宛先エンドポイントへの接続が長時間失われ、大量の要求のバックログが存在する場合、StorageGRIDへの追加のクライアント要求 (PUT 要求など) は失敗します。エンドポイントに到達可能になったら、これらの失敗したリクエストを再試行する必要があります。
宛先エンドポイントのスロットリング	リクエストの送信速度が宛先エンドポイントがリクエストを受信できる速度を超えた場合、 StorageGRIDソフトウェアはバケットの受信 S3 リクエストを調整することがあります。スロットルは、宛先エンドポイントへの送信を待機しているリクエストのバックログがある場合にのみ発生します。 目に見える唯一の影響は、受信する S3 リクエストの実行に時間がかかるようになることです。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。リクエストのバックログが増え続けると、クライアントの S3 操作 (PUT リクエストなど) は最終的に失敗します。 CloudMirror リクエストは、通常、検索統合リクエストやイベント通知リクエストよりも多くのデータ転送を伴うため、宛先エンドポイントのパフォーマンスの影響を受ける可能性が高くなります。

考慮事項	詳細
注文保証	StorageGRID は、サイト内のオブジェクトに対する操作の順序を保証します。オブジェクトに対するすべての操作が同じサイト内で行われる限り、最終的なオブジェクトの状態 (レプリケーションの場合) は常にStorageGRID内の状態と同じになります。 StorageGRID は、 StorageGRIDサイト間で操作が行われるときに、リクエストを順序付けるために最善を尽くします。たとえば、最初にサイト A にオブジェクトを書き込み、その後サイト B で同じオブジェクトを上書きした場合、CloudMirror によって宛先バケットに複製された最終的なオブジェクトが新しいオブジェクトである保証はありません。
ILMによるオブジェクトの削除	AWS CRR および Amazon Simple Notification Service の削除動作と一致させるため、 StorageGRID ILM ルールによりソースバケット内のオブジェクトが削除された場合、CloudMirror およびイベント通知リクエストは送信されません。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 またはイベント通知リクエストは送信されません。 対照的に、検索統合リクエストは、ILM によってオブジェクトが削除されたときに送信されます。
Kafkaエンドポイントの使用	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、もしあなたが `ssl.client.auth`に設定 `required`Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生する可能性があります。 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、ユーザー名とパスワードの認証情報が必要です。 • SASL/プレーン • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 注: 構成されたストレージ 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。

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
レプリケーションステータス	StorageGRIDはサポートしていません `x-amz-replication-status`ヘッダ。

考慮事項	詳細
オブジェクトのサイズ	CloudMirror レプリケーション サービスによって宛先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 5 TiB で、これはサポートされているオブジェクトの最大サイズと同じです。 注: 1 回の PutObject 操作の最大 推奨 サイズは 5 GiB (5,368,709,120 バイト) です。 5 GiB を超えるオブジェクトがある場合は、代わりにマルチパートアップロードを使用します。
バケットのバージョン管理とバージョンID	StorageGRIDのソース S3 バケットでバージョン管理が有効になっている場合は、宛先バケットでもバージョン管理を有効にする必要があります。 バージョン管理を使用する場合、S3 プロトコルの制限により、宛先バケット内のオブジェクト バージョンの順序付けはベスト エフォートであり、CloudMirror サービスによって保証されないことに注意してください。 注意: StorageGRIDのソース バケットのバージョン ID は、宛先バケットのバージョン ID とは関連がありません。
オブジェクトバージョンのタグ付け	CloudMirror サービスは、S3 プロトコルの制限により、バージョン ID を提供する PutObjectTagging または DeleteObjectTagging リクエストを複製しません。ソースと宛先のバージョン ID は関連していないため、特定のバージョン ID へのタグ更新が確実に複製されるかどうかはわかりません。 対照的に、CloudMirror サービスは、バージョン ID を指定しない PutObjectTagging リクエストまたは DeleteObjectTagging リクエストを複製します。これらのリクエストは、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バージョン) のタグを更新します。タグ付きの通常の取り込み (タグ付けの更新ではない) も複製されます。
マルチパートアップロードと `ETag`価値観	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する場合、CloudMirror サービスはパートを保持しません。その結果、`ETag`ミラーリングされたオブジェクトの値は、 `ETag`元のオブジェクトの値。
SSE-C（顧客提供のキーによるサーバー側暗号化）で暗号化されたオブジェクト	CloudMirror サービスは、SSE-C で暗号化されたオブジェクトをサポートしていません。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もうとする際に、リクエストに SSE-C リクエストヘッダーが含まれていると、操作は失敗します。
S3 オブジェクトロックが有効になっているバケット	S3 オブジェクトロックが有効になっているソースバケットまたは宛先バケットでは、レプリケーションはサポートされません。

CloudMirrorレプリケーションサービスを理解する

StorageGRID がバケットに追加された特定のオブジェクトを 1 つ以上の外部宛先バケットに複製するようにする場合は、S3 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。

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 サービスを活用してデータの分析を実行することができます。

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

CloudMirrorとILM

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、オブジェクトがソース バケットに保存されるとすぐにそれを複製し、できるだけ早く宛先バケットに配信します。オブジェクトの取り込みが成功すると、複製されたオブジェクトの配信がトリガーされます。

CloudMirrorとクロスグリッドレプリケーション

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の重要な類似点と相違点があります。。 "クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する" 。

CloudMirrorとS3バケット

CloudMirror レプリケーションは通常、外部の S3 バケットを宛先として使用するように構成されます。ただし、別のStorageGRIDデプロイメントまたは任意の S3 互換サービスを使用するようにレプリケーションを構成することもできます。

既存のバケット

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複製されません。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できます。

CloudMirror レプリケーションを使用してオブジェクトを Amazon S3 の宛先にコピーする場合、Amazon S3 では各 PUT リクエスト ヘッダー内のユーザー定義メタデータのサイズが 2 KB に制限されていることに注意してください。オブジェクトに 2 KB を超えるユーザー定義のメタデータがある場合、そのオブジェクトは複製されません。

複数の宛先バケット

単一のバケット内のオブジェクトを複数の宛先バケットに複製するには、レプリケーション設定 XML で各ルールの宛先を指定します。オブジェクトを同時に複数のバケットに複製することはできません。

バージョン管理されたバケットまたはバージョン管理されていないバケット

バージョン管理されたバケットまたはバージョン管理されていないバケットで CloudMirror レプリケーションを設定できます。宛先バケットはバージョン管理付きでもバージョン管理なしでも構いません。バージョン管理されたバケットとバージョン管理されていないバケットを任意に組み合わせて使用できます。たとえば、バージョン管理されたバケットをバージョン管理されていないソース バケットの宛先として指定したり、その逆を行ったりすることができます。バージョン管理されていないバケット間でレプリケートすることもできます。

削除、レプリケーションループ、イベント

削除動作

Amazon S3 サービス、クロスリージョンレプリケーション (CRR) の削除動作と同じです。ソースバケット内のオブジェクトを削除しても、宛先内の複製されたオブジェクトは削除されません。ソースバケットと宛先バケットの両方がバージョン管理されている場合、削除マーカーが複製されます。宛先バケットがバージョン管理されていない場合、ソースバケット内のオブジェクトを削除しても、削除マーカーが宛先バケットに複製されず、宛先オブジェクトも削除されません。

レプリケーションループからの保護

オブジェクトが宛先バケットに複製されると、 StorageGRID はそれらを「レプリカ」としてマークします。宛先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度レプリケートしないため、偶発的なレプリケーション ループから保護されます。このレプリカ マーキングはStorageGRID内部のものであり、Amazon S3 バケットを宛先として使用するときに AWS CRR を活用できないことはありません。

> ⓘ レプリカをマークするため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 は、2 つのグリッド間の双方向 CloudMirror をサポートしています。

宛先バケット内のイベント

宛先バケット内のイベントの一意性と順序は保証されません。配信の成功を保証するために実行された操作の結果として、ソース オブジェクトの複数の同一コピーが宛先に配信される場合があります。まれに、同じオブジェクトが 2 つ以上の異なるStorageGRIDサイトから同時に更新されると、宛先バケットでの操作の順序がソース バケットでのイベントの順序と一致しない場合があります。

バケットの通知を理解する

StorageGRID が指定されたイベントに関する通知を宛先の Kafka クラスターまたは Amazon Simple Notification Service に送信するようにする場合は、S3 バケットのイベント通知を有効にすることができます。

たとえば、バケットに追加された各オブジェクト（重要なシステム イベントに関連付けられたログ ファイルを表すオブジェクト）に関するアラートを管理者に送信するように設定できます。

イベント通知は、通知設定で指定されたとおりにソース バケットで作成され、宛先に配信されます。オブジェクトに関連付けられた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、配信のためにキューに入れられます。

通知の一意性と順序は保証されません。配信の成功を保証するために実行された操作の結果として、イベントの通知が複数宛先に配信される場合があります。また、配信は非同期であるため、特に異なるStorageGRIDサイトから発信された操作の場合、宛先での通知の時間順序がソース バケット上のイベントの順序と一致することは保証されません。使用することができます `sequencer`Amazon S3 ドキュメントで説明されているように、イベント メッセージ内のキーを使用して、特定のオブジェクトのイベントの順序を決定します。

StorageGRIDイベント通知は、いくつかの制限付きで Amazon S3 API に準拠します。

- 次のイベント タイプがサポートされています。
  - s3:オブジェクトが作成されました:
  - s3:オブジェクト作成:配置
  - s3:オブジェクト作成:投稿

- s3:オブジェクト作成:コピー
- s3:ObjectCreated:CompleteMultipartUpload
- s3:オブジェクトが削除されました:
- s3:オブジェクトが削除されました:削除
- s3:オブジェクトが削除されました:削除マーカーが作成されました
- s3:オブジェクトの復元:投稿

- StorageGRIDから送信されるイベント通知では標準の JSON 形式が使用されますが、表に示すように、一部のキーは含まれず、他のキーには特定の値が使用されます。

キー名	**StorageGRID**の価値
イベントソース	`sgws:s3`
awsリージョン	含まれていません
x-amz-id-2	含まれていません
アーン	`urn:sgws:s3:::bucket_name`

検索統合サービスを理解する

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、オブジェクトが作成または削除されるか、そのメタデータまたはタグが更新されるたびに、S3 オブジェクトのメタデータを宛先エンドポイントに自動的かつ非同期的に送信するカスタムStorageGRIDサービスです。その後、宛先サービスによって提供される高度な検索、データ分析、視覚化、または機械学習ツールを使用して、オブジェクト データを検索、分析し、洞察を得ることができます。

たとえば、S3 オブジェクトのメタデータをリモート Elasticsearch サービスに送信するようにバケットを設定できます。その後、Elasticsearch を使用してバケット全体の検索を実行し、オブジェクト メタデータに存在するパターンの高度な分析を実行できます。

S3 オブジェクト ロックが有効になっているバケットで 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 (保持期限や法的保留ステータスを含む) は、Elasticsearch に送信されるメタデータに含まれません。

> 検索統合サービスによりオブジェクト メタデータが宛先に送信されるため、その構成 XML は「メタデータ 通知構成 XML」と呼ばれます。この構成 XML は、イベント 通知を有効にするために使用される「通知構成 XML」とは異なります。

検索統合と**S3**バケット

バージョン管理されているバケットまたはバージョン管理されていないバケットに対して検索統合サービスを有効にできます。検索統合は、メタデータ通知構成 XML を、操作対象のオブジェクトとオブジェクト メタデータの宛先を指定するバケットに関連付けることによって構成されます。

メタデータ通知は、バケット名、オブジェクト名、およびバージョン ID (存在する場合) で名前が付けられた JSON ドキュメントの形式で生成されます。各メタデータ通知には、オブジェクトのすべてのタグとユーザー 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。

> タグとユーザー メタデータの場合、 StorageGRID は日付と数値を文字列または S3 イベント通知として Elasticsearch に渡します。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 を構成するには、動的フィールド マッピングと日付形式のマッピングに関する Elasticsearch の指示に従います。検索統合サービスを構成する前に、インデックスで動的フィールド 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が作成された後は、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。

検索通知

メタデータ通知は次の場合に生成され、配信キューに追加されます。

- オブジェクトが作成されます。
- グリッドの ILM ポリシーの操作の結果としてオブジェクトが削除される場合を含め、オブジェクトが削除されます。
- オブジェクトのメタデータまたはタグが追加、更新、または削除されます。更新時には、変更された値だけでなく、メタデータとタグの完全なセットが常に送信されます。

メタデータ通知構成 XML をバケットに追加すると、作成した新しいオブジェクトと、データ、ユーザー メタデータ、またはタグを更新して変更したオブジェクトについて通知が送信されます。ただし、バケット内にすでに存在するオブジェクトについては通知は送信されません。バケット内のすべてのオブジェクトのオブジェクト メタデータが宛先に送信されることを確認するには、次のいずれかを実行する必要があります。

- バケットを作成した直後、オブジェクトを追加する前に、検索統合サービスを構成します。
- バケット内にすでに存在するすべてのオブジェクトに対してアクションを実行し、メタデータ通知メッセージを宛先に送信するようにトリガーします。

検索統合サービスと**Elasticsearch**

StorageGRID検索統合サービスは、Elasticsearch クラスターを宛先としてサポートします。他のプラットフォーム サービスと同様に、宛先は、サービスの構成 XML で URN が使用されるエンドポイントで指定されます。使用 "NetApp Interoperability Matrix Tool"サポートされている Elasticsearch のバージョンを確認します。

プラットフォーム サービスのエンドポイントを管理する

プラットフォーム サービスのエンドポイントを構成する

バケットのプラットフォーム サービスを構成する前に、プラットフォーム サービスの宛先となるエンドポイントを少なくとも 1 つ構成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管理者によってテナントごとに有効化されます。プラットフォーム サービス エンドポイントを作成または使用するには、ストレージ ノードが外部エンドポイント リソースにアクセスできるようにネットワークが構成されているグリッド内で、エンドポイントの管理権限またはルート アクセス権限を持つテナント ユーザーである必要があります。 1 つのテナントに対して、最大 500 個のプラットフォーム サービス エンドポイントを構成できます。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 エンドポイントは、 StorageGRID が外部の宛先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複製する場合は、StorageGRID がAmazon の宛先バケットにアクセスするために必要な情報と認証情報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。

各タイプのプラットフォーム サービスには独自のエンドポイントが必要であるため、使用する予定のプラットフォーム サービスごとに少なくとも 1 つのエンドポイントを構成する必要があります。プラットフォーム サービス エンドポイントを定義した後、サービスを有効にするために使用される構成 XML で、エンドポイントの URN を宛先として使用します。

複数のソース バケットの宛先として同じエンドポイントを使用できます。たとえば、複数のソース バケットを構成して、オブジェクト メタデータを同じ検索統合エンドポイントに送信するようにすることで、複数のバケットにわたって検索を実行できるようになります。また、ソースバケットを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 1 つの Amazon Simple Notification Service (Amazon SNS) トピックに送信し、オブジェクトの削除に関する通知を 2 番目の Amazon SNS トピックに送信するといったことが可能になります。

CloudMirror レプリケーションのエンドポイント

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ています。これらのバケットは、Amazon Web Services、同じまたはリモートのStorageGRIDデプロイメント、あるいは別のサービスでホストされている場合があります。

通知のエンドポイント

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、もしあなたが `ssl.client.auth` に設定 `required`Kafka ブローカー構成では、Kafka エンドポイント構成の問題が発生す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 クラスターを表す検索統合エンドポイントをサポートしています。これらの Elasticsearch クラスターは、ローカルデータセンターに配置することも、AWS クラウドやその他の場所でホストすることもできます。

検索統合エンドポイントは、特定の Elasticsearch 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する必要があります。そうしないと、エンドポイントの作成は失敗します。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 エンドポイントの **URN** を指定します

プラットフォーム サービス エンドポイントを作成するときは、一意のリソース名 (URN) を指定する必要があります。プラットフォーム サービスの構成 XML を作成するときに、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。

StorageGRID は、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にそれを検証します。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、アクセスでき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エンドポイントのURNは、次のいずれかで始まる必要があります。 `arn:aws`または `urn:mysite`、 次のように：

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

たとえば、 StorageGRIDでホストされているCloudMirrorエンドポイントのURNを指定する場合、URNは次のようになります。 `urn:sgws` 。

URN の次の要素は、次のようにプラットフォーム サービスの種類を指定します。

サービス	タイプ
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でホストされているCloudMirrorエンドポイントのURNを引き続き指定するには、以下を追加します。 `s3`取得するため `urn:sgws:s3`。

URN の最後の要素は、宛先 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`

サービス	特定のリソース
検索統合	`domain-name/index-name/type-name` 注: Elasticsearch クラスターがインデックスを自動的に作成するように設定されていない場合は、エンドポイントを作成する前に手動でインデックスを作成する必要があります。

AWS および **GCP** でホストされているサービスの **URN**

AWS および GCP エンティティの場合、完全な URN は有効な AWS ARN です。例えば：

- 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、 `domain-name`リテラル文字列を含める必要があります `domain/`、ここに示すように。

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、URN の 3 番目と最後の位置に必要な要素が含まれていれば、有効で一意の URN を作成する任意の方法で URN を指定できます。オプションで指定された要素は空白のままにしておくことも、リソースを識別して URN を一意にする方法で指定することもできます。例えば：

- CloudMirror レプリケーション:

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

StorageGRIDでホストされているCloudMirrorエンドポイントの場合、次の文字で始まる有効な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
  ```

  ローカルにホストされた検索統合エンドポイントの場合、 `domain-name`エンドポイントの URN が一意である限り、要素には任意の文字列を指定できます。

プラットフォーム サービス エンドポイントを作成する

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 つ作成する必要があります。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。
- 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が作成されました。
  - 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: 宛先クラスターがインデックスを自動的に作成するように構成されていない場合の Elasticsearch インデックス。
- 宛先リソースに関する情報は次の通りです。
  - URI (Uniform Resource Identifier) 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予定の場合は、グリッド管理者に問い合わせて、入力する必要がある値を確認してください。

  - ユニークリソース名 (URN)

"プラットフォーム サービス エンドポイントの URN を指定します"

- 認証資格情報（必要な場合）：

  検索統合エンドポイント

  検索統合エンドポイントでは、次の資格情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー
  - 基本的なHTTP: ユーザー名とパスワード

  CloudMirror レプリケーションエンドポイント

  CloudMirror レプリケーション エンドポイントの場合、次の認証情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー
  - CAP (C2S アクセス ポータル): 一時資格情報 URL、サーバーおよび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キー パスフレーズ。

  Amazon SNSエンドポイント

  Amazon SNS エンドポイントの場合、次の認証情報を使用できます。

  - アクセスキー: アクセスキーIDとシークレットアクセスキー

  Kafkaエンドポイント

  Kafka エンドポイントの場合、次の資格情報を使用できます。

  - SASL/PLAIN: ユーザー名とパスワード
  - SASL/SCRAM-SHA-256: ユーザー名とパスワード
  - SASL/SCRAM-SHA-512: ユーザー名とパスワード

- セキュリティ証明書（カスタム CA 証明書を使用している場合）

- Elasticsearch セキュリティ機能が有効になっている場合は、接続テストのためのクラスター監視権限と、ドキュメント更新のためのインデックス書き込み権限またはインデックスとインデックス削除の両方の権限が付与されます。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、エンドポイント ページにリストされるときにエンドポイント名の横に表示されるため、名前にその情報を含める必要はありません。

4. **URI** フィールドに、エンドポイントの一意のリソース識別子 (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の場合はポート443、HTTP URIの場合はポート80（ほとんどのエンドポイント）
- HTTPS および HTTP URI 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高可用性（HA）グループの仮想IP（VIP）のDNSエントリを表し、 `10443`ロード バランサーのエンドポイントで定義されたポートを表します。

> 可能な限り、単一障害点を回避するために、負荷分散ノードの 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。 **URN** フィールドにバケット名を含めます。

5. エンドポイントの一意のリソース名 (URN) を入力します。

> エンドポイントを作成した後は、エンドポイントの URN を変更することはできません。

6. *続行*を選択します。
7. *認証タイプ*の値を選択します。

検索統合エンドポイント

検索統合エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
基本的なHTTP	ユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード

CloudMirror レプリケーションエンドポイント

CloudMirror レプリケーション エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー
CAP（C2Sアクセスポータル）	証明書とキーを使用して、宛先への接続を認証します。	• 一時認証情報URL • サーバー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） • クライアントの秘密鍵のパスフレーズ（オプション）

Amazon SNSエンドポイント

Amazon SNS エンドポイントの認証情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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 スタイルの認証情報を使用して、宛先との接続を認証します。	• アクセス キー ID • シークレット アクセス キー

Kafkaエンドポイント

Kafka エンドポイントの資格情報を入力またはアップロードします。

指定する資格情報には、宛先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	**Credentials**
匿名	宛先への匿名アクセスを提供します。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ー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-256	チャレンジ レスポンス プロトコルと SHA-256 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード
SASL/SCRAM-SHA-512	チャレンジ レスポンス プロトコルと SHA-512 ハッシュを使用したユーザー名とパスワードを使用して、宛先への接続を認証します。	• ユーザー名 • パスワード

ユーザー名とパスワードが Kafka クラスターから取得された委任トークンから派生している場合は、委任された認証を使用する を選択します。

8. *続行*を選択します。
9. *サーバーの検証*のラジオ ボタンを選択して、エンドポイントへの TLS 接続を検証する方法を選択します。

証明書検証の種類	説明
カスタムCA証明書を使用する	カスタム 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コピーして、[CA 証明書] テキスト ボックスに貼り付けます。
オペレーティング システムの CA 証明書を使用する	接続を保護するには、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 証明書を使用します。
証明書を検証しない	TLS 接続に使用される証明書が検証されていません。このオプションは安全ではありません。

10. *エンドポイントのテストと作成*を選択します。
    - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、*エンドポイントのテストと作成*を選択します。

> 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場合、エンドポイントの作成は失敗します。 StorageGRID管理者に問い合わせてください。

エンドポイントを構成したら、その URN を使用してプラットフォーム サービスを構成できます。

関連情報

- "プラットフォーム サービス エンドポイントの URN を指定します"
- "CloudMirrorレプリケーションを構成する"
- "イベント通知の設定"
- "検索統合サービスを構成する"

プラットフォーム サービス エンドポイントのテスト接続

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、エンドポイントの接続をテストして、宛先リソースが存在し、指定した資格情報を使用してアクセスできることを検証できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

タスク概要

StorageGRID は、資格情報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 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

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。

3. *テスト接続*を選択します。

   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、[構成] を選択して情報を更新します。次に、[テストして変更を保存]を選択します。

プラットフォーム サービス エンドポイントを編集する

プラットフォーム サービス エンドポイントの構成を編集して、名前、URI、その他の詳細を変更できます。たとえば、期限切れの資格情報を更新したり、フェイルオーバーのためにバックアップ Elasticsearch インデックスを指すように URI を変更したりする必要がある場合があります。プラットフォーム サービス エンドポイントの URN を変更することはできません。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

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. *構成*を選択します。
4. 必要に応じて、エンドポイントの構成を変更します。

   エンドポイントを作成した後は、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、**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 キーを貼り付けて、必要に応じてキーを変更します。変更をキャンセルする必要がある場合は、「**S3** キー編集を元に戻す」を選択します。
- CAP (C2S アクセス ポータル) 認証の場合、一時的な資格情報の URL またはオプションのクライアント秘密キーのパスフレーズを変更し、必要に応じて新しい証明書とキー ファイルをアップロードします。

> クライアントの秘密キーは、OpenSSL 暗号化形式または暗号化されていない秘密キー形式である必要があります。

d. 必要に応じて、サーバーの検証方法を変更します。

5. *テストして変更を保存*を選択します。
   - 指定された資格情報を使用してエンドポイントに到達できる場合は、成功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に失敗した場合、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、[テストして変更を保存] 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する

関連付けられているプラットフォーム サービスを使用したくなくなった場合は、エンドポイントを削除できます。

開始する前に

- テナントマネージャーにサインインするには、"サポートされているウェブブラウザ" 。
- あなたは、"エンドポイントまたはルートアクセス権限を管理する" 。

手順

1. ストレージ **(S3)** > プラットフォーム サービス 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、すでに構成されているプラットフォーム サービス エンドポイントのリストが表示されます。

2. 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、その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付けられたプラットフォーム サービスが無効になります。まだ完了していないリクエストはすべて削除されます。削除された URN を参照しないようにバケット構成を変更するまで、新しいリクエストは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。

3. 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。

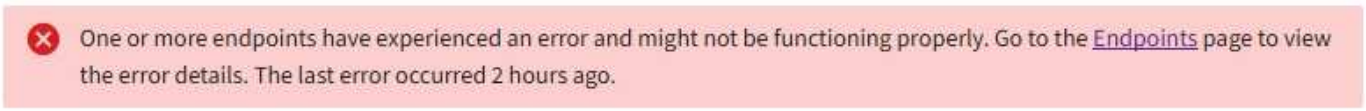
4. *エンドポイントの削除*を選択します。

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

StorageGRID がプラットフォーム サービス エンドポイントとの通信を試行する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。プラットフォーム サービス エンドポイント ページの [最後のエラー] 列には、エラーが発生した時間が表示されます。エンドポイントの資格情報に関連付けられた権限が正しくない場合、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する

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、Tenant Manager ダッシュボードに警告メッセージが表示されます。エラーの詳細を確認するには、プラットフォーム サービス エンドポイント ページにアクセスしてください。



ダッシュボードに表示されるのと同じエラーが、プラットフォーム サービス エンドポイント ページの上部にも表示されます。より詳細なエラー メッセージを表示するには:

手順

1. エンドポイントのリストから、エラーが発生している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のみが表示され、エラーが発生した時間を示します。赤いXアイコンを含むエラー過去 7 日以内に発生しました。

エラーがまだ発生しているか確認する

一部のエラーは、解決された後も 最後のエラー 列に引き続き表示される場合があります。エラーが最新であるかどうかを確認するか、解決済みのエラーをテーブルから強制的に削除するには、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。

*テスト接続*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し、現在の資格情報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。

エンドポイントエラーを解決する

エンドポイントの詳細ページの 最後のエラー メッセージを使用すると、エラーの原因を特定するのに役立ちます。エラーによっては、問題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があります。たとえば、適切なアクセス権限がないかアクセス キーの有効期限が切れているためにStorageGRID が宛先 S3 バケットにアクセスできない場合、CloudMirroring エラーが発生する可能性があります。メッセージは「エンドポイント資格情報または宛先アクセスのいずれかを更新する必要があります」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、[テストして変更を保存] 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、現在の資格情報でアクセス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構成を編集します。
4. 接続 > *接続テスト*を選択します。

権限が不十分なエンドポイント認証情報

StorageGRID は、プラットフォーム サービス エンドポイントを検証する際に、エンドポイントの資格情報を使用して宛先リソースに接続できることを確認し、基本的な権限チェックを実行します。ただし、StorageGRID は、特定のプラットフォーム サービス操作に必要なすべての権限を検証するわけではありません。このため、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) が発生した場合は、エンドポイントの資格情報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する"
- "プラットフォーム サービス エンドポイントのテスト接続"
- "プラットフォーム サービス エンドポイントを編集する"

CloudMirrorレプリケーションを構成する

バケットの CloudMirror レプリケーションを有効にするには、有効なバケット レプリケーション構成 XML を作成して適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- レプリケーション ソースとして機能するバケットはすでに作成されています。
- CloudMirror レプリケーションの宛先として使用するエンドポイントがすでに存在し、その URN があること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

CloudMirror レプリケーションは、ソース バケットからエンドポイントで指定された宛先バケットにオブジェクトをコピーします。

バケットレプリケーションとその設定方法に関する一般的な情報については、以下を参照してください。

"Amazon Simple Storage Service (S3) ドキュメント: オブジェクトのレプリケーション" 。 StorageGRIDがGetBucketReplication、DeleteBucketReplication、およびPutBucketReplicationを実装する方法については、"バケットの操作" 。

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の重要な類似点と相違点があります。詳細については、"クロスグリッドレプリケーションとCloudMirrorレプリケーションを比較する" 。

CloudMirror レプリケーションを構成するときは、次の要件と特性に注意してください。

- 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場合、各宛先の 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になっているソースバケットまたは宛先バケットでは、レプリケーションはサポートされません。
- 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は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 クラスを指定すると、 StorageGRID は宛先 S3 エンドポイントに対して操作を実行するときにそのクラスを使用します。宛先エンドポイントも指定されたストレージ クラスをサポートする必要があります。宛先システムベンダーから提供される推奨事項に必ず従ってください。

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。
    - テキスト エディターを使用して、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構成 XML を作成します。
    - XML を構成する場合:
        - StorageGRID はレプリケーション構成の V1 のみをサポートすることに注意してください。これは、 StorageGRIDが `Filter`ルールの要素であり、オブジェクト バージョンの削除については V1 規則に従います。詳細については、レプリケーション構成に関する Amazon のドキュメントを参照してください。
        - 宛先として S3 バケットエンドポイントの URN を使用します。
        - オプションで `<StorageClass>`要素を選択し、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、 `STANDARD`ストレージクラスが使用されます。
            - `STANDARD_IA`: (標準 - アクセス頻度が低い)このストレージ クラスは、アクセス頻度は低いが、必要なときに迅速なアクセスが必要なデータに使用します。
            - `REDUCED_REDUNDANCY`: このストレージクラスは、冗長性が低くても保存できる、重要でない再現可能なデータに使用します。 `STANDARD`ストレージクラス。
        - 指定する場合 `Role`構成 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. ダッシュボードから*バケットの表示*を選択するか、ストレージ **(S3)** > *バケット*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. レプリケーション構成 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。

   プラットフォーム サービスは、Grid Manager または Grid Management API を使用して、StorageGRID管理者によって各テナント アカウントに対して有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. レプリケーションが正しく構成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複製されます。

   b. オブジェクトが宛先バケットに複製されたことを確認します。

      小さなオブジェクトの場合、レプリケーションはすぐに行われます。

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する"

イベント通知の設定

バケットの通知を有効にするには、通知設定 XML を作成し、テナント マネージャを使用してその XML をバケットに適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- 通知のソースとして機能するバケットはすでに作成されています。
- イベント通知の宛先として使用するエンドポイントがすでに存在し、その URN を所有していること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

通知設定 XML をソース バケットに関連付けることで、イベント通知を設定します。通知設定 XML は、バケット通知を設定するための S3 規則に従い、宛先の 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。

イベント通知とその設定方法に関する一般的な情報については、 "Amazonのドキュメント" 。 StorageGRIDがS3バケット通知設定APIを実装する方法については、"S3 クライアントアプリケーションの実装手順" 。

バケットのイベント通知を構成するときは、次の要件と特性に注意してください。

- 有効な通知構成 XML を作成して適用する場合は、各宛先の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。
- S3 オブジェクト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 (保持期限や法的保留ステータスを含む) は通知メッセージに含まれません。
- 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に対して指定されたイベントが発生するたびに通知が生成され、宛先エンドポイントとして使用される Amazon SNS または Kafka トピックに送信されます。
- オブジェクトを含むバケットに対してイベント通知を有効にすると、通知設定が保存された後に実行されたアクションに対してのみ通知が送信されます。

手順

1. ソースバケットの通知を有効にします。
    - テキスト エディタを使用して、S3 通知 API で指定されているように、イベント通知を有効にするために必要な通知設定 XML を作成します。
    - XML を構成するときは、イベント通知エンドポイントの URN を宛先トピックとして使用します。

```
<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. テナント マネージャーで、ストレージ **(S3)** > バケット 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選択します。
6. 通知構成 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。

   > プラットフォーム サービスは、Grid Manager または Grid Management API を使用して、StorageGRID管理者によって各テナント アカウントに対して有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. イベント通知が正しく構成されていることを確認します。

   a. 構成 XML で設定された通知をトリガーするための要件を満たすソース バケット内のオブジェクトに対してアクションを実行します。

      この例では、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/`接頭辞。

   b. 通知が宛先の Amazon SNS または Kafka トピックに配信されたことを確認します。

      たとえば、宛先トピックが 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電子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":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

+ 通知が宛先トピックで受信された場合、ソース バケットがStorageGRID通知用に正常に構成されています。

関連情報

"バケットの通知を理解する"

"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する"

検索統合サービスを構成する

バケットの検索統合を有効にするには、検索統合 XML を作成し、テナント マネージャを使用してその XML をバケットに適用します。

開始する前に

- StorageGRID管理者によって、テナント アカウントに対してプラットフォーム サービスが有効化されました。
- インデックスを作成する内容を含む S3 バケットはすでに作成されています。
- 検索統合サービスの宛先として使用するエンドポイントが既に存在し、その URN を所有していること。
- あなたは、"すべてのバケットまたはルートアクセス権限を管理する" 。これらの権限は、テナント マネージャを使用してバケットを構成するときに、グループまたはバケット ポリシーの権限設定をオーバーライドします。

タスク概要

ソース バケットの検索統合サービスを構成すると、オブジェクトを作成するか、オブジェクトのメタデータまたはタグを更新すると、オブジェクトのメタデータが宛先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に対して検索統合サービスを有効にすると、既存のオブジェクトのメタデータ通知は自動的に送信されません。これらの既存のオブジェクトを更新して、そのメタデータが宛先検索インデックスに追加されるようにします。

手順

1. バケットの検索統合を有効にします。
    - テキスト エディターを使用して、検索統合を有効にするために必要なメタデータ通知 XML を作成します。
    - XML を構成するときは、検索統合エンドポイントの URN を宛先として使用します。

      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、プレフィックスを持つオブジェクトのメタデータを送信できます。 `images` 1つの宛先に、そしてプレフィックスを持つオブジェクトのメタデータ `videos`別の人に。プレフィックスが重複する構成は無効であり、送信時に拒否されます。たとえば、プレフィックスを持つオブジェクトに対して1つのルールを含む構成では、 `test`接頭辞を持つオブジェクトに対する2番目のルール `test2`は許可されません。

      必要に応じて、メタデータ構成XMLの例 。

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知構成 XML の要素:

Name	説明	必須
メタデータ通知構成	メタデータ通知のオブジェクトと宛先を指定するために使用されるルールのコンテナ タグ。 1 つ以上の Rule 要素が含まれます。	はい
Rule	指定されたインデックスにメタデータを追加するオブジェクトを識別するルールのコンテナ タグ。 プレフィックスが重複するルールは拒否されます。 MetadataNotificationConfiguration 要素に含まれます。	はい
ID	ルールの一意の識別子。 ルール要素に含まれます。	いいえ
ステータス	ステータスは「有効」または「無効」になります。無効にされているルールに対してはアクションは実行されません。 ルール要素に含まれます。	はい
接頭辞	プレフィックスに一致するオブジェクトはルールの影響を受け、そのメタデータは指定された宛先に送信されます。 すべてのオブジェクトを一致させるには、空のプレフィックスを指定します。 ルール要素に含まれます。	はい
デスティネーション	ルールの宛先のコンテナ タグ。 ルール要素に含まれます。	はい

Name	説明	必須
壷	オブジェクト メタデータが送信される宛先の URN。次のプロパティを持つStorageGRIDエンドポイントの URN である必要があります。 • `es`3 番目の要素である必要があります。 • URNは、メタデータが格納されているインデックスとタイプで終わる必要があります。形式は次のようになります。 `domain-name/myindex/mytype` 。 エンドポイントは、テナント マネージャーまたはテナント管理 API を使用して構成されます。それらは次の形式をとります: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` 構成 XML を送信する前にエンドポイントを構成する必要があります。そうしないと、404 エラーが発生して構成が失敗します。 URN は Destination 要素に含まれます。	はい

2. テナント マネージャーで、ストレージ **(S3)** > バケット 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選択します。
6. メタデータ通知構成をテキスト ボックスに貼り付け、[変更を保存] を選択します。

   プラットフォーム サービスは、Grid Manager または Management API を使用して、StorageGRID管理者がテナント アカウントごとに有効にする必要があります。構成 XML を保存するときにエラーが発生した場合は、 StorageGRID管理者に問い合わせてください。

7. 検索統合サービスが正しく構成されていることを確認します。
   a. 構成 XML で指定されているメタデータ通知をトリガーするため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、バケットに追加されたすべてのオブジェクトによってメタデータ通知がトリガーされます。

   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。

終了後の操作

必要に応じて、次のいずれかの方法を使用してバケットの検索統合を無効にすることができます。

- ストレージ **(S3)** > バケット を選択し、検索統合を有効にする 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 メタデータ通知リクエストを使用します。 S3 クライアント アプリケーションの実装手順を参照してください。

例: すべてのオブジェクトに適用されるメタデータ通知設定

この例では、すべてのオブジェクトのオブジェクト メタデータが同じ宛先に送信されます。

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

例: **2**つのルールを使用したメタデータ通知構成

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 `/images`一つの宛先に送信される一方、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は `/videos`2 番目の宛先に送信されます。

```
<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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

メタデータ通知形式

バケットの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が追加、更新、または削除されるたびに、JSON ドキュメントが生成され、宛先エンドポイントに送信されます。

この例では、キーを持つオブジェクトが生成された場合に生成されるJSONの例を示します。 `SGWS/Tagging.txt`バケットに作成されます `test`。その `test`バケットはバージョン管理されていないため、 `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"
  }
}
```

JSONドキュメントに含まれるフィールド

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。

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`: オブジェクト バージョン（バージョン管理されたバケット内のオブジェクトの場合）

`region`: バケット領域、例 `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サイズ（バイト単位）

`md5`: オブジェクトハッシュ

ユーザーメタデータ

`metadata`: オブジェクトのすべてのユーザーメタデータ（キーと値のペア）

`key:value`

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（キーと値のペア）

`key:value`

Elasticsearchで結果を表示する方法

タグとユーザー メタデータの場合、 StorageGRID は日付と数値を文字列または S3 イベント通知として

Elasticsearch に渡します。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 を構成するには、動的フィールド マッピングと日付形式のマッピングに関する Elasticsearch の指示に従います。検索統合サービスを構成する前に、インデックスで動的フィールド マッピングを有効にします。ドキュメントのインデックスが作成された後は、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

商標に関する情報